

IBM Security Identity Manager
Version 7.0.2

Administration Guide



Contents

Tables.....	XV
--------------------	-----------

Chapter 1. Virtual appliance management.....	1
---	----------

Appliance Dashboard.....	1
Viewing the Disk Usage widget.....	1
Viewing the Partition Information widget.....	1
Viewing IP addresses.....	2
Viewing the Notifications widget.....	2
Viewing the Quick Links widget.....	3
Viewing the Server Control widget.....	3
Viewing the Middleware Monitor widget.....	3
Viewing the Cluster Status widget.....	4
Manage system settings for the virtual appliance.....	5
Managing the update history information.....	5
Managing the licensing information.....	6
Managing the firmware settings.....	6
Installing a fix pack.....	7
Managing the About page information.....	7
Managing the memory usage.....	8
Managing the CPU usage.....	9
Managing the storage usage.....	9
Monitoring the IBM Security Identity Manager Server.....	10
Viewing the event log.....	13
Managing the SNMP monitoring.....	14
Managing the application interfaces.....	15
Managing advanced tuning settings.....	17
Managing hosts file.....	21
Configuring static routes.....	22
Managing the date and time settings.....	23
Managing the administrator settings.....	24
Managing the snapshots.....	24
Managing the support files.....	26
Updating the management SSL certificate.....	27
Configuring system audit events.....	28
Restarting or shutting down.....	32

Chapter 2. Administration console.....	33
---	-----------

Home.....	33
Change Password.....	34
Select a User.....	34
Change Passwords.....	35
Service Details.....	36
Account Information.....	37
View Personal Profile.....	37
Personal Information.....	37
Business Information.....	37
Contact Information.....	38
Business Unit Details.....	38
Manage Roles.....	38
Manage Roles.....	38

Export access data.....	41
Import access data.....	41
Organizational Role.....	42
Create Role.....	42
Role Information.....	49
Role Information.....	51
Change Role.....	52
Manage User Members and Child Roles.....	59
Add User Members.....	62
Associate role assignment attributes.....	63
Add Child Roles.....	63
Select Users.....	64
Select Roles.....	65
Definition (Rule).....	66
Schedule.....	66
Schedule.....	66
Set Assignment Values.....	66
Enable Access.....	66
Manage Services.....	67
Manage Organization Structure.....	159
Manage Organization Structure.....	159
Organization Details.....	160
Admin Domain Details.....	161
Business Partner Unit Details.....	161
Location Details.....	161
Organizational Unit Details.....	161
Manage Users.....	162
Select a User.....	162
Select User Type.....	164
Create a User.....	164
Associate role assignment attributes.....	167
Set assignment values.....	167
User Information.....	168
Change Profile.....	168
Change Profile.....	169
Associate role assignment attributes.....	172
Set assignment values.....	172
Change Profile.....	172
Change Passwords.....	173
Select a User.....	175
Reset Passwords.....	176
Accounts.....	176
Account category.....	178
Request an Account.....	179
Change an Account.....	187
Noncompliant Value.....	196
Manage Access.....	196
Access Details.....	197
Select Access.....	197
Select Accounts.....	198
Request Access Confirmation.....	198
Remove Access.....	199
Select a Recertification Policy.....	200
Select a Service.....	200
Select a User.....	201
Success.....	202
Confirm.....	202
Manage Services.....	202

Select a Service.....	202
Export access data.....	205
Import access data.....	206
Enable Access.....	206
Service Status Information.....	207
Create a Service.....	208
Search Results.....	228
Change a Service.....	228
Change a Manual Service.....	248
Change Message: <i>Operation</i>	251
Set Up Account Reconciliation.....	251
Set Up Account Reconciliation.....	252
Select Query.....	253
Select Action.....	254
Configure Policy Enforcement.....	255
Manage Groups on Service.....	256
Define Access.....	257
Manage Group Members.....	259
Add Members.....	260
Manage Group Membership.....	261
Access Recertification Status.....	262
Account Information.....	263
Accounts.....	271
Noncompliant Account Attributes.....	274
Change an Account.....	274
Account Recertification Status.....	283
Confirm.....	284
Manage Account Defaults.....	284
Manage Orphan Accounts.....	295
Manage Orphan Accounts.....	295
Manage Groups.....	296
Select a Service.....	296
Select Group.....	297
Export access data.....	298
Import access data.....	299
Change Group.....	299
Business Unit Details.....	299
Enable Access.....	300
Create Group.....	300
Manage Policies.....	302
Adoption Policies.....	302
Separation of Duty Policies.....	315
Password Policies.....	325
ID Policies.....	333
Provisioning Policies.....	337
Service Selection Policies.....	349
Recertification Policies.....	352
Design Workflow.....	400
Manage Account Request Workflows.....	400
Manage Access Request Workflows.....	408
Set system security.....	416
Configure Forgotten Password Settings.....	416
Set Security Properties.....	418
Select Group.....	419
Create a Group.....	420
Add Members.....	422
Select a Service.....	422
Select Group.....	423

Create a Group.....	425
Advanced Search.....	433
Change a group.....	433
Add Members.....	439
Change Group.....	441
View Membership.....	441
Group Details.....	442
Membership.....	442
Manage Access Control Items.....	442
ACI Owners.....	443
Create Access Control Item.....	444
Change Access Control Item.....	457
Define Views.....	469
View Details.....	470
Reports.....	473
Options.....	473
Account Operations.....	473
Account Operations Performed by an Individual.....	474
Approvals and Rejections.....	474
Operation Report.....	475
Pending Approvals.....	476
Rejected Report.....	476
User Report.....	477
Options.....	477
Account Report.....	478
Accounts/Access Pending Recertification Report.....	478
Individual Access.....	479
Individual Accounts.....	479
Individual Accounts by Role associated with Provisioning Policy.....	480
Recertification Change History Report.....	480
Suspended Individuals.....	481
Options.....	482
Reconciliation Statistics.....	482
Services.....	482
Summary of Accounts on Service.....	483
Options.....	483
Access Control Information (ACIs).....	484
Access Report.....	484
Audit Events.....	485
Dormant Accounts.....	485
Non-Compliant Accounts.....	486
Orphan Accounts.....	486
Policies.....	486
Policies Governing a Role.....	487
Recertification Policies Report.....	487
Entitlements Granted to an Individual.....	488
Suspended Accounts.....	488
Separation of Duty Policy Definition.....	489
Options.....	489
Custom Report.....	489
Select Entity Attributes.....	489
Custom Report Template.....	490
Design Report.....	490
Report Column Details.....	493
Data Synchronization.....	494
Synchronization Schedule.....	494
Configure System.....	495
Manage Service Types.....	495

Manage Service Types.....	496
Add Group.....	499
Change Group.....	500
Select LDAP Class.....	500
Select a Super Class.....	500
Add Attribute to Custom Service Schema.....	501
Change Custom Service Schema Attribute.....	501
View Attribute.....	502
Select Attribute.....	502
Select Attribute.....	502
Import Service Type.....	503
Global Adoption Policies.....	503
Global Adoption Policies.....	504
Workflow Notification Properties.....	505
Notification Template.....	506
Post Office.....	506
Test E-mail.....	507
Design Forms.....	507
Manage Entities.....	518
Create an Entity.....	519
Change an Entity.....	521
Select LDAP Class.....	522
Select Attribute.....	523
Manage Operations.....	523
Add Operation.....	524
Define Operation.....	525
Manage Life Cycle Rules.....	526
Manage Life Cycle Rules.....	527
Define Schedule.....	528
Configure Policy Join Behavior.....	529
Select Action.....	531
Configure Policy Enforcement.....	532
Import Data.....	533
Upload File.....	534
Evaluate Import File.....	534
Export Data.....	534
Create a Partial Export.....	535
Select Objects.....	536
Partial Export.....	536
Export All.....	537
Manage Access Types.....	537
Access Type Details.....	537
Manage Ownership Types.....	538
Create Ownership Type.....	538
View Requests.....	538
View Pending Requests by User.....	538
General.....	539
View All Requests by User.....	540
General.....	541
View Pending Requests by Service.....	542
General.....	542
View All Requests by Service.....	543
General.....	544
View All Requests.....	545
General.....	547
Activity Details.....	547
Request Details.....	547
Error and Warning Messages.....	549

View Personal Profile.....	549
User Details.....	550
Select a Service.....	551
Select a User.....	552
Activity Details.....	553
View Approval Details.....	553
Compliance Alert Details.....	554
Service Details.....	554
Activity Owners.....	555
Manage Activities.....	555
View Activities.....	555
View Activities by User.....	556
View Activities by User.....	557
Select a User.....	558
Request Details.....	558
Success.....	560
Approval Details.....	561
Grouped Approval Details.....	562
Complete a Grouped Approval.....	562
Provide Information for a Grouped RFI.....	563
RFI Details.....	564
Provide Information.....	564
Local Groups.....	573
Work Order Details.....	573
Complete a Grouped Work Order.....	574
Grouped Compliance Alerts.....	574
Compliance Alert Details.....	575
Compliance Correction.....	576
Defer Compliance Alert.....	576
Recertification Details.....	577
Complete a Grouped Recertification.....	577
Grouped User Recertification Activities.....	578
Preview Impact.....	579
Manage Delegation Schedules.....	579
Set Up Delegation.....	580
Select Login Account.....	581
Assign Activities.....	581
View Request Details.....	581
Select Delegate Account.....	582
Success.....	582
Message.....	583
About.....	583
Common Helps.....	583
Advanced Search.....	583
Miscellaneous Common Helps.....	593
Logon.....	600
Login.....	600
Forgot Your Password.....	600
Change Forgotten Password Information.....	601
Your Password Expired.....	601
Specify Forgotten Password Information.....	601
Specify New Password.....	602
Change Forgotten Passwords.....	602
Password.....	604
Password.....	604
About.....	604
Message.....	604
Page help does not display.....	605

Chapter 3. User administration.....	607
User management.....	607
Creating user profiles.....	608
Changing user profiles.....	609
Deleting user profiles.....	610
Transferring users.....	611
Suspending users.....	612
Restoring users.....	612
Recertifying users.....	613
Account management.....	614
Requesting an account for a user.....	615
Viewing accounts for a user.....	616
Viewing or changing account details.....	616
Deleting user accounts.....	617
Suspending user accounts.....	618
Restoring user accounts.....	619
Access management.....	620
Requesting access for users.....	620
Viewing access for users.....	621
Deleting user access.....	621
Password management.....	622
Changing user passwords.....	622
Resetting user passwords.....	623
Changing user passwords for sponsored accounts.....	624
Resetting user passwords for sponsored accounts.....	625
Delegating activities.....	626
Delegating activities for another user.....	626
Chapter 4. Login administration.....	629
Enabling password expiration.....	629
Setting a maximum number of login attempts.....	629
Chapter 5. Password administration.....	631
Enabling password resetting.....	631
Hiding generated reset passwords.....	632
Showing generated reset passwords.....	632
Enabling password editing and changing.....	633
Enabling password synchronization.....	634
Setting a password when a user is created.....	635
Setting a password retrieval expiration.....	635
Setting password notification.....	636
Creating password strength rules.....	637
Password strength rules.....	637
Enabling forgotten password authentication.....	640
Configuring user-defined forgotten password questions.....	641
Configuring administrator-defined forgotten password questions.....	641
Excluding specific passwords.....	642
Passwords for system users.....	643
Changing the itimuser user password.....	643
Changing the db2admin user password for Windows.....	644
Changing the ldapdb2 user password.....	644
Chapter 6. Organization administration.....	645
Administrator domains.....	645
Making a user a domain administrator.....	646
Creating a node in an organization tree.....	647

Changing a node in an organization tree.....	648
Deleting a node in an organization tree.....	648
Transferring a business unit.....	649
Business unit transfer activity completion might take a long time.....	650
Chapter 7. Security administration.....	651
View management.....	651
Creating a view.....	651
Changing a view.....	652
Deleting a view.....	652
Defining a custom task.....	653
Changing a custom task.....	655
Deleting a custom task.....	656
Access control item management.....	656
Default access control items.....	657
Creating an access control item.....	663
Changing an access control item.....	663
Deleting an access control item.....	664
Chapter 8. Role administration.....	667
Role overview.....	667
Role hierarchy change enforcement.....	668
Creating roles.....	668
Modifying roles.....	669
Values and formats for CSV access data.....	670
Exporting access data for a role.....	670
Importing access data for a role.....	671
Defining access by default for a role.....	673
Classifying roles.....	673
Specifying owners of a role.....	674
Displaying a role-based access in the user interface.....	675
Role assignment attributes.....	676
Defining assignment attributes when creating a role.....	677
Defining assignment attributes for an existing role.....	678
Setting assignment attribute values to the user members of a role.....	679
Configuring access catalog information for a role	680
Deleting roles.....	682
Managing users as members of a role.....	682
Adding users to membership of a role.....	683
Removing users from membership of a role.....	685
Managing child roles.....	686
Adding child roles to a parent role.....	687
Removing child roles from a parent role.....	688
Creating an access type based on a role.....	689
Transferring roles.....	689
Enabling access for multiple roles.....	690
Disabling access for multiple roles.....	691
Chapter 9. Services administration.....	693
Service types.....	693
Service status.....	695
Creating services.....	696
Creating a service that has manual connection mode.....	698
Enabling connection mode.....	700
Creating manual services.....	701
Changing services.....	703
Changing connection mode from manual to automatic.....	704

Changing a manual service.....	705
Values and formats for CSV access data.....	706
Exporting access data for a service.....	707
Importing access data for a service.....	708
Configuring access catalog information for a service.....	709
Deleting services.....	710
Management of reconciliation schedules.....	711
Maximum duration setting on reconciliation schedule.....	713
Reconciling accounts immediately on a service.....	714
Creating a reconciliation schedule.....	715
Changing a reconciliation schedule.....	716
Deleting a reconciliation schedule.....	717
Configuring a manual service type to support groups.....	718
Reconciling accounts immediately on a service.....	719
Example comma-separated value (CSV) file.....	720
Management of accounts on a service.....	721
Displaying accounts on a service.....	721
Requesting accounts on a service.....	722
Changing accounts on a service.....	724
Deleting accounts from a service.....	725
Suspending accounts on a service.....	726
Restoring accounts on a service.....	727
Assigning an account to a user.....	728
Orphan accounts.....	730
Management of account defaults on a service.....	731
Adding account defaults to a service.....	732
Changing account defaults for a service.....	733
Removing account defaults from a service.....	734
Using global account defaults for the service type.....	735
Service tagging.....	736
Adding the tag attribute to the service template.....	737
Adding tags to the service.....	737
Policy enforcement.....	737
Configuring policy enforcement behavior.....	740
Configuring compliance alert rules.....	742
Enforcing policies.....	743
Account recertification.....	744
Displaying account recertification status.....	744
Recertifying accounts on a service.....	745
Management of groups or access on a service.....	746
Clearing access.....	747
Enabling access for multiple services.....	749
Enabling access for multiple groups.....	749
Disabling access for multiple groups.....	750
Disabling access for multiple services.....	751
Chapter 10. Group administration.....	753
Creating groups.....	753
Viewing group membership.....	754
Adding members to groups.....	755
Removing members from groups.....	756
Modifying groups.....	758
Values and formats for CSV access data.....	759
Exporting access data for a group.....	760
Importing access data for a group.....	761
Deleting groups.....	762
Defining access on a group.....	763

Configuring access catalog information for a group.....	764
Recertifying access on a group.....	766
Enabling automatic group membership.....	767

Chapter 11. Report administration..... 769

IBM Cognos reporting framework.....	770
IBM Cognos reporting framework overview.....	770
Prerequisites for IBM Cognos report server.....	771
Installation of IBM Cognos reporting components.....	772
Configuration of IBM Cognos reporting components.....	773
Importing the report package.....	774
Creating a data source for IBM Security Identity Manager Cognos reports.....	775
Enabling the drill-through for PDF format.....	776
Security layer configuration around the data model and reports.....	776
Globalization overview.....	782
Report models.....	783
Report descriptions and parameters.....	785
Query subjects and query items for the report models.....	795
References for IBM Cognos report model items.....	860
Troubleshooting report problems.....	865
IBM Security Identity Manager console reports.....	868
Types of reports.....	868
Generating reports.....	870
Regular expression notation usage for searching.....	872
Report customization.....	872
Data synchronization.....	894
Data synchronization for reports.....	895
Incremental data synchronizer overview.....	898
Utility for external report data synchronization.....	899
Access control items (ACI) for reports.....	901
ACI object filters used for reporting.....	902

Chapter 12. Policy administration..... 903

Adoption policies.....	903
Creating an adoption policy.....	904
JavaScript examples for writing adoption policies.....	905
Changing an adoption policy.....	907
Deleting an adoption policy.....	907
Attribute matching.....	908
Account reconciliation and orphan accounts.....	908
Identity policies.....	908
Identities.....	909
Identity policy script example (advanced approach).....	910
Creating an identity policy.....	911
Changing an identity policy.....	912
Deleting an identity policy.....	913
Password policies.....	913
Creating a password policy.....	914
Adding targets to a password policy.....	915
Creating a password policy rule.....	915
Changing a password policy.....	916
Changing targets for a password policy.....	917
Changing a password policy rule.....	917
Deleting a password policy.....	918
Customized password rules.....	918
Provisioning policies.....	923
Policy enforcement.....	924

Provisioning policy parameter enforcement rules.....	924
Creating a provisioning policy.....	926
Changing a provisioning policy.....	926
Previewing a modified provisioning policy.....	927
Creating a draft of an existing provisioning policy.....	928
Committing a draft provisioning policy.....	929
Deleting a provisioning policy.....	929
Managing provisioning policies by role.....	929
Recertification policies.....	930
Recertification activities.....	933
Recertification message templates and schedule.....	933
Recertification policy results.....	935
Creating an account recertification policy.....	936
Creating an access recertification policy.....	937
Creating a user recertification policy.....	938
Changing a recertification policy.....	939
Deleting a recertification policy.....	940
Recertification default notifications.....	940
Separation of duty policies.....	942
ACI operations for the separation of duty policy protection category.....	943
Default ACIs for the separation of duty policy.....	943
Separation of duty approval workflow operation.....	944
Separation of duty policy violations and exemptions.....	945
Enabling the Manage Separation of Duty Policies portfolio task.....	946
Creating separation of duty policies.....	947
Modifying separation of duty policies.....	948
Evaluating separation of duty policies.....	949
Deleting separation of duty policies.....	950
Viewing policy violations and exemptions.....	951
Approving policy violations.....	952
Revoking policy exemptions.....	953
Service selection policies.....	954
Creating a service selection policy.....	955
Changing a service selection policy.....	955
Deleting a service selection policy.....	956

Chapter 13. Workflow management..... 957

Adding an entitlement workflow.....	957
Changing an entitlement workflow.....	958
Deleting an entitlement workflow.....	958
Creating a mail activity template with the workflow designer.....	959
Workflow notification properties.....	960
Configuring the workflow escalation period.....	961
Configuring the work item reminder interval and reminder content.....	961
Enabling workflow notification.....	962
Disabling workflow notification.....	962
Changing a workflow notification template.....	963
Manually applying the email notification template changes for canceling a request.....	963
Sample workflows.....	964
Sample workflow: manager approval of accounts.....	964
Sample workflow: multiple approvals.....	965
Sample workflow: multiple approvals with loop processing.....	968
Sample workflow: RFI and subprocess.....	971
Sample workflow: approval loop.....	973
Sample workflow: mail activity.....	975
Sample workflow: sequential approval for user recertification with packaged approval node.....	976
Sample workflow: packaged approval combined with simple approval node.....	979

Sample workflow: access owner approval.....	983
Chapter 14. Activity administration.....	985
Viewing activities.....	985
Viewing activities for a user.....	986
Locking an activity.....	986
Unlocking an activity.....	986
Delegating activities.....	987
Creating a delegation schedule.....	987
Changing delegation schedules.....	987
Deleting delegation schedules.....	988
Assigning activities to another user.....	988
Requests and activities.....	988
Escalation.....	989
Activity types.....	991
Approval activities.....	991
Request for information activities.....	992
Work order activities.....	993
Compliance alert activities.....	994
Recertification activities.....	995
Chapter 15. Requests administration.....	997
Requests and activities.....	997
Request states.....	997
Viewing all requests.....	998
Viewing pending requests of users.....	999
Viewing all requests of users.....	1000
Viewing pending requests by service.....	1001
Viewing all requests by service.....	1001
Canceling pending requests.....	1002
Index.....	1005

Tables

1. Application monitoring actions.....	11
2. Application Interfaces action items.....	16
3. Advanced tuning operations.....	18
4. Security protocol operations.....	19
5. Security cipher suite operations.....	20
6. Advanced tuning parameters.....	21
7. Static route actions.....	22
8. Descriptions of the password attributes.....	328
9. Separation of duty policy definition report.....	489
10. Form designer applet menu and toolbar buttons.....	507
11. SubForm parameters.....	515
12. Descriptions of the password attributes.....	637
13. Default access control items.....	657
14. CSV fields and values.....	670
15. Part 1 of 2: Role access CSV file values, formats.....	670
16. Part 2 of 2: Role access CSV file values, formats.....	670
17. CSV fields and values.....	706
18. Part 1 of 2: Service access CSV file values, formats.....	706
19. Part 2 of 2: Service access CSV file values, formats.....	707
20. Default compliance alert settings.....	740
21. CSV fields and values.....	759
22. Part 1 of 2: Group access CSV file values, formats.....	759
23. Part 2 of 2: Group access CSV file values, formats.....	759

24. Product documentation installation roadmap for IBM Cognos report server.....	771
25. Installation and data synchronization process.....	772
26. Configure IBM Cognos reporting components.....	773
27. LDAP advanced mapping values.....	777
28. Recertification model namespaces.....	784
29. Accounts model namespaces.....	784
30. Provisioning model namespaces.....	784
31. Roles model namespaces.....	784
32. Separation of duty model namespaces.....	785
33. Access model namespaces.....	785
34. Reports and the namespaces.....	786
35. Subreports.....	786
36. Filters for access definition report.....	787
37. Filters for Account Status Report.....	787
38. Audit History subreports.....	788
39. Filters for access audit history report.....	788
40. Filters for account audit history report.....	789
41. Filters for Entitlements Report.....	790
42. Recertification Definition subreports.....	791
43. Filters for Recertification Definition Report.....	791
44. Filters for Separation of Duty Policy Definition Report.....	791
45. Filters for Separation of Duty Policy Violation Report.....	792
46. Filters for Services Report.....	792
47. User Access subreports.....	792
48. Filters for the User Access report - View by Access report type.....	793

49. Filters for the User Access report - View by User report type.....	793
50. Filters for User Recertification History Report.....	794
51. Query subjects in the Recertification Audit namespace for the recertification model.....	795
52. Query items in the Recertification Audit namespace.....	796
53. Query subjects in the Recertification Config namespace.....	801
54. List of query items in the Recertification Config namespace.....	803
55. Query subjects in the Account Audit namespace.....	807
56. Query items in the Account Audit namespace.....	808
57. Query subjects in the Account Configuration namespace.....	810
58. Query items in the Account Configuration namespace.....	812
59. Query subjects in the Provisioning Policy Audit namespace.....	819
60. Query items in the Provisioning Policy Audit namespace	820
61. Query subjects in the Provisioning Policy Config namespace.....	821
62. Query items in the Provisioning Policy Config namespace.....	822
63. Query subjects in the Role Audit namespace.....	824
64. List of query items in the Role Audit namespace.....	824
65. Query subjects in the Role Configuration namespace.....	826
66. List of query items in the Role Configuration namespace.....	827
67. Query subjects in the Separation of Duty Audit namespace.....	831
68. Query items in the Separation of Duty Audit namespace.....	832
69. Query subjects in the Separation of Duty Configuration namespace.....	836
70. Query items in the Separation of Duty Configuration namespace.....	837
71. Query subjects in the User Configuration namespace.....	838
72. List of query items in the User Configuration namespace.....	839
73. Query subjects in the Service Audit namespace.....	844

74. List of query items in the Service Audit namespace.....	845
75. Query subjects in the Access Audit(Deprecated) namespace.....	847
76. List of query items in the Access Audit(Deprecated) namespace.....	849
77. Query subjects in the Access Audit namespace.....	852
78. List of query items in the Access Audit namespace.....	853
79. Query subjects in the Access Configuration namespace.....	856
80. List of query items in the Access Configuration namespace.....	856
81. Mapping the attributes and entities.....	860
82. Basic tasks to configure report model.....	861
83. Entities and Attributes.....	877
84. Filter conditions.....	877
85. Entities and attributes.....	878
86. Filter conditions.....	879
87. Entities and attributes.....	880
88. Filter conditions.....	880
89. User input values.....	884
90. User input filters	886
91. Specifying the location of the Java runtime environment.....	900
92. System attribute enforcement rules.....	924
93. Recertification policies and access control items.....	931
94. Node properties: Sample workflow for manager approval.....	965
95. Node properties: Sample workflow for multiple approvals.....	966
96. Node properties: Sample workflow for multiple approvals with loop processing.....	968
97. Node properties: Sample workflow with an RFI and a subprocess.....	971
98. Node properties: Sample workflow with an approval loop.....	973

99. Node properties: sample workflow for packaged approvals.....	976
100. Link properties: sample workflow for packaged approvals.....	978
101. Sample workflow node properties: Simple approval for user recertification with packaged approval node.....	979
102. Link properties: Simple approval for user recertification.....	982
103. Relevant Data.....	983
104. Node properties: Sample workflow for access request.....	984
105. States of approval activities.....	991
106. Descriptions of the states of RFIs.....	992
107. Descriptions of the states of work order requests.....	993
108. Descriptions of the states of requests.....	997

Chapter 1. Virtual appliance management

For the virtual appliance, connect to the IBM® Security Identity Manager virtual appliance console to manage the virtual appliance settings.

Appliance Dashboard

The **Appliance Dashboard** provides important status information, statistics, and quick links to the administrative consoles.

Viewing the Disk Usage widget

You can view the disk space status and remaining disk life information with the **Disk Usage** widget on the **Appliance Dashboard**.

Procedure

1. On the **Appliance Dashboard**, locate the **Disk Usage** widget.
The disk usage statistics are displayed.

Disk Space Pie Chart

Information about used disk space and free disk space is visualized in the pie chart.

Used space

Displays how much space (in GB) is already used.

Note: Most of the disk space is typically used by log files and trace files. To minimize the disk footprint, set the virtual appliance to store log and trace files on a remote server. You can also clear unused log and trace files on a periodic basis.

Free space

Displays how much space (in GB) is available.

Total space

How much space in total (in GB) is available to the virtual appliance.

Note: The disk space in a hardware appliance is limited by the capacity of the hard disk drive it holds.

2. Optional: Click **Refresh** to display the recently updated data.

Viewing the Partition Information widget

You can view information about the active and backup partitions with the **Partition Information** widget on the **Appliance Dashboard**.

Procedure

1. On the **Appliance Dashboard**, locate the **Partition Information** widget. Details about the active and backup partition are displayed.

Firmware version

Displays the version information about the virtual appliance firmware. For example, 7.0.

Installation date

Displays the date on which the virtual appliance firmware was installed. For example, Dec 01, 2014 8:15:51 PM.

Installation type

Displays the type of the virtual appliance firmware installation. For example, ISO.

Last boot

Displays the time when the virtual appliance was last booted. For example, Dec 01, 2014 8:19:40 PM.

2. Click **Firmware Settings** to go the page to modify settings of the firmware.
See [“Managing the firmware settings”](#) on page 6.

Viewing IP addresses

You can view a categorized list of IP addresses that the virtual appliance is listening on with the **Interfaces** widget.

Procedure

1. On the **Appliance Dashboard**, locate the **Interfaces** widget.
The **Interfaces** widget displays a categorized list of IP addresses in a table with the following columns:
 - **Type**
 - **Name**
 - **Address**
2. Optional: Click **Refresh** to display the recently updated data.

Viewing the Notifications widget

You can view warning information about potential problems and required actions on the **Notifications** widget on the **Appliance Dashboard**.

About this task

The **Notifications** widget refreshes automatically after every two minutes to display the most recent state or condition of the IBM Security Identity Manager virtual appliance.

Procedure

1. On the **Appliance Dashboard**, locate the **Notifications** widget. Warning messages about potential problems and expected actions can be displayed as follows:

```
Security Identity Manager server restart required
Appliance restart required
Middleware components not configured
The disk space utilization has exceeded the warning threshold.
```

2. Take appropriate actions as necessary.
For example:

If the following warning message is displayed, restart the IBM Security Identity Manager Server by using the option in the **Server Control** widget.

```
Security Identity Manager server restart required
```

If a message for restarting the **Appliance Dashboard** is displayed, restart the virtual machine from the vSphere console. This condition occurs only if you did not restart after your first configuration.

3. Optional: Click **Refresh** to display the most recent state or condition of the IBM Security Identity Manager virtual appliance.

Viewing the Quick Links widget

You can view the quick links for accessing the administration console application. This option is mainly for a virtual appliance administrator to validate the success of the IBM Security Identity Manager configuration.

Procedure

1. On the **Appliance Dashboard**, locate the **Quick Links** widget.
2. Click a quick link to work with the application that is based on your requirement.
For example, click **Identity Service Center**.

Note: The default user ID is `itim_manager` and password is `secret`.

Viewing the Server Control widget

You can view the status and control different servers in the **Appliance Dashboard** by using the **Server Control** widget.

About this task

Procedure

1. On the **Appliance Dashboard**, locate the **Server Control** widget.
The **Server name** column displays a list of all the servers. For example:
 - IBM Security Identity Manager server
 - IBM Security Directory Integrator server
 - Cluster Manager server
2. Select a server from the list.
3. Do one of the following actions:

Start

Click **Start** to start the selected server.

Stop

Click **Stop** to stop the selected server.

Restart

Click **Restart** to restart the selected server.

The **Server status** column displays the status of each server as follows:

Started

Indicates that the server is started.

Stopped

Indicates that the server is stopped.

4. Optional: Click **Refresh** to display the recently updated data.

Viewing the Middleware Monitor widget

The health status of a server is determined by the state of the middleware and services. You can view the health status information with the **Middleware Monitor** dashboard widget.

Procedure

1. On the **Appliance Dashboard**, locate the **Middleware Monitor** widget.
The widget displays the various middleware servers. For example:
 - Identity data store
 - Directory Server status

The **Middleware status** displays the status of a server as follows:

Started

Indicates that the server is started.

Stopped

Indicates that the server is stopped.

Not configured

Indicates that the server is not configured.

2. Optional: Click **Refresh** to display the recently updated data.

Viewing the Cluster Status widget

You can view a list of all the nodes in the cluster on the **Cluster Status** widget of the **Appliance Dashboard**.

About this task

You can view the **Cluster Status** widget only on a cluster node of the IBM Security Identity Manager virtual appliance.

The **Cluster Status** widget is displayed only when you are in a cluster setup. In stand-alone environment, the widget is not displayed.

Procedure

1. On the **Appliance Dashboard**, locate the **Cluster Status** widget.

If the **Cluster Status** widget is not displayed on the **Appliance Dashboard**, select **Dashboard > Cluster Status** and click **Save**.

The **Cluster Status** widget displays the following table columns:

Host Name

Displays the host name of a node in the cluster. Click the host name of a node to open the **Appliance Dashboard** in a separate web browser. A node with no link indicates that it is the same node that you are working from.

Role

Displays the role of the node in the cluster.

Primary

Indicates that the node is Primary.

Member

Indicates that the node is Member.

Status

Displays the status of the node in the cluster.

Available

It indicates that the node is available for your business requirement.

Not Available

It indicates that the node is not available for your business requirement.

Note: If the status of a node is displayed as Not Available, you can still click the host name link to start the **Appliance Dashboard**.

Undetermined

It indicates that the status of the node cannot be determined.

Note:

Diagnose the status of the node by verifying the following prerequisites. If all of the following conditions are met, the **Available** status is displayed.

- The database and LDAP server must be started. The IBM Security Identity Manager application must be able to establish the connection successfully.
- The IBM Tivoli® Directory Integrator server process must be running.
- The CPU usage must be less than 90%.

To check CPU usage, see [“Managing the CPU usage” on page 9](#).

- The system memory (RAM) usage must be less than 80%.

To check memory usage, see [“Managing the memory usage” on page 8](#).

If not, the **Not Available** status is displayed.

If an exception occurs while connecting or fetching data from the host, the status is **Undetermined**. For more information about the exception, see [Managing the log configuration](#).

Synchronization State

Displays the synchronization state for the node.

Not Connected

Displays when a member node cannot connect to a primary node or when a primary node cannot connect to the member node.

Not Synchronized

Displays when the member node is not synchronized with the primary node.

Synchronized

Displays when the member node is synchronized with the primary node.

Synchronizing

Displays when the member node is synchronizing with the primary node.

Not Applicable

Displays if the cluster node is a primary node because the primary node does not require any synchronization.

Note: If an error occurs, an error icon is displayed. Check the logs for more information. See [Managing the log configuration](#).

2. Optional: Click the **Refresh** icon to display the recently updated data.

Manage system settings for the virtual appliance

For your virtual appliance, you can work with system settings such as the log management and configuration, licensing, update history, firmware settings, fix packs, snapshots, support files, and other settings.

To manage the configured virtual appliance, log on to the **Appliance Dashboard** at https://isimva_hostname. For example: <https://isimva1.jk.example.com>.

Managing the update history information

View the update history to see a which firmware and security content updates are downloaded, installed, or rolled back on the IBM Security Identity Manager virtual appliance.

About this task

After you install an update, the update package is deleted from the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > Updates and Licensing > Update History**.

The **Update History** page is displayed.

The update history information is displayed in a table with the following columns:

- **Name**
- **Action Taken**
- **Status**
- **Version**
- **Release Date**

2. Optional: Click **Refresh** to display the recently updated data.

Managing the licensing information

View the service agreement that you accepted when you installed the IBM Security Identity Manager virtual appliance. You can also add a license module to manage the licensing and performance.

About this task

A service agreement defines the agreement and formal commitments about the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > Updates and Licensing > Licensing**.
The **Licensing and Performance** page is displayed.
2. Click **View Service Agreement** to view the service agreement.
3. Optional: Click **Select license** to add a license.
Browse to the location to search and select the license module.

Managing the firmware settings

The IBM Security Identity Manager virtual appliance has two partitions with separate firmware on each partition. Partitions are swapped during firmware updates so that you can roll back the firmware updates.

About this task

Either partition can be active on the virtual appliance. In the factory-installed state, partition 1 is active and contains the firmware version of the currently released product. When you apply a firmware update, the update is installed on partition 2, and your policies and settings are copied from partition 1 to partition 2. The virtual appliance restarts the system by using partition 2, which is now the active partition.

Note: The virtual appliance comes with identical firmware versions installed on both of the partitions so that you have a backup of the initial firmware configuration.

Tip: Avoid swapping partitions to restore configuration and policy settings. Use snapshots to back up and restore configuration and policy settings.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > Updates and Licensing > Firmware Settings**.
2. On the **Firmware Settings** page, do one or more of the following actions.

Option	Description
Edit	Select the partition and click Edit to revise the partition comment.

Option	Description
Create Backup	<p>Important: Create a backup of your firmware only when you are installing a fix pack from IBM Customer Support.</p> <p>Fix packs are installed on the active partition, and you might not be able to uninstall the fix pack.</p> <p>Note: The backup process can take several minutes to complete.</p>
Set Active	<p>Set a partition to active when you want to use the firmware that is installed on that partition. For example, you might want to set a partition to active to use firmware that does not contain a recently applied update or fix pack.</p>

3. Click **Yes**. If you set a partition to active, the virtual appliance restarts the system from the newly activated partition.

Installing a fix pack

Install a fix pack on the virtual appliance to address software maintenance updates for reliability and performance enhancements.

Before you begin

Restriction: You cannot uninstall a fix pack by using the local management interface. You must use the command-line interface to uninstall a fix pack.

Fix packs are applied to your active partition. You can manually create a backup of your active partition before you apply a fix pack so that you can roll back your changes.

About this task

If a fix pack is installed on your virtual appliance, you can view information about who installed the fix pack, comments, patch size, and the installation date.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > Updates and Licensing > Fix Packs**.
2. On the **Fix Packs** page, click **New**.
3. In the **Add Fix Pack** window, click **Browse for fix pack**.
The **Browse for fix pack** table displays the fix pack details.
4. Click **Save Configuration** to install the fix pack.

Managing the About page information

View the **About** page to learn or manage about the IBM Security Identity Manager virtual appliance and its content.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > Maintenance > About**.
2. View the product-specific information for the virtual appliance.

Results

The following information is displayed in the **About** page:

```
Product Name: IBM Security Identity Manager
Product Version: 7.0.1
Server Name: isimva1.in.ibm.com
Installed Fix Packs: None
```

Build number: 20151111-1328
Build Date and Time: Nov 11, 2015 1:32:57 AM

Product Name

Displays the name of product that you are using.

Product Version

Displays the version of product that you are using.

Server Name

Displays the server name.

Installed Fix Packs

Displays the last fix pack level that was installed for the version of the product that you are using.

Build number

Displays the current build number for the version of the product that you are using.

Build Date and Time

Displays the date and the exact time and the time zone on which the last build occurred.

What to do next

Read the IBM Security Identity Manager virtual appliance product information to determine how it can be useful in your work.

Managing the memory usage

View the memory graph to see the memory that is used by the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor > Monitoring > Memory**.
The **System Memory Statistics** page is displayed.
2. Select a **Date Range**.

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last 3 days. Each data point is an average of the activity that occurred in that hour.
7 Days	Displays data points every 20 minutes during the last 7 days. Each data point is an average of the activity that occurred in that hour.
30 Days	Displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.

3. In the legend area, select **Memory Used** to review the total used memory.

The **Details** section displays these statistics:

Total

Indicates the total system memory.

Used

Indicates the system memory that is used.

Free

Indicates the system memory that is available.

As of

Indicates the current date, time, and the UTC identifier.

Managing the CPU usage

View the CPU graph to see the CPU that is used by the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor > Monitoring > CPU**.
The **System CPU Statistics** page is displayed.
2. Select a **Date Range**.

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last 3 days. Each data point is an average of the activity that occurred in that hour.
7 Days	Displays data points every 20 minutes during the last 7 days. Each data point is an average of the activity that occurred in that hour.
30 Days	Displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.

3. In the legend area, select the following options to review the CPU data.

The **Details** section displays these statistics:

User CPU

Indicates the CPU use by the user.

System CPU

Indicates the CPU use by the system.

Idle CPU

Indicates the idle use of the CPU.

As of

Indicates the current date, time, and the UTC identifier.

Managing the storage usage

View the storage graph to see the percentage of disk space that is used by the boot and root partitions of the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor > Monitoring > Storage**.
The **Storage Statistics** page is displayed.
2. Select a **Date Range**.

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last 3 days. Each data point is an average of the activity that occurred in that hour.
7 Days	Displays data points every 20 minutes during the last 7 days. Each data point is an average of the activity that occurred in that hour.
30 Days	Displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.

3. In the Legend area, select which partitions that you want to review.

The **Details** section displays these statistics:

Boot

Indicates the boot partition. It displays the size, used, and available storage information in MB.

Root

Indicates the base file system, where the system user is root. It displays the size, used, and available storage information in MB.

Monitoring the IBM Security Identity Manager Server

Configure the IBM Security Identity Manager Server monitoring with IBM Tivoli Monitoring to collect performance metrics and service statistics from the IBM Security Identity Manager over a time.

Before you begin

Make sure that IBM Tivoli Monitoring Version 6.2.3 is installed before you work with the IBM Security Identity Manager Server monitoring.

Make sure that the Universal Agent is installed with the product. It might be installed on a separate computer.

For more information, see http://www.ibm.com/support/knowledgecenter/SSTFXA_6.2.3.1/com.ibm.itm.doc_6.2.3fp1/itm623FP1_install118.htm%23installation.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Monitor > Monitoring > Application**.
2. On the **IBM Security Identity Manager Server Monitoring** page, do one of these actions.

Table 1. Application monitoring actions

<p>Configure the IBM Security Identity Manager Server monitoring</p>	<p>a. Click Configure.</p> <p>b. On the Confirm action window, click Yes.</p> <p>c. On the IBM Security Identity Manager server monitoring configuration window, provide these details.</p> <p>Identity Manager administrator ID The ID for the Security Identity Manager administrator. For example, <code>itim manager</code>.</p> <p>Identity Manager administrator password The password for the Security Identity Manager administrator. For example, <code>secret</code>.</p> <p>Universal Agent host name The host name of the Universal Agent. For example, specify <code>isimhost.mycompany.com</code>.</p> <p>Universal Agent port The port of the Universal Agent. For example, <code>7500</code>.</p> <p>Monitoring interval The time interval between 2 performance updates of the IBM Security Identity Manager Server. For example, <code>120</code> seconds.</p> <p>Monitoring metrics Select the items that you want to monitor for the IBM Security Identity Manager Server.</p> <p>Select all Select this option to monitor all the metrics for the IBM Security Identity Manager Server.</p> <p>Service summary Select this option to monitor the service summary. This metric contains cumulative information about all the IBM Security Identity Manager services. It includes statistics such as the number of services that failed and recovered. It also contains useful information such as the number of active processed requests, and number of threads that did not process.</p> <p>Service details Select this option to monitor the service details. This metric contains information about individual IBM Security Identity Manager services. It includes similar information as the service summary for each individual service instance.</p> <p>Service failures Select this option to monitor the service failures. This metric contains information about individual services that did not succeed. It includes this information:</p> <ul style="list-style-type: none"> • The service name that did not succeed. • The number of requests that are blocked. • The date and time the service first did not succeed. • The error message that describes the failure. <p>Workflow requests Select this option to monitor workflow requests. This metric contains information about requests that are processed by the IBM Security Identity Manager workflow. It contains statistics such as the number of processes that started and finished.</p> <p>JMS queues Select this option to monitor the JMS queues. This metric contains the sizes of the IBM Security Identity Manager JMS queues. These queues are an indication of the current workload.</p> <p>Process statistics Select this option to monitor the process statistics. This metric contains statistics about the Java™ process that runs IBM Security Identity Manager, such as CPU usage, memory consumption, thread count, and garbage collection. The thread count and garbage collection statistics are not enabled by default in WebSphere® Application Server. To see these statistics, enable the Java virtual computer profiler data. For more information, see http://www.ibm.com/support/knowledgecenter/SSAW57_7.0.0/com.ibm.websphere.nd.doc/info/ae/ae/tprf_jvmpidata.html.</p> <p>d. Click Save Configuration.</p> <p>e. Restart the cluster manager server if the Notifications widget indicates you to do it.</p> <p>A record is created for the IBM Security Identity Manager Server monitoring.</p>
<p>Enable the IBM Security Identity Manager Server monitoring</p>	<p>a. Select the record that you configured for the IBM Security Identity Manager Server monitoring.</p> <p>b. Click Enable.</p> <p>c. On the Confirm action window, click Yes.</p> <p>d. Restart the cluster manager server if the Notifications widget indicates you to do it.</p>
<p>Disable the IBM Security Identity Manager Server monitoring</p>	<p>a. Select the record that you configured for the IBM Security Identity Manager Server monitoring.</p> <p>b. Click Disable.</p> <p>c. Restart the cluster manager server if the Notifications widget indicates you to do it.</p>

Table 1. Application monitoring actions (continued)

<p>Reconfigure the IBM Security Identity Manager Server monitoring</p>	<p>a. Click Reconfigure.</p> <p>b. On the Edit IBM Security Identity Manager server monitoring configuration window, provide these details.</p> <p>Identity Manager administrator ID The ID for the Security Identity Manager administrator. For example, <code>itim.manager</code>.</p> <p>Identity Manager administrator password The password for the Security Identity Manager administrator. For example, <code>secret</code>.</p> <p>Universal Agent host name The host name of the Universal Agent. For example, specify <code>isimhost1.mycompany.com</code>.</p> <p>Universal Agent port The port of the Universal Agent. For example, <code>7500</code>.</p> <p>Monitoring interval The time interval between 2 performance updates of the IBM Security Identity Manager Server. For example, <code>180</code> seconds.</p> <p>Monitoring metrics Select the items that you want to monitor for the IBM Security Identity Manager Server.</p> <p>Select all Select this option to monitor all the metrics for the IBM Security Identity Manager Server.</p> <p>Service summary Select this option to monitor the service summary. This metric contains cumulative information about all the IBM Security Identity Manager services. It includes statistics such as the number of services that failed and recovered. It also contains useful information such as the number of active processed requests, and number of threads that did not process.</p> <p>Service details Select this option to monitor the service details. This metric contains information about individual IBM Security Identity Manager services. It includes similar information as the service summary for each individual service instance.</p> <p>Service failures Select this option to monitor the service failures. This metric contains information about individual services that did not succeed. It includes this information:</p> <ul style="list-style-type: none"> • The service name that did not succeed. • The number of requests that are blocked. • The date and time the service first did not succeed. • The error message that describes the failure. <p>Workflow requests Select this option to monitor workflow requests. This metric contains information about requests that are processed by the IBM Security Identity Manager workflow. It contains statistics such as the number of processes that started and finished.</p> <p>JMS queues Select this option to monitor the JMS queues. This metric contains the sizes of the IBM Security Identity Manager JMS queues. These queues are an indication of the current workload.</p> <p>Process statistics Select this option to monitor the process statistics. This metric contains statistics about the Java process that runs IBM Security Identity Manager, such as CPU usage, memory consumption, thread count, and garbage collection. The thread count and garbage collection statistics are not enabled by default in WebSphere Application Server. To see these statistics, enable the Java virtual computer profiler data. For more information, see http://www.ibm.com/support/knowledgecenter/SSAW57_7.0.0/com.ibm.websphere.nd.doc/info/ae/ae/tprf_jvmpidata.html.</p> <p>c. Click Save Configuration.</p>
<p>Export the IBM Security Identity Manager Server monitoring</p>	<p>a. Select the record that you configured for the IBM Security Identity Manager Server monitoring.</p> <p>b. Click Export to save the file on your local computer.</p> <p>c. Import the <code>isim.md1</code> file into IBM Tivoli Monitoring Universal Agent to define the syntax of the metrics that the monitor sends to the Universal Agent.</p> <p>d. Transfer this file to the computer where IBM Tivoli Monitoring is running.</p> <p>e. On the IBM Tivoli Monitoring computer, copy the <code>isim.md1</code> file into the directory that contains the Universal Agent meta files. For example: <code>C:\IBM\ITM\TMAITM6\metafiles</code>.</p> <p>f. Ensure that the IBM Tivoli Monitoring Server and the IBM Tivoli Monitoring Universal Agent are running.</p> <p>g. Import the metafile by using one of the following examples:</p> <ul style="list-style-type: none"> • Example 1: <ol style="list-style-type: none"> 1) Open a command editor. 2) Type the <code>C:\IBM\ITM\bin\um_console -h ITM_HOME</code> command to go to the Universal Agent prompt. 3) Type the <code>import C:\IBM\ITM\TMAITM6\metafiles\isim.md1</code> command. • Example 2: <ol style="list-style-type: none"> 1) Open a command editor. 2) Type the <code>C:\IBM\ITM\TMAITM6> kumpcon import isim.md1</code> command.

Viewing the event log

System events are logged when the system settings are changed or when problems occur with the IBM Security Identity Manager virtual appliance. Use the **Event Log** page to view and to export system events on your network.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor > Logs > Event Log**.

The **Event Log** page displays system events in the **System Events** tab.

2. From the **System Events** tab, do one of the following actions.

- Click **Pause Live Streaming** to stop the live updating of the event log.
- Click **Start Live Streaming** to resume live updating of the event log.
- Filter the system events with the following steps:

- a. Click **Filter** to display the **Filter** window.

- b. From the **Column** list, select a column name to filter on it. The column names are as follows:

- **Any Column**
- **Priority**
- **Event ID**
- **Event Description**
- **Time Occurred**

Note: The virtual appliance does not return results for the **Time Occurred** column when you select **Any Column**. Select the **Time Occurred** column to filter values in that column.

- c. From the **Condition** list, select a filter condition. Available filter conditions vary depending on the tab that you selected in the event log. The possible filtering conditions include these options:

- **contains**
- **is**
- **starts with**
- **ends with**
- **before**
- **after**
- **range**

Note: You can also add a rule for filtering the system events.

- d. In the **Value** field, specify a filter value.

- e. Click **Filter**.

- f. Click **Clear** to clear all the filter changes.

- Click **Export** to download the displayed event log data to a CSV file.

Note: The default file name is `export.csv`.

- a. In the exported event log file, the **Time Occurred** column shows the time since Epoch (1 January 1970, 00:00:00 Universal time).

- b. When you use the table filter on the **Priority** field, the values that can be filtered are in English only (low, medium, and high) on all language versions of the virtual appliance.

Managing the SNMP monitoring

You can monitor the current virtual appliance status with SNMP. This status shows an SNMP agent, which can be queried by any SNMP manager or monitoring tools that support SNMP to obtain the status of the running virtual appliance.

About this task

When configured, the SNMP agent listens on all management interfaces.

The SNMP Monitoring function can monitor the virtual appliance in an IBM Tivoli Monitoring environment. Use the Agentless Monitoring for Linux® OS agent to monitor a virtual appliance.

For more information about configuring the IBM Tivoli Monitoring environment and the Agentless Monitoring for Linux OS agent, see the [IBM Tivoli Monitoring Knowledge Center](#).

The following management information bases, or MIBs, are used by the SNMP agent:

SNMPv2-MIB	TCP-MIB
SNMPv2-SMI	UDP-MIB
SNMP-FRAMEWORK-MIB	HOST-RESOURCES-MIB
SNMP-MPD-MIB	MTA-MIB
SNMP-TARGET-MIB	DISMAN-EVENT-MIB
SNMP-USER-BASED-SM-MIB	NOTIFICATION-LOG-MIB
SNMP-VIEW-BASED-ACM-MIB	UCD-SNMP-MIB
IF-MIB	UCD-DLMOD-MIB
IP-MIB	UCD-DISKIO-MIB
IPV6-MIB	UCD-SNMP-MIB
IP-FORWARD-MIB	NET-SNMP-AGENT-MIB
NET-SNMP-VACM-MIB	

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor > Monitoring > SNMP Monitoring**.
2. On the **SNMP Monitoring** page, click **Configure**.
3. In the **Configure SNMP** window, select the **SNMP Protocol** version that the agent must use. The choices are as follows.

- **Disabled**
- **SNMPv1/SNMPv2c**
- **SNMPv3**

4. In the **Port** field, type the number that the SNMP agent must listen on. Alternatively, you can also change the port number with the range controller next to it.

Note: The default port number is 161.

5. Select one of the following SNMP protocols.

SNMPv1/SNMPv2c

In the **Community** field, type the name of the community that the SNMP manager uses to authenticate with the SNMP agent.

SNMPv3

Configure the following options to describe the user that accesses the SNMP agent.

Option	Description
Security Level	The security level of the user.
Security User	Type the name of the user that accesses the SNMP agent.
Auth Protocol	From the Auth Protocol list, select the authentication protocol to use.
Auth Password	Type the password to use for authentication. The password must be a minimum 8 characters in length.
Auth Password (Confirm)	Retype the authentication password to confirm.
Privacy Protocol	From the Privacy Protocol list, select the privacy protocol to use.
Privacy Password	Type the password to be used as a privacy passphrase. The password must be a minimum of 8 characters in length.
Privacy Password (Confirm)	Retype the privacy password to confirm.

6. Click **Save Configuration**.
7. Optional: To reconfigure an existing SNMP Monitoring configuration, do these steps:
 - a) From the **SNMP Monitoring** table, select a record.
 - b) Click **Reconfigure**.
 - c) In the **Reconfigure SNMP** window, edit the details.
 - d) Click **Save Configuration**.
8. Optional: To unconfigure an existing SNMP Monitoring configuration, do these steps:
 - a) From the **SNMP Monitoring** table, select a record.
 - b) Click **Unconfigure**.
 - c) Click **Yes** to confirm the deletion.

Managing the application interfaces

To manage application interfaces, use the **Application Interfaces** page.

About this task

An IP address and its corresponding fully qualified domain name for any application interface must have a static IP address, which must be different from the local management interface address.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > Network Settings > Application Interfaces**.

The **Application Interfaces** page displays these tabs.

- **Interface 1**
- **Interface 2**
- **Interface 3**
- **Interface 4**

Each tab displays a table with these column names.

Type

Indicates whether the type is **IPv4** or **IPv6**.

Address

Indicates the address of the application interface. For example, 9.122.125.175.

Interface FQDN

Indicates the fully qualified domain name of the application interface. For example, `isim.example.com`.

Interface Gateway

Indicates the IP address of the application interface subnet gateway. For example, `9.122.126.1`.

Netmask/Prefix

Indicates the netmask or prefix of the application interface. For example, `255.255.255.0`.

A netmask is used for **IPv4**, and a prefix is used for **IPv6**.

2. On any tab of the **Application Interfaces** page, do one of these actions.

Action	Button	Description
Add an address	New	<p>Note:</p> <ul style="list-style-type: none">• You must add an address at least in Interface 1; adding addresses for other interfaces is not mandatory.• Make sure the IP address that you assign is not used by any other system. <p>Important: The application works only on Interface 1.</p> <ol style="list-style-type: none">a. Select the Interface 1 tab.b. Click New to display the Add Address window.c. Select one of the following options to indicate the type of address to add. IPv4 IPv4 defines each interface on a network uniquely. It is a 32-bit numeric address, which is written in decimal as four sets of digits that are separated by periods with no spaces or consecutive periods. Each number can be 0 - 255. For example, <code>192.0.2.12</code>. IPv6 IPv6 improves the efficiency of routing and provides greater security. It is a 128-bit IP address, which is written in hexadecimal and separated by colons. For example, <code>4ffe:1800:8484:3:220:f9ff:fe25:70cf</code>d. Specify the fully qualified domain name of the application interface in the Interface FQDN field.e. Specify the IP address for the subnet gateway of the application interface in the Interface Gateway field.f. Do one of these actions.<ul style="list-style-type: none">• For IPv4 Settings, do these steps.<ol style="list-style-type: none">1) Type an address value in the Address field.2) Type a net mask value in the NetMask field.• For the IPv6 settings, do these steps.<ol style="list-style-type: none">1) Type an address value in the Address field.2) From a range of 0-64, specify a prefix value in the Prefix field.g. Click Save.h. If any notifications are displayed in the Notifications widget, take appropriate actions as necessary. <p>A message indicates that the application address is added successfully, and the record is listed in the Interface 1 table.</p>

<i>Table 2. Application Interfaces action items (continued)</i>		
Action	Button	Description
Edit an address	Edit	<p>a. Select an application interface.</p> <p>b. Select the address.</p> <p>c. Click Edit to display the Edit Address window.</p> <p>d. Edit the fully qualified domain name of the application interface in the Interface FQDN field.</p> <p>e. Edit the IP address for the subnet gateway of the application interface in the Interface Gateway field.</p> <p>f. Do one of these actions.</p> <ul style="list-style-type: none"> • For IPv4 Settings, do these steps. <ol style="list-style-type: none"> 1) Edit address value in the Address field. 2) Edit net mask value in the NetMask field. • For IPv6 Settings, do these steps. <ol style="list-style-type: none"> 1) Edit address value in the Address field. 2) Edit prefix value in the Prefix field. <p>g. Click Save.</p> <p>A message indicates that the address is updated successfully.</p>
Delete an address	Delete	<p>a. Select an application interface.</p> <p>b. Select the address.</p> <p>c. Click Delete to display the Confirm Action window.</p> <p>d. Click Yes.</p> <p>A message indicates that the address is deleted successfully.</p>
Test a connection	Test	<p>a. Click Test to display the Ping Server window.</p> <p>b. In the Server field, enter the IP address or name of the server to test the connection with.</p> <p>c. Click Test.</p> <p>A message indicates whether the test connection was successful or not.</p>
Refresh the application interface data	Refresh	Click Refresh to display the most recent version of the data, including changes that were made to the data since it was last refreshed.

3. Click **Save**.

Managing advanced tuning settings

You can set tuning parameters that are used with the virtual appliance.

About this task

Note: Change these advanced tuning parameter values only under the supervision of IBM® software support.

For information about advanced tuning parameters, see [Advanced tuning parameters](#).

Procedure

1. Click **Manage System Settings > Advanced Tuning Parameters**.
2. Perform any of the following actions.

<i>Table 3. Advanced tuning operations</i>	
Button	Procedure
New	<ol style="list-style-type: none"> Click New. A dialog opens. Type the name for the key. Type a value for the key. Multiple values can be specified as a space-separated list. Type a comment that describes the key that you created. Click Save Configuration.
Edit	<ol style="list-style-type: none"> Select a key. Click Edit. A dialog opens. Modify then name for the key. Modify the value for the key. Multiple values can be specified as a space-separated list. Modify the comment that describes the key. Click Save Configuration.
Delete	<ol style="list-style-type: none"> Select one or more keys. If you want to delete all the keys, select the Key check box. Click Delete. A confirmation message is displayed. Click Yes to delete the key or No to cancel the operation.

Configuring Open VM Tools support

Configure Open VM Tools support for more seamless virtual appliance monitoring, administration, and management experience with VMware products.

About this task

You must enable Open VM Tools support in the local management interface before you can use the feature. If you enable Open VM Tools support, you enable the following features in VMware products:

- Shut down and restart the virtual appliance gracefully from the hypervisor console.
- Synchronized clocks between the virtual appliance and the VMware ESXi server.
- Support for VMware statistics with the **vmware support** command.

Procedure

1. Go to **Manage > System Settings > Advanced Tuning Parameters**.
2. Perform one of the following tasks:

If you want to	Do
Enable Open VM Tools support	Set vmtoolsd.enabled to true .
Disable Open VM Tools support	Set vmtoolsd.enabled to false .

Note: For more information about other tuning parameters for Open VM Tools, see [“Advanced tuning parameters for the virtual appliance”](#) on page 20.

3. Reload the page.
4. Apply the changes to the system.

Managing local management interface security protocols for the virtual appliance

You can set the security protocols that are used with the virtual appliance.

About this task

Note: Change these advanced tuning parameter values only under the supervision of IBM® software support.

Procedure

1. Click **Manage System Settings > Advanced Tuning Parameters**.
2. Perform any of the following actions.

Button	Procedure
New	<ol style="list-style-type: none">a. Click New. A dialog opens.b. Type the name for the key such as <code>lmi.security.protocol</code>.c. Type a value for the key. Multiple values can be specified as a space-separated list. Valid values are TLS TLSv1.1 TLSv1.2d. Type a comment that describes the protocol that you created.e. Click Save Configuration.
Edit	<ol style="list-style-type: none">a. Select a protocol key.b. Click Edit. A dialog opens.c. Modify then name for the key.d. Modify the value for the key. Multiple values can be specified as a space-separated list. Valid values are TLS TLSv1.1 TLSv1.2e. Modify the comment that describes the key.f. Click Save Configuration.
Delete	<ol style="list-style-type: none">a. Select one or more keys. If you want to delete all the keys, select the Key check box.b. Click Delete. A confirmation message is displayed.c. Click Yes to delete the key or No to cancel the operation.

Managing local management interface security cipher suites for the virtual appliance

You can set the security cipher suites that are used with the virtual appliance.

About this task

Note: Change these advanced tuning parameter values only under the supervision of IBM software support.

For information about advanced tuning parameters, see [“Advanced tuning parameters for the virtual appliance”](#) on page 20.

Procedure

1. Click **Manage System Settings > Advanced Tuning Parameters**.
2. Perform any of the following actions.

Button	Procedure
New	<ol style="list-style-type: none">a. Click New. A dialog opens.b. Type the name for the key such as <code>lmi.security.ciphers</code>.c. Type a value for the key. Multiple values can be specified as a space-separated list. The virtual appliance supports all the cipher suites that are supported by Java 7. For a list of cipher suites that the virtual appliance supports, see https://www.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/ciphersuites.html.d. Type a comment that describes the cipher key that you created.e. Click Save Configuration.
Edit	<ol style="list-style-type: none">a. Select a cipher key.b. Click Edit. A dialog opens.c. Modify then name for the key.d. Modify the value for the key. Multiple values can be specified as a space-separated list. The virtual appliance supports all the cipher suites that are supported by Java 7. For a list of cipher suites that the virtual appliance supports, see https://www.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/ciphersuites.html.e. Modify the comment that describes the key.f. Click Save Configuration.
Delete	<ol style="list-style-type: none">a. Select one or more keys. If you want to delete all the keys, select the Key check box.b. Click Delete. A confirmation message is displayed.c. Click Yes to delete the key or No to cancel the operation.

Advanced tuning parameters for the virtual appliance

Change the advanced tuning parameter values only under the supervision of IBM software support.

Local management interface (LMI)

The following table lists the advanced tuning parameters that are available.

Table 6. Advanced tuning parameters

Parameter	Description
lmi.security.ciphers	Enables specific ciphers for the local management interface. Valid values are specified as a space-separated list. The virtual appliance supports all the cipher suites that are supported by Java 7. See https://www.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/ciphersuites.html for a list of the supported cipher suites.
lmi.security.protocol	Enables specific protocols for the local management interface. Valid values are TLS , TLSv1 , and TLSv1.2 .
lmi.customfiles.accepted.filetypes	Specifies the accepted file extensions for files that you can upload from the Custom File Management page. Valid values are ALL or a space-separated list of valid file extensions.
lmi.sslcert.accepted.filetypes	Specifies the accepted file extensions for files that you can upload from the SSL Certificate Management page. Valid values are ALL or a space-separated list of valid file extensions.
vmtoolsd.enabled	Enables the use of Open VM Tools. To enable, set to true . To disable, set to false . By default, Open VM Tools is disabled. With Open VM Tools enabled, you can use the following services. <ul style="list-style-type: none"> • Shutdown and restart the virtual appliance gracefully from the hypervisor console. • Synchronize clocks between the virtual appliance and the ESXi Server. • Use the vmware support command to retrieve VMware statistics.
vmtoolsd.timesync.enable	Enables clock synchronization between the virtual appliance and the ESXi server. To enable, set to true . Set to false to disable. If your network uses a Network Time Protocol (NTP) server, this parameter is automatically set to false .

Note: After you modify any parameter values, reload the page. You can review the undeployed changes, rollback, or apply the changes to the system.

Managing hosts file

To manage hosts file with the virtual appliance, use the **Manage Hosts File** page.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage System Settings > Network Settings > Hosts File**.
All current host records with their IP addresses and host names are displayed.
2. On the **Manage Hosts File** page, work with host records or host names.

- Add a host record
 - a. Select the root level **Host Records** entry or do not select any entries.
 - b. Click **New**.
 - c. On the **Create Host record** page, do these actions.
 - Address**
Specify the IP address of the host record.
 - Host Name**
Specify the host name of the host record.
 - d. Click **Save**.
- Add a host name to a host record
 - a. Select a host record entry to add the host name to.
 - b. Click **New**.
 - c. On the **Add Hostname to Host Record** page, enter the host name.
 - d. Click **Save**.
- Remove a host record
 - a. Select a host record entry to delete.
 - b. Click **Delete**.
 - c. On the confirmation page, click **Yes** to confirm the deletion.
- Remove a host name from a host record
 - a. Select host name entry to delete.
 - b. Click **Delete**.
 - c. On the confirmation page, click **Yes** to confirm the deletion.
 - Note:** If the removed host name is the only associated host name for the IP address, then the entire host record (the IP address and host name) is removed.
- Refresh the data

Click **Refresh** to display the most recent version of the data since it was last refreshed.

Configuring static routes

Configure static routes to the paired protection interfaces on your virtual appliance to enable network routers to redirect users to block pages or authentication pages.

About this task

This task is only necessary for networks that contain an extra network segment between the user segment and the virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > Network Settings > Routes**.
2. On the **Static Routes** page, complete one of these steps.

<i>Table 7. Static route actions</i>	
Field	Action
IPv4 Default Gateway	a. Specify an address value. For example: 9.113.50.1. b. Click Save . Note: Click Reset to update the displayed value back to the current default gateway. It does not make any updates to the actual default gateway value.

Table 7. Static route actions (continued)	
Field	Action
IPv6 Default Gateway	<p>a. Specify an address value. For example: 3001:0DB9:0000:0000:02AB:00FF:FE29:9C6A.</p> <p>b. Click Save.</p> <p>Note: Click Reset to update the displayed value back to the current default gateway. It does not make any updates to the actual default gateway value.</p>
New	<p>a. Click New to create a route.</p> <p>b. In the Add Route window, define values in these fields.</p> <ul style="list-style-type: none"> • Destination • Gateway • Metric • Interface or Segment <p>c. Click Save Configuration.</p>
Edit	<p>a. Select an existing route.</p> <p>b. Click Edit to change the settings.</p> <p>c. In the Edit Route window, edit values in these fields.</p> <ul style="list-style-type: none"> • Destination • Gateway • Metric • Interface or Segment <p>d. Click Save Configuration.</p>
Delete	<p>a. Select an existing route.</p> <p>b. Click Delete.</p> <p>c. Click Yes to confirm your action.</p>

Results

The new and edited system routes are displayed in the **Currently active system routes** table.

Managing the date and time settings

Use the **Date/Time** page to configure the date, time, time zone, and NTP server information of the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > Date/Time**. The **Date/Time** page is displayed.
2. Configure the following options on the **Date/Time** page.

Option	Description
Date	Specifies the day, month, and year for the IBM Security Identity Manager virtual appliance.
Time	Specifies the time for the IBM Security Identity Manager virtual appliance.

Option	Description
Time Zone	Specifies the time zone for the IBM Security Identity Manager virtual appliance.
NTP Server address	Select Enable NTP to list the NTP (NIST Internet Time Service) servers that the IBM Security Identity Manager virtual appliance uses. You can enter multiple NTP servers, which are separated by commas.

Note: You cannot set the **Time Zone** or **Date/Time** by using the system console. You can specify only NTP server addresses.

3. Click **Save Configuration**.
4. Optional: Click **Reset** to set the configuration again or differently.

Managing the administrator settings

Use the administrator settings to change the password that you use to access your IBM Security Identity Manager virtual appliance. Use the settings to also access the length of idle time that is granted to pass before your session times out.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > Administrator Settings**.

The **Administrator Settings** page is displayed.

2. On the **Administrator Settings** page, type your current password in the **Current Password** field.
3. Type your new password in the **New Password** field.

Set a strong password. It must be at least 8 characters and contain one uppercase and one lowercase character, one numerical character, and one special character. You can try special characters such as !, @, #, or %. The special character cannot be any of the following symbols : <, >, `, &, \$, \, ", :, and |.

4. Type your new password in the **New Password Confirmation** field.
5. In the **Session Timeout** field, click the arrows to select the amount of time that you are allowed to be idle before you are automatically logged out.
6. Click **Save Configuration**.

Managing the snapshots

Use snapshots to restore prior configuration and policy settings to the IBM Security Identity Manager virtual appliance.

Before you begin

Ensure that these steps are done before you want to create or apply a snapshot from the **Snapshots** page.

1. From the **Server Control** widget on the **Appliance Dashboard** for the primary node, do these steps.
 - a. Select **Cluster Manager server**.
 - b. Click **Stop**.
2. From the **Server Control** widget on the **Appliance Dashboard** for the member node, do these steps.
 - a. Select **Security Identity Manager server**.
 - b. Click **Stop**.
 - c. Select **Security Directory Integrator server**.
 - d. Click **Stop**.

When you restore the primary node from the backup node, some user requests remain in pending state. For example, Request for Service Access. Therefore, when you restore a backup node as a primary node, do these steps.

1. Clear the **Service Integration Bus** tables from the database and commit the changes. For more information, see Step 3 in "Reconfiguring the data store connection".
2. Restart the database server that you are using, such as DB2® or Oracle.
3. Restart the primary node virtual appliance.
4. Restart the member node virtual appliance.

About this task

Snapshots are stored on the IBM Security Identity Manager virtual appliance. However, you can download the snapshots to an external drive in case of system failure.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > Snapshots**. The **Snapshots** page is displayed.
2. On the **Snapshots** page, do one or more of the following actions.

Option	Description
New	To create a snapshot, do these steps: <ol style="list-style-type: none"> a. Click New. b. On the Add Snapshot window, specify helpful comments in the Comments field, so that the snapshot is easy to identify in the virtual appliance. c. Click Save Configuration.
Edit	To edit the comment for a snapshot, do these steps: <ol style="list-style-type: none"> a. Select a snapshot. b. Click Edit. c. On the Edit Snapshot window, edit the existing comment in the Comments field. d. Click Save Configuration.
Delete	To delete snapshots, do these steps: <ol style="list-style-type: none"> a. Select one or more snapshots. b. Click Delete. c. Click Yes to confirm.

Option	Description
Apply	<p>To apply a snapshot, do these steps:</p> <ol style="list-style-type: none"> Select a snapshot. Click Apply. Click Yes to confirm. <p>Important:</p> <ul style="list-style-type: none"> You can apply a snapshot of the primary node on the backup node only from the command-line interface. You must apply the snapshot of the same node that you are working on. If you revert a snapshot in a cluster, apply the same level snapshot on each node in the cluster. If configuration or policy versions are newer than the firmware version, the settings are rejected. If the configuration and policy versions are older than the firmware version, the settings are moved to the current firmware version.
Download	<p>To download snapshots, do these steps:</p> <ol style="list-style-type: none"> Select one or more snapshots. Click Download. Browse to the location where you want to save the snapshot. Save the file. <p>Note: If you download multiple snapshots, the snapshots are compressed into a .zip file.</p>
Upload	<p>To upload a snapshot, do these steps:</p> <ol style="list-style-type: none"> Click Upload. In the Upload Snapshot window, click Browse for Snapshot. Select the snapshot that you want to upload. The snapshot information is displayed in the Files to upload table. In the Comments field, type a comment to describe the snapshot. Click Save Configuration. <p>Note: You can upload only 1 snapshot at a time.</p>
Refresh	To display the most recent list of snapshots, click Refresh .

Managing the support files

IBM Customer Support uses support files to help you troubleshoot problems with the IBM Security Identity Manager virtual appliance. Support files contain all log files, temporary and intermediate files, and command output that is needed to diagnose customer support problems.

About this task

Support files might contain customer-identifiable information, such as IP addresses, host names, user names, and policy files. Support files do not contain confidential information, such as passwords, certificates, and keys. All files inside a support file contain text that can be inspected and censored by the customer.

The support file contents are stored in a .zip file.

Tip: You can create multiple support files to track an issue over time.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > Support Files**.

The **Support Files** page is displayed.

2. On the **Support Files** page, do one or more of the following actions.

Option	Description
New	To create a support file, do these steps: <ol style="list-style-type: none">a. Click New.b. In the Comments field of the Create Support file window, type a comment to describe the support file.c. Click Save Configuration. A new support file is created on the IBM Security Identity Manager virtual appliance.
Edit	To edit the comment for a support file, do these steps: <ol style="list-style-type: none">a. Select a support file.b. Click Edit.c. On the Edit Support file window, edit the existing comment in the Comments field.d. Click Save Configuration.
Delete	To delete support files, do these steps: <ol style="list-style-type: none">a. Select one or more support files.b. Click Delete.c. Click Yes to confirm.
Download	To download support files, do these steps: <ol style="list-style-type: none">a. Select one or more support files.b. Click Download.c. Browse to the location where you want to save the support files.d. Save the file. Note: If you download multiple support files, the files are compressed into a .zip file.

Updating the management SSL certificate

If the management certificate expires, the local management interface is not reachable. Use this task to update the keystore certificate for the local management interface.

Before you begin

You must have an SSL certificate. See [Managing the SSL certificate configuration](#).

Procedure

1. Log on to the Appliance Dashboard.
2. Click **Manage > System Settings > Management SSL Certificate**.
3. Click the **LMI key store** check box.
LMI is the local management interface.
4. Click **Edit**.

The **Certificate** page opens.

5. Select the certificate.
6. Select either **Update** to upload a new certificate or **Export** to use the existing certificate for another virtual appliance.

- Click **Update**.

A dialog opens.

- a. Provide the certificate information.

- Use the **Browse** function to select the keystore file that has the certificate.
- Type a label for the certificate such as admin.
- Type the keystore password.
- Select the type of keystore, such as PKCS#12.

- b. Click **Save**.

- Click **Export**.

- Select **Save File**.
- Click **OK**.
- Select the local directory where you want to save the certificate.
- Click **Save**.

Configuring system audit events

Configure where you want the IBM Security Identity Manager virtual appliance to send notifications about changes to system settings and problems with the virtual appliance.

About this task

Available objects include system audit events that are predefined in the virtual appliance and any system audit event objects that you created.

Important: Predefined system audit event objects cannot be deleted from the virtual appliance because they contain all the events that take place on the virtual appliance eventually. When you create objects such as SNMP, email, or syslog, you can delete these created objects.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > System Audit Events**.

The **System Audit Events** page displays the **Available Objects** pane and the **Added Objects** pane.

2. In the **System Audit Events** page, complete one or more of the following tasks.

- To create a system audit event object, click **New**.

The following system audit event objects are listed:

- SNMP
- Email
- Remote Syslog

See these related topics to configure one or more of the following system audit event objects.

- [“Configuring SNMP objects” on page 29](#)
- [“Configuring email objects” on page 30](#)
- [“Configuring remote syslog objects” on page 31](#)
-

- To receive notifications for problems with the system, select one or more system audit event objects from the **Available Objects** pane, and add or move them to the **Added Objects** pane.
- To edit a system audit event object, complete the following steps:
 - a. Select a system audit event object in the **Added Objects** pane.
 - b. Click **Edit**.
 - c. Change the values in these fields according to your requirement.
 - **Name**
 - **Total Event Storage Limit**
 - **NAP Events Allocation**
 - **IPS Events Allocation**
 - **System Events Allocation**
 - **Comment**
 - d. Click **Save Configuration**.
- 3. Optional: To delete a system audit event object, do these steps.
 - a) Select a system audit event object that you created.
 - b) Click **Delete**.
 - c) Click **Yes** to confirm.
- 4. Click **Save Configuration**.
- 5. Optional: Click **Reset** to revert to the last updated changes.

Configuring SNMP objects

Configure Simple Network Management Protocol (SNMP) objects to enable the IBM Security Identity Manager virtual appliance to send system audit events to an SNMP manager. The SNMP notifications identify certain values and send them to an SNMP manager.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > System Audit Events**.
2. In the **System Audit Events** page, take one of the following actions.
 - Click **New > SNMP** to display the **Add SNMP Object** window.
 - Select an existing SNMP object and then click **Edit** to display the **Edit SNMP Object** window.
3. In the **General** tab, type a name for the object.
4. Select an **SNMP version** from the list.
 - V1
 - V2C
 - V3
5. In the **SNMP Manager** field, type the IP address, host name, or fully qualified domain name (FQDN) of the SNMP manager.

Note: The SNMP host must be accessible to the virtual appliance to send SNMP traps.
6. Type the port number that the SNMP manager monitors for notifications.

Note: The default port number is 162.
7. Type a comment to describe the SNMP object.
8. For SNMP versions V1 or V2c, type the name of the community that is used to authenticate with the SNMP agent.
9. For SNMP version 3, configure the following options.

Option	Description
Name	Type the user name to be authenticated in the SNMP database.
Notification Type	<p>On the Notification Type tab, complete these steps.</p> <ol style="list-style-type: none"> Select Inform or Trap in the Notification Type field. Specify the SNMP Timeout in seconds. <p>Note: Specifying a timeout value is not mandatory.</p>
Authentication and Privacy	<p>On the Authentication and Privacy tab, complete these steps.</p> <ol style="list-style-type: none"> From the Enable Authentication list, select Enabled to enable authentication. In Authentication Passphrase, type the relevant passphrase. From the Authentication Type list, select a type. From the Enable Privacy list, select Enabled to enable privacy. In Privacy Passphrase, type the relevant passphrase. From the Privacy Type list, select a type.

10. Click **Save Configuration**.

What to do next

After you configure an SNMP object, add the object to the **Added Objects** pane on the **System Audit Events** page. Add it so that the virtual appliance initiates the response when specified events occur.

Configuring email objects

You can create email objects to send an email notification to specified users or to administrators when specified events occur on your network. You can also select the event parameters to include in the message so that important information about detected events is provided.

Procedure

- From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > System Audit Events**.
- In **System Audit Events** page, take one of the following actions.
 - Click **New > Email** to display the **Add Email Object** window.
 - Select an existing email object and then click **Edit** to display the **Edit Email Object** window.
- Configure the following options.

Option	Description
Name	<p>Specifies a meaningful name for the response.</p> <p>Note: This name displays when you select responses for events, so give the response a name that allows users to easily identify what they are selecting.</p>
From	<p>Specifies the email address that displays in the From field of the email.</p>
To	<p>Specifies the email address or group of addresses to receive the email.</p> <p>Note: Separate individual email addresses with a comma or semicolon.</p>

Option	Description
SMTP Server	Specifies the fully qualified domain name or IP address of the mail server. Note: The SMTP server must be accessible to the virtual appliance to send email notifications.
SMTP Port	Specifies the custom port that is used to connect to the SMTP server. The default is 25.
Comment	Type a comment to identify the email object.

4. Click **Save**.

What to do next

After you configure an email object, add the object to the **Added Objects** pane on the **System Audit Events** page. Add it so that the virtual appliance initiates the response when specified events occur.

Configuring remote syslog objects

Configure remote syslog objects to enable the system to record system events in a remote log file.

About this task

If the connection to the remote syslog server drops, the virtual appliance generates a system audit event. If you are using TCP protocol, the virtual appliance writes the events to an auxiliary storage file. When the connection is restored, events that are stored in this file are sent to the remote syslog server. If the connection is not restored before the storage file size exceeds, any additional events are dropped. The virtual appliance generates another system audit event when the connection is reestablished.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > System Audit Events**.
2. In the **System Audit Events** page, do one of the following steps.
 - Click **Remote Syslog** to display the **Add Remote Syslog Object** window.
 - Select an existing remote syslog object and then click **Edit** to display the **Edit Remote Syslog Object** window.
3. Configure the following options.

Option	Description
Name	Specifies a meaningful name for the response.
Remote Syslog Collector	Specifies the fully qualified domain name or IP address of the host on which you want to save the log. Note: The host must be accessible to the virtual appliance.
Remote Syslog Collector Port	Specifies the custom port that is used to connect to the syslog collector. The default is 514.
QRadar Format Enabled	Select this check box to enable the virtual appliance to send events in QRadar LEEF format instead of RFC5424 remote syslog format.
Comment	Type a comment to identify the remote syslog object.

4. Click **Save Configuration**.

What to do next

After you configure a remote syslog object, add the object to the **Added Objects** pane on the **System Audit Events** page. Add it so that the virtual appliance initiates the response when specified events occur.

Restarting or shutting down

Use the **Restart or Shutdown** page to restart or shut down the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > Restart or Shut down**.

The **Restart or Shutdown** page is displayed.

2. Do one of the following tasks.

Option	Description
Restart	Restarting the IBM Security Identity Manager virtual appliance takes it offline for several minutes.
Shut Down	Shutting down the IBM Security Identity Manager virtual appliance takes it offline and makes it inaccessible over the network until you restart it.

Chapter 2. Administration console

Learn to use the features in the administration console to configure your identity management solution.

Home

Use this page to directly access the tasks that you can perform.

The **Home** page is displayed after you log in to the system. It includes status information and links to tasks that you can perform.

After you have clicked on a task link, you can exit the task and navigate back to the **Home** page by closing the task or selecting the **Home** link that displays in the upper left corner of the task page.

Service Connection Status table

Lists the current status of services you own. The table is displayed only when the login user is a service owner. Click the ▶ icon to toggle the table open or closed. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Status

Displays the current status of the service.



Indicates that the connection to the service was successful.



Indicates the status of the connection is unknown.



Indicates that the connection to the service failed.

Refresh

Click this button to obtain the updated status of the services. However, perform a **Test Connection** before refreshing the service status.

Service Name

Identifies the name of the service. Click the service name to view and make changes to the service.

Service Description

Provides a description of the service.

Last Status Date

Identifies the last time that IBM Security Identity Manager attempted to contact the service and query the connection status.

Common Tasks

Provides a list of common administrative tasks you can perform. Click the ▶ icon to toggle the task list open or closed.

To perform a task, click the task link within the task panel.

Related information

For more information, see the [IBM Knowledge Center](#).

Change Password

Select a User

Use this page to search for and select a user whose password you want to change.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select an attribute from the list. All searchable attributes and the personal profile are included in this list. If you select an attribute, the search is based on that attribute. If you select **Entire profile**, the search is based on all attributes associated with the user.

Last Name searches for the user's last name.

Full Name searches for the user's full name.

E-mail Address searches for the user's e-mail address.

Entire Profile searches all attributes associated with the user.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Users table

Lists the users matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

Name

Identifies a value for distinguishing a user, such as the user's full name. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the user's e-mail address.

Last Name

Identifies the user's last name.

Business Unit

Identifies the business unit. Click to view details about the organization.

Status

Identifies the user's status.

Users are either active or inactive. A user must be active to log in to the system. Users become inactive when they are suspended. The suspended users still exist, but they cannot access the system. System administrators can restore inactive users.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Change Passwords

Use this page to change the password for one or more accounts that belong to another user. You can change the password only when password editing is enabled.

Generate a password for me

Select this option to allow the system to generate a new password for you.

Allow me to type a password

Select this option to specify a password for the account.

Password

Type a new password for the account in this field. Asterisks (*) are displayed as you type. To edit this field, select the **Allow me to type a password** option.


Confirm password

Type the new password again. Asterisks (*) are displayed as you type. To edit this field, select the **Allow me to type a password** option.

Note: For some accounts, you cannot specify a password, even if you select **Allow me to type a password**. For these accounts, passwords must be generated. For example, some accounts are put into the credential vault. If the credentials for the account are configured to require check out and check in, you cannot specify the password, even if you select **Allow me to type a password**. The system generates a different password for these accounts. For these accounts, you must check out its credential to view the password.

If you have multiple accounts, and you select **Allow me to type a password**, your password is only applied to the accounts that permit a user-specified password.

Password strength rules

Click the  icon next to **View password strength rules** to display a list of password strength rules that must be applied for this account. The new password must conform to the password strength rules for the account, or the password is not changed. The password strength rules vary for an account, based on your organization guidelines.

Password Rule table

Lists the rules that the password policy has defined.

Password Rule

Identifies the password rule.

Setting

Identifies the value for password rule.

If no password policy has been set, the **Password Rule** table might not be displayed.

Selecting accounts

Accounts table

Lists the accounts, including your IBM Security Identity Manager login account. Each account is represented by the service that hosts the account and the user ID for the account. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account.

If password synchronization is not enabled, the check box next to the accounts are preselected. The password change applies only to selected accounts. If you cannot change the password for an account, the check box is disabled.

If password synchronization is enabled, the table displays a list of individual accounts whose passwords are automatically changed by this action. The Select column is not displayed when password synchronization is enabled.

Service Name

Identifies the name of the service that hosts the account. Click the name of the service to view information about the service.

User ID

Identifies the user ID for the account. Click the user ID to view the details about the account.

Ownership Type

Identifies the ownership type for an account. This column is displayed when password synchronization is disabled.

Scheduling your request

If you want to schedule your request for a later date and time, click the ▶ icon next to **Schedule**.

Immediate

Runs the request immediately after you click **Submit**. This option is selected by default.

Effective Date

Runs the request at a day and hour that you specify. After you select this option, click the calendar icon to specify the scheduled day and the clock icon to specify the scheduled hour.

Submitting your request

Click **Submit** to submit your request. If password synchronization is not enabled, you must select an account before clicking **Submit**.

Related information

For more information, see the [IBM Knowledge Center](#).

Service Details

Use this page to view the details that are related to the selected service. Each service has its own unique set of information. Refer to the documentation provided with the adapter for details about the displayed fields.

The following fields are common for most services. All fields are read-only, so you cannot change any information related to the service. These fields might or might not be displayed on the service form by default. Except for the **Service name** field, these fields can be added or removed.

Service name

Displays the name of the service.

Description

Displays the description of the service that was provided by the service owner.

URL

For remote services, displays the URL used to connect to the resource hosting the service. The *address* value is displayed in brackets for IPv6 addresses.

User ID

Displays the user ID used to log into the remote resource.

Owner

Displays the name of the service provider.

Service prerequisite

Displays the prerequisite that must be met before the service can be used, for example, at least one service account must exist.

Related information

For more information, see the [IBM Knowledge Center](#).

Account Information

Use this page to review the details related to the selected account. All fields are read-only.

The fields that are displayed on this page vary based on the type of service that you selected and by the authority the system administrator has granted you.

User ID

The user ID associated with the account. This field is common for all accounts.

If additional tabs are available, click the tabs to continue reviewing information.

Related information

For more information, see the [IBM Knowledge Center](#).

View Personal Profile

Use this page to view the personal profile information for the user that you have selected.

The profile contains personal, business, and contact information about who the user is, how to contact the user, and so on. Your ability to change and view profile information is determined by the authority your system administrator has granted to you.

Related information

For more information, see the [IBM Knowledge Center](#).

Personal Information

Use this notebook page to review the user's personal information.

The following fields are the default fields:

Last name

Specifies the user's last name, or family name.

Full name

Displays a value for distinguishing users, such as the user's full name.

Preferred user ID

Displays the default user ID that new accounts and access use when they are created.

First name

Specifies the user's first name, or given name.

Initials

Specifies the user's initial.

Home address

Specifies the user's postal address at home.

Shared secret

Specifies a value that is used to retrieve a new password when a password is reset.

Organizational roles

Specifies the organizational roles to which the user belongs.

Related information

For more information, see the [IBM Knowledge Center](#).

Business Information

Use this notebook page to review the user's business information.

The following fields are the default fields:

Office number

Specifies the office number.

Employee number

Specifies the employee number. This information is a numeric or alphanumeric identifier assigned to a user by the business/organization.

Title

Specifies the user's job title.

Manager

Specifies the user's manager.

Postal address

Specifies the user's postal address at work.

Administrative assistant

Specifies the personal or departmental administrative assistant.

Related information

For more information, see the [IBM Knowledge Center](#).

Contact Information

Use this page to review the user's contact information.

The following fields are the default fields:

E-mail address

Specifies the e-mail address.

Telephone number

Specifies the work telephone number.

Mobile telephone number

Specifies the mobile telephone number.

Pager

Specifies the pager number.

Home telephone number

Specifies the home telephone number.

Aliases

Specifies any aliases that are associated with the user ID.

Related information

For more information, see the [IBM Knowledge Center](#).

Business Unit Details

Use this page to view business unit details for an organization. The business unit fields available on this page vary according to the business unit type. All text fields are read-only.

Context within the organization

Provides a root structure below a Root Organization showing the organization structure, including organizations, organizational units, business partner organizational units, locations, and admin domains.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Roles

Manage Roles

Use the **Manage Roles** page to create, change, or delete roles. You can also manage role membership and role hierarchy.

The role hierarchy defines a parent-child relationship between an organizational role and its child roles. A child role itself is an organizational role.

The user members of a child role inherit the following attributes from the parent role:

- The entitlements associated with provisioning policies

- The permissions associated with the Access Control Items (ACIs)
- The ability to participate in workflow activities

When a child role is removed from a parent role, the entitlements associated with the parent role might be removed and are no longer inherited by the members of the child role.

You cannot delete a role that has user members or child roles. You must remove all of the users and child roles from the role before you can delete it.

You cannot delete a static role that is associated with a separation of duty policy or a provisioning policy. You must first remove the static role from the role separation list in the policy.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Role name or description searches for a role with a name or description that contains text that is entered in the **Search information** field.

Business unit searches for a role that is associated with a business unit that contains text that is entered in the **Search information** field.


Roles table

Lists the roles that match the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Name

Identifies the name of the role. Click the icon () next to the role name to display the tasks that can be carried out on the role:

Change

Click to change the role membership or entitlements.

Delete

Click to remove the selected role from the system.

Manage User Members

Click to see which users are members of the selected role, or to manage membership of the selected role.

Manage Child Roles

Click to see which roles are children of the selected role, or to manage membership of the selected role.

Add User Members

Click to add users as members of the selected role. This choice is not available for dynamic roles.

Add Child Roles

Click to add roles as children of the selected role. This choice is not available for dynamic roles.

Manage Provisioning Policies

Click to manage provisioning policies associated with the selected role.

Transfer

You can transfer static and dynamic roles to the business unit that is under the same organization root. Following are a few restrictions for role transfer activity:

- Roles cannot be transferred across different organization hierarchy.

- Static and dynamic roles cannot be transferred together.
- When dynamic roles are transferred, old entitlements might be lost. A user entitlements or membership is recomputed based on the new business unit under which the dynamic role is transferred.
- Roles to be transferred must contain an Access Control Item (ACI) granted for the Modify operation.

Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

Role Type

Indicates whether the role is static or dynamic.

Access Status

Access status for the associated role. Access status displays the following values:

Access Enabled

Access is defined and enabled.

Common Access Enabled

Access is defined and enabled as common.

Access Disabled

Access is disabled or undefined.

Access Type

Access type for the associated service.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a role.

Change

Click to change the role membership or entitlements.

Delete

Click to remove the selected role from the system.

Export Access Data

Click to open the **Export Access Data** page, and export the role access data. The **Export Access Data** button is not active until you select some accesses to activate it. Only the role access that you selected are exported.

Import Access Data

Click to open the **Import Access Data** page to import the access data for a role access. You can also import access data for a set of roles.

Enabled Access

Click to enable access for the selected roles.

Disable Access

Click to disable access for the selected roles.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Export access data

Use the **Export Access Data** page to export the role access data. The access data is specified in a comma-separated value (CSV) file. IBM Security Identity Manager uses the settings that are indicated in the CSV file.

The **Export Access Data** page is displayed after you click **Export Access Data** in the **Manage Roles** page.

After you submit the export request, a process status indicates the progress of the export operation.

Download Exported Data

Click to download the exported data for the group access. Download the file on your local system by using your web browser settings.

The exported data contains information such as Role DN, Role name, Define as Access, Access type, Icon URL, Search terms, Additional information, and Badges.

Download Export Log File

Click to view any error or log information about the export operation. This button is displayed only if the submitted export operation contains any log information or encountered any errors.

Cancel

Click to cancel the export operation. The operation is discontinued if you cancel it during an active export session.

Close

Click to close the **Export Access Data** page. The operation fails if you close the **Export Access Data** page during an active export session.

Import access data

Use the **Import Access Data** page to import the role access data. The access data is specified in the comma-separated value (CSV) file. IBM Security Identity Manager uses the settings that are indicated in the CSV file.

Note: The value of `True` in the `DEFINE_AS_ACCESS` attribute in the CSV file is considered as `TRUE`. Any other value in the `DEFINE_AS_ACCESS` field is considered `FALSE`.

File to Upload (.CSV)

Displays the name of the CSV file that contains all the role access data. This field is required.

Browse

Click to locate and upload the CSV file for import. You can also type the complete and correct path to the file on your workstation along with the file name.

Import

Click to immediately import the CSV file.

After you submit the import request, a process status indicates the progress of the import operation.

Note: If you click **Import** with an invalid file format, a message is displayed to inform you that the file format is not valid.

Cancel

Click to cancel the import operation. The operation is discontinued if you cancel it during an active import session.

Download Import Log File

Click to view any error or log information about the import operation. This button is displayed only if the submitted import operation contains any log information or encountered any errors.

Close

Click to close the **Import Access Data** page. The operation fails if you close the **Import Access Data** page during an active import session.

Organizational Role

Use this page to add, change, or delete a role that you want to manage.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Role name or description searches for a role with a name or description that contains text that is entered in the **Search information** field.

Business unit searches for a role associated with a business unit that contains text that is entered in the **Search information** field.

Roles table

Lists the roles matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Name

Identifies the name of the role.

Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

Role Type

Indicates whether the role is static or dynamic.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Create Role

Use this wizard to specify information about a role.

Role type

Select either a static or a dynamic role.

Static

Creates a role for a list of members that you manually specify.

Dynamic

Creates a role that selects users based on the attributes in a filter.

Related information

For more information, see the [IBM Knowledge Center](#).

Creating a static role

Complete these tabs to create a static role.

Role Type

Use this page to specify information about a static role type.

Role classification

Optionally specify how the role must be classified.

Business unit

Select the business unit to which the role applies.

Related information

For more information, see the [IBM Knowledge Center](#).

General Information

Use this page to specify general information about a role.

Role name

Type the name of the new role.

Description

Type information about the intended purpose of the role.


You can type values for role name, description, and any additional custom attributes in the **General Information** tab. The additional attributes can be added in the role definition schema using the form designer.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Information

Use the **Access Information** page to specify access information about a role, and also to specify business metadata for accesses.

To specify roles and users that have ownership of the role, click the twistie icon  next to **Owners**.

Role Owners table

Add one or more roles as owners for the role. The table contains these columns:

Select

Select the check box in this column to select a role. Select the check box at the top of the column to select all roles.

Role Name

Identifies the name of the role.

Role Description

Provides a brief description of the role.

Business Unit

Identifies the business unit that is associated with the role.

User Owners table

Add one or more users as owners for the role. The table contains these columns:

Select

Select the check box in this column to select a user. Select the check box at the top of the column to select all users.

Full Name

Identifies the full name of the user. Click the name of the user to view the personal profile for the user.

E-mail Address

Identifies the email address of the user.

Last Name

Identifies the surname of the user.

Business Unit

Identifies the business unit that is associated with the user.

Use these buttons with the role or user policy owners table:

Add

Click to add a role or user to the list. A search panel opens from which you can select the appropriate roles or users.

Remove

Click to remove one or more roles or users from the list.

Enable access for this role

Select to display the role in the user interface. When this option is selected, the user can request access for this role, view the access for this role, or delete the access for this role.

Show this role as a common access

Select to display this role as an access that a user can select in the user interface. This choice is available only if you previously selected **Enable access for this role**. This choice is available only for static roles.

Select access type

Select the access type from the tree structure. This choice is available only if you previously selected **Enable access for this role**.

Access Types

Expand or collapse a node in the tree to view and select an access type. For example, Application, Role, and other access types.

Icon URL

Provide a uniform resource identifier (URI) string for the icon. A preview of the icon is displayed that is based on the following conditions:

- If an icon URL is not specified, and the category image exists, then the preview displays the category image. An information message is displayed that this image is used.
- If an icon URL is not specified, and the category image does not exist, then the preview displays a message that there is no image.
- If an icon URL is specified, then the referenced image is displayed.

For more information, see the [Customizing an access card in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Search terms

Type the search strings that you want to add to return specific search terms. You can use multiple values for the search terms.

Use these buttons for the search terms:

Add

Click to add a search term.


Delete

Click to delete one or more search terms.

Additional information

Displays information about the access card by default. It is a free form information about the access item that the administrator considers useful.

Badges

Specify one or more badges for an access item that is associated with this role. Click the twistie icon  next to **Badges** to specify one or more badges. You can add a maximum of five badges for an access item.

Use these buttons for the badges:

Add

Click to add a badge. The button becomes inactive after a maximum of five badges are assigned to an access item.

Remove

Click to remove a badge. The button is not active until a badge is added.

Select a check box next to a badge to modify or delete it.

Badge text

Type a short text string for the badge. For example, High risk.

To customize the value of a badge text, add a \$ prefix to it. For example, \$Risk. You can customize only the value of a badge text when it is prefixed with \$. For example, \$Risk=High Risk. You cannot customize a badge text if it is not prefixed with \$.

You might want to configure the CustomLabels.properties file to customize the value for the badge text. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Badge class

Select a specific CSS class from the list to apply to the badge text. You can customize a badge class, where you can specify your own styles to be displayed in the **Badge class** list. For example, a CSS class can consist of font type, size, color, or other formatting styles, which you can apply to the specified badge text.

You might want to customize a badge CSS style to suit your requirements. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Preview

A preview displays the badge text that is based on the badge class you selected.

Related information

For more information, see the [IBM Knowledge Center](#).

Role Membership

Use this page to add or remove members from a static role.

Members table

Lists the current users who are members of the role. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

User Name

Identifies the full name of the user. Click the name of the user to view the user's personal profile.

Business Unit

Identifies the user's business unit.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a member to the role.

Remove

Click to remove a selected member from the role.

Related information

For more information, see the [IBM Knowledge Center](#).

Assignment Attributes

Use this page to add assignment attributes for a role. Only static roles support assignment attributes.

Attribute Name

Enter the name for a role assignment attribute.

Add

Click this button to add the attribute, whose name you entered in the Attribute Name field, to the role.

Attributes table

Lists the role assignment attributes. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a role assignment attribute. To select one or more role assignment attributes, select the check box next to the assignment attribute. To select all role assignment attributes, select the check box at the top of the column.

Attribute Name

Specifies the name of the role assignment attribute.

Attribute Label

Specifies the custom label associated with role assignment attribute. The custom label is displayed from the `CustomLabels.properties` file.

Remove

Click to remove a selected role assignment attribute.

Related information

For more information, see the [IBM Knowledge Center](#).

Creating a dynamic role

Complete these tabs to create a dynamic role.

Role Type

Use this page to specify information about a dynamic role type.

Role classification

Optionally specify how the role must be classified.

Business unit

Select the business unit to which the role applies.

Make role applicable to persons in

Set the extent to which the role applies.

This business unit and its subunits

Applies to users in the specified business unit and all subordinate business units.

This business unit only

Applies to users in the specified business unit only.

General Information

Use this page to specify general information about a role.

Role name

Type the name of the new role.

Description

Type information about the intended purpose of the role.


You can type values for role name, description, and any additional custom attributes in the **General Information** tab. The additional attributes can be added in the role definition schema using the form designer.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Information

Use the **Access Information** page to specify access information about a role, and also to specify business metadata for accesses.

To specify roles and users that have ownership of the role, click the twistie icon  next to **Owners**.

Role Owners table

Add one or more roles as owners for the role. The table contains these columns:

Select

Select the check box in this column to select a role. Select the check box at the top of the column to select all roles.

Role Name

Identifies the name of the role.

Role Description

Provides a brief description of the role.

Business Unit

Identifies the business unit that is associated with the role.

User Owners table

Add one or more users as owners for the role. The table contains these columns:

Select

Select the check box in this column to select a user. Select the check box at the top of the column to select all users.

Full Name

Identifies the full name of the user. Click the name of the user to view the personal profile for the user.

E-mail Address

Identifies the email address of the user.

Last Name

Identifies the surname of the user.

Business Unit

Identifies the business unit that is associated with the user.

Use these buttons with the role or user policy owners table:

Add

Click to add a role or user to the list. A search panel opens from which you can select the appropriate roles or users.

Remove

Click to remove one or more roles or users from the list.

Enable access for this role

Select to display the role in the user interface. When this option is selected, the user can request access for this role, view the access for this role, or delete the access for this role.

Show this role as a common access

Select to display this role as an access that a user can select in the user interface. This choice is available only if you previously selected **Enable access for this role**. This choice is available only for static roles.

Select access type

Select the access type from the tree structure. This choice is available only if you previously selected **Enable access for this role**.

Access Types

Expand or collapse a node in the tree to view and select an access type. For example, Application, Role, and other access types.

Icon URL

Provide a uniform resource identifier (URI) string for the icon. A preview of the icon is displayed that is based on the following conditions:

- If an icon URL is not specified, and the category image exists, then the preview displays the category image. An information message is displayed that this image is used.
- If an icon URL is not specified, and the category image does not exist, then the preview displays a message that there is no image.
- If an icon URL is specified, then the referenced image is displayed.

For more information, see the [Customizing an access card in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Search terms

Type the search strings that you want to add to return specific search terms. You can use multiple values for the search terms.

Use these buttons for the search terms:

Add

Click to add a search term.


Delete

Click to delete one or more search terms.

Additional information

Displays information about the access card by default. It is a free form information about the access item that the administrator considers useful.

Badges

Specify one or more badges for an access item that is associated with this role. Click the twistie icon  next to **Badges** to specify one or more badges. You can add a maximum of five badges for an access item.

Use these buttons for the badges:

Add

Click to add a badge. The button becomes inactive after a maximum of five badges are assigned to an access item.

Remove

Click to remove a badge. The button is not active until a badge is added.

Select a check box next to a badge to modify or delete it.

Badge text

Type a short text string for the badge. For example, High risk.

To customize the value of a badge text, add a \$ prefix to it. For example, \$Risk. You can customize only the value of a badge text when it is prefixed with \$. For example, \$Risk=High Risk. You cannot customize a badge text if it is not prefixed with \$.

You might want to configure the CustomLabels.properties file to customize the value for the badge text. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Badge class

Select a specific CSS class from the list to apply to the badge text. You can customize a badge class, where you can specify your own styles to be displayed in the **Badge class** list. For example, a CSS class can consist of font type, size, color, or other formatting styles, which you can apply to the specified badge text.

You might want to customize a badge CSS style to suit your requirements. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Preview

A preview displays the badge text that is based on the badge class you selected.

Related information

For more information, see the [IBM Knowledge Center](#).

Definition (Rule)

Use this page to specify the rule that selects members of a dynamic role.

Definition (Rule)

Type an LDAP filter rule to define the attributes of users who receive this role. For example, type (departmentnumber=audit123) to select all members in an auditing department that is named audit123.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule

Use this notebook page to schedule a request.

Immediate

Runs the request immediately.

Effective date

Runs the request at a day and hour that you specify. After you select this option, click the calendar icon to specify the scheduled day and click the clock icon to specify the scheduled hour.

Click **Finish** when you are done with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Role Information

Use this page to change information about a static role.

Name

Identifies the name of the role.

Description


Provides additional information about the role.

Role classification

Optionally specify how the role must be classified.

Business unit

Displays the business unit to which the role applies.

To specify roles and users to have ownership of the role, click the twistie icon  next to **Owners**.

Role Owners table

Add one or more roles as owners for the role. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Role Name

Identifies the name of the role.

Role Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

User Owners table

Add one or more users as owners for the role. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box next to the user. To select all users, select the check box at the top of the column.

Full Name

Identifies the user's full name. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the user's email address.

Last Name

Identifies the user's family name.

Business Unit

Identifies the business unit associated with the user.

Use these buttons with the role or user policy owners table:

Add

Click to add a role or user to the list. A search panel is displayed from which you can select the appropriate roles or users.

Remove

Click to remove one or more roles or users from the list.

Enable access for this role


Select to display the role in the user interface. When this option is selected, the user can request access for this role, view the access for this role, or delete the access for this role.

Show this role as a common access

Select to display this role as an access that a user can select in the user interface. This choice is available only if you previously selected **Enable access for this role**.

Select access type

Select the access type from the tree structure. This choice is available only if you previously selected **Enable access for this role**.

To view the junior roles for the role that you selected, click the icon  next to **Junior Roles**.

Junior Roles table

Lists the junior roles for the role that you selected. This table is displayed only for the static role that is a member of other roles. In other words, the junior roles have this role as a member. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Name

Identifies the name of the role.

Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

Related information

For more information, see the [IBM Knowledge Center](#).

Role Information

Use this page to change information about a dynamic role.

Name

Identifies the name of the role.

Description

Provides additional information about the role.

Role classification

Optionally specify how the role must be classified.

Definition (Rule)

Type an LDAP filter rule to define the attributes of users who receive this role. For example, type (departmentnumber=audit123) to select all members in an auditing department that is named audit123.

Business unit

Displays the business unit to which the role applies. You cannot modify this field.

Scope


Sets the extent to which the rule applies.

Applicable to users in this business unit only

Applies to users in the specified business unit only.

Applicable to users in this business unit and all its subunits

Applies to users in the specified business unit and all subordinate business units.

To specify roles and users to have ownership of the role, click the twistie icon  next to **Owners**.

Role Owners table

Add one or more roles as owners for the role. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Role Name

Identifies the name of the role.

Role Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

User Owners table

Add one or more users as owners for the role. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box next to the user. To select all users, select the check box at the top of the column.

Full Name

Identifies the user's full name. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the user's email address.

Last Name

Identifies the user's family name.

Business Unit

Identifies the business unit associated with the user.

You can use these buttons with the role or user policy owners table:

Add

Click to add a role or user to the list. A search panel is displayed, from which you can select the appropriate roles or users.

Remove

Click to remove one or more roles or users from the list.

Enable access for this role

Select to display the role in the user interface. When this option is selected, the user can request access for this role, view the access for this role, or delete the access for this role.

Select access type

Select the access type from the tree structure. This choice is available only if you previously selected **Enable access for this role**.

You can use these buttons:

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request.

Related information

For more information, see the [IBM Knowledge Center](#).

Change Role

Use this page or notebook to view and change information about a role.

The role information contains role type, role classification, and business unit. Your ability to change and view role information is determined by the authority your system administrator has granted you.

Click any available tabs to view or specify additional information. After you view or specify information in any available tabs, select an option to save any changes you made and complete your request.

Related information

For more information, see the [IBM Knowledge Center](#).

Changing static role information

Complete these tabs to change the properties for a static role.

Role Type

Use this notebook page to view and change information for a static role.

Your ability to change and view role information is determined by the authority your system administrator has granted to you. Contact your help desk or system administrator for information about roles. The following fields are the default fields:

Role type

Displays the selection as either static or dynamic.

Role classification

Optionally specify how the role must be classified.

Business unit

Displays the business unit to which the role applies.

OK

Click to save the changes.

Related information

For more information, see the [IBM Knowledge Center](#).

General Information

Use this notebook page to view and change general information for a static role.

Your ability to change and view role information is determined by the authority your system administrator has granted to you. Contact your help desk or system administrator for information about roles. The following fields are the default fields:

Name

Identifies the name of the role.

Description

Provides additional information about the role.

OK

Click to save the changes.

You can type values for any additional custom attributes in the **General Information** tab. The additional attributes can be added in the role definition schema using the form designer.


Related information

For more information, see the [IBM Knowledge Center](#).

Access Information

Use the **Access Information** page to view and change access information for a static role, and also to specify business metadata for accesses.

Your ability to change and view role information is determined by the authority that your system administrator granted to you. Contact your help desk or system administrator for information about roles. The following fields are the default fields:

To specify roles and users that have ownership of the role, click the twistie icon  next to **Owners**.

Role Owners table

Add one or more roles as owners for the role. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Role Name

Identifies the name of the role.

Role Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

User Owners table

Add one or more users as owners for the role. The table contains these columns:

Select

Select the check box in this column to select a user. Select the check box at the top of the column to select all users.

Full Name

Identifies the full name of a user. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the email address of a user.

Last Name

Identifies the surname of a user.

Business Unit

Identifies the business unit that is associated with the user.

Use these buttons with the role or user policy owners table:

Add

Click to add a role or user to the list. A search panel opens from which you can select the appropriate roles or users.

Remove

Click to remove one or more roles or users from the list.

Enable access for this role

Select to display the role in the user interface. When this option is selected, the user can request access for this role, view the access for this role, or delete the access for this role.

Show this role as a common access

Select to display this role as an access that a user can select in the user interface. This choice is available only if you previously selected **Enable access for this role**. This choice is available only for static roles.

Access type for this role

Identifies the access type for this role.

Change access type

Expand or collapse a node in the tree to view and select an access type. This choice is available only if you previously selected **Enable access for this role**.

Access Types

Expand or collapse a node in the tree to view and select an access type. For example, Application, Role, and other access types.

Icon URL

Provide a uniform resource identifier (URI) string for the icon. A preview of the icon is displayed that is based on the following conditions:

- If an icon URL is not specified, and the category image exists, then the preview displays the category image. An information message is displayed that this image is used.
- If an icon URL is not specified, and the category image does not exist, then the preview displays a message that there is no image.
- If an icon URL is specified, then the referenced image is displayed.

For more information, see the [Customizing an access card in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Search terms

Type the search strings that you want to add to return specific search terms. You can use multiple values for the search terms.

Use these buttons for the search terms:

Add

Click to add a search term.


Delete

Click to delete one or more search terms.

Additional information

Displays information about the access card by default. It is a free form information about the access item that the administrator considers useful.

Badges

Specify one or more badges for an access item that is associated with this role. Click the twistie icon  next to **Badges** to specify one or more badges. You can add a maximum of five badges for an access item.

Use these buttons for the badges:

Add

Click to add a badge. The button becomes inactive after a maximum of five badges are assigned to an access item.

Remove

Click to remove a badge. The button is not active until a badge is added.

Select a check box next to a badge to modify or delete it.

Badge text

Type a short text string for the badge. For example, High risk.

To customize the value of a badge text, add a \$ prefix to it. For example, \$Risk. You can customize only the value of a badge text when it is prefixed with \$. For example, \$Risk=High Risk. You cannot customize a badge text if it is not prefixed with \$.

You might want to configure the CustomLabels.properties file to customize the value for the badge text. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Badge class

Select a specific CSS class from the list to apply to the badge text. You can customize a badge class, where you can specify your own styles to be displayed in the **Badge class** list. For example, a CSS class can consist of font type, size, color, or other formatting styles, which you can apply to the specified badge text.

You might want to customize a badge CSS style to suit your requirements. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Preview

A preview displays the badge text that is based on the badge class you selected.

OK

Click to save the changes.

Related information

For more information, see the [IBM Knowledge Center](#).

Assignment Attributes

Use this page to change assignment attributes for a role. Only static roles support assignment attributes.

Attribute Name

Enter the name for a role assignment attribute.

Add

Click this button to add the attribute, whose name you entered in the Attribute Name field, to the role.

Attributes table

Lists the role assignment attributes. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a role assignment attribute. To select one or more role assignment attributes, select the check box next to the assignment attribute. To select all role assignment attributes, select the check box at the top of the column.

Attribute Name

Specifies the name of the role assignment attribute.

Attribute Label

Specifies the custom label associated with role assignment attribute. The custom label is displayed from the CustomLabels.properties file.

Remove


Click to remove a selected role assignment attribute.

Related information

For more information, see the [IBM Knowledge Center](#).

Parent roles

Use this notebook page to view parent roles for a static role.

To view the parent roles for the role that you selected, click the icon  next to **Parent Roles**.

Parent Roles table

Lists the parent roles for the role that you selected. This table is displayed only for the static role that is a member of other roles. In other words, the parent roles have this role as a member. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Name

Identifies the name of the role.

Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

OK

Click to save the changes.

Related information

For more information, see the [IBM Knowledge Center](#).

Changing dynamic role properties

Complete these tabs to change the properties for a dynamic role.

Role Type

Use this notebook page to view and change information for a dynamic role.

Your ability to change and view role information is determined by the authority your system administrator has granted to you. Contact your help desk or system administrator for information about roles. The following fields are the default fields:

Role type

Displays the selection about a dynamic role. You cannot modify this field.

Role classification

Optionally specify how the role must be classified.

Business unit

Displays the business unit to which the role applies. You cannot modify this field.

Scope

Sets the extent to which the rule applies.

Applicable to users in this business unit only

Applies to users in the specified business unit only.

Applicable to users in this business unit and all its subunits

Applies to users in the specified business unit and all subordinate business units.

You can use these buttons:

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request.

Related information

For more information, see the [IBM Knowledge Center](#).

General Information

Use this notebook page to view and change general information for a dynamic role.

Your ability to change and view role information is determined by the authority your system administrator has granted to you. Contact your help desk or system administrator for information about roles. The following fields are the default fields:

Name

Identifies the name of the role.

Description

Provides additional information about the role.

You can use these buttons:

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request.

You can type values for any additional custom attributes in the **General Information** tab. The additional attributes can be added in the role definition schema using the form designer.


Related information

For more information, see the [IBM Knowledge Center](#).

Access Information

Use the **Access Information** page to view and change access information for a dynamic role, and also to specify business metadata for accesses.

Your ability to change and view role information is determined by the authority that your system administrator granted to you. Contact your help desk or system administrator for information about roles. The following fields are the default fields:

To specify roles and users that have ownership of the role, click the twistie icon  next to **Owners**.

Role Owners table

Add one or more roles as owners for the role. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Role Name

Identifies the name of the role.

Role Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

User Owners table

Add one or more users as owners for the role. The table contains these columns:

Select

Select the check box in this column to select a user. Select the check box at the top of the column to select all users.

Full Name

Identifies the full name of a user. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the email address of a user.

Last Name

Identifies the surname of a user.

Business Unit

Identifies the business unit that is associated with the user.

Use these buttons with the role or user policy owners table:

Add

Click to add a role or user to the list. A search panel opens from which you can select the appropriate roles or users.

Remove

Click to remove one or more roles or users from the list.

Enable access for this role

Select to display the role in the user interface. When this option is selected, the user can request access for this role, view the access for this role, or delete the access for this role.

Access type for this role

Identifies the access type for this role.

Change access type

Expand or collapse a node in the tree to view and select an access type. This choice is available only if you previously selected **Enable access for this role**.

Access Types

Expand or collapse a node in the tree to view and select an access type. For example, Application, Role, and other access types.

Icon URL

Provide a uniform resource identifier (URI) string for the icon. A preview of the icon is displayed that is based on the following conditions:

- If an icon URL is not specified, and the category image exists, then the preview displays the category image. An information message is displayed that this image is used.
- If an icon URL is not specified, and the category image does not exist, then the preview displays a message that there is no image.
- If an icon URL is specified, then the referenced image is displayed.

For more information, see the [Customizing an access card in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Search terms

Type the search strings that you want to add to return specific search terms. You can use multiple values for the search terms.

Use these buttons for the search terms:

Add

Click to add a search term.


Delete

Click to delete one or more search terms.

Additional information

Displays information about the access card by default. It is a free form information about the access item that the administrator considers useful.

Badges

Specify one or more badges for an access item that is associated with this role. Click the twistie icon  next to **Badges** to specify one or more badges. You can add a maximum of five badges for an access item.

Use these buttons for the badges:

Add

Click to add a badge. The button becomes inactive after a maximum of five badges are assigned to an access item.

Remove

Click to remove a badge. The button is not active until a badge is added.

Select a check box next to a badge to modify or delete it.

Badge text

Type a short text string for the badge. For example, High risk.

To customize the value of a badge text, add a \$ prefix to it. For example, \$Risk. You can customize only the value of a badge text when it is prefixed with \$. For example, \$Risk=High Risk. You cannot customize a badge text if it is not prefixed with \$.

You might want to configure the CustomLabels.properties file to customize the value for the badge text. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Badge class

Select a specific CSS class from the list to apply to the badge text. You can customize a badge class, where you can specify your own styles to be displayed in the **Badge class** list. For example, a CSS class can consist of font type, size, color, or other formatting styles, which you can apply to the specified badge text.

You might want to customize a badge CSS style to suit your requirements. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Preview

A preview displays the badge text that is based on the badge class you selected.

You can use these buttons:

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request.

Related information

For more information, see the [IBM Knowledge Center](#).

Definition (Rule)

Use this notebook page to specify the rule that selects members of a dynamic role.

Your ability to change and view role information is determined by the authority your system administrator has granted to you. Contact your help desk or system administrator for information about roles. The following field is the default field:

Definition (Rule)

Type an LDAP filter rule to define the attributes of users who receive this role. For example, type (departmentnumber=audit123) to select all members in an auditing department that is named audit123.

You can use these buttons:

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage User Members and Child Roles

Use this page to view, add, or remove the user members and child roles of an organizational role.

In the **Type** list, specify whether to search by **User member** or **Child role**.

User member searches for user members by the attribute values that contain text that is entered in the **Search information** field. When you select this option, the **Users** table is displayed.

Child role searches for child roles by the name, description, or business name that contains text that is entered in the **Search information** field. When you select this option, the **Child Roles** table is displayed.

Users

User members can be associated with the role.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select an attribute from the list. All searchable attributes and the personal profile are included in this list. If you select an attribute, the search is based on that attribute. If you select **Entire profile**, the search is based on all attributes associated with the user.

Last Name searches for the user's last name.

Full Name searches for the user's full name.

E-mail Address searches for the user's e-mail address.

Entire Profile searches all attributes associated with the user.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Users table

Lists the users matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

Name

Identifies a value for distinguishing a user, such as the user's full name. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the user's e-mail address.

Last Name

Indicates the user's last name.

Business Unit

Identifies the business unit in which the user is located. Click the link for more information about the business unit.

Status

Identifies the user's status.

Users are either active or inactive. A user must be active to log in to the system. A user becomes inactive when they are suspended. The suspended user still exists, but cannot access the system. System administrators can restore inactive users.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add user members to the organizational role.

Remove

Click to remove the selected user members from the role.

Set Assignment Attributes

Click to set assignment attributes. The **Associate Role Assignment Attributes** page is displayed.

Child Roles

The role hierarchy defines a parent-child relationship between an organizational role and its child roles. A child role itself is an organizational role.

The user members of a child role inherit the following attributes from the parent role:

- The entitlements associated with provisioning policies
- The permissions associated with the Access Control Items (ACIs)
- The ability to participate in workflow activities

When a child role is removed from a parent role, the entitlements associated with the parent role might be removed and are no longer inherited by the members of the child role.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Role name or description searches for roles that contain text that is entered in the **Search information** field as a role name or description.

Business unit searches for roles that contain text that is entered in the **Search information** field as a business unit name in which the role is located.

Child Roles table

Lists the child roles matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Name

Identifies the name of the role.

Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add child roles to the organizational role.

Remove

Click to remove the selected child roles from the role.

Refresh

Click to update the list of roles in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Add User Members

Use this page to add users to membership in a role.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select an attribute from the list. All searchable attributes and the personal profile are included in this list. If you select an attribute, the search is based on that attribute. If you select **Entire profile**, the search is based on all attributes associated with the user.

Last Name searches for the user's last name.

Full Name searches for the user's full name.

E-mail Address searches for the user's e-mail address.

Entire Profile searches all attributes associated with the user.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Users table

Lists the users matching the specified search criteria in the **Search information** field. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

Name

Identifies a value for distinguishing a user, such as the user's full name. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the user's e-mail address.

Last Name

Indicates the user's last name of.

Note: This column is the value of *ercustomdisplay*, which has the initial, default value of Last Name. To change the value of *ercustomdisplay*, update the corresponding label in the *CustomLabels.properties* file.

Business Unit

Identifies the business unit in which the user is located. Click the link for more information about the business unit.

Status

Identifies the user's status.

Users are either active or inactive. A user must be active to log in to the system. Users become inactive when they are suspended. The suspended users still exist, but they cannot access the system. System administrators can restore inactive users.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **OK** to add the selected users to the role, or click **Cancel**.

Related information

For more information, see the [IBM Knowledge Center](#).

Associate role assignment attributes

Use this page to add or modify values for each role assignment attribute.

The role assignment attributes table displays the attributes associated with this user member of the role. If the role is a child role of one or more parent roles, the attributes includes the attributes from the all of the parent roles.

Each attribute is listed on a row in the attribute table. The table contains the following columns:

Attribute

A link to the attribute. Click the link to display another page, where you can modify values for the selected attribute.

Defined Role

The name of the role for which the attribute is defined.

Value

The current values for the attribute. You can specify more than one value for each attribute. Attributes are not required to have a value.

Actions

Several administration tasks use this panel. The actions you can take depend on the task.

- When managing user members, as part of Managing Roles, you can select **Continue** to save any modifications you made to the values for the attribute. The console continues to a confirmation page that displays the schedule for submission of the role changes.
- When creating or changing a user profile, as part of Managing Users, you can select **OK** to save the modifications you made to the attribute values and return to the panel that describes the user profile.
- For all tasks, you can elect **Cancel** to discard the modifications you made to the attribute values and return to the previous panel.

Related information

For more information, see the [IBM Knowledge Center](#).

Add Child Roles

Use this page to add child roles to an organizational role. The role hierarchy defines a parent-child relationship between an organizational role and its child roles. A child role itself is an organizational role. When you add child roles to a parent role, ensure that there is not a separation of duty policy violation.

The user members of a child role inherit the following attributes from the parent role:

- The entitlements associated with provisioning policies
- The permissions associated with the Access Control Items (ACIs)
- The ability to participate in workflow activities

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Role name or description searches for roles that contain text that is entered in the **Search information** field as a role name or description.

Business unit searches for roles that contain text that is entered in the **Search information** field as a business unit name in which the role is located.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Child Roles table

Lists the child role candidates matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Name

Identifies the name of the role.

Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

Role Type

Indicates whether the role is static or dynamic.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **OK** to add the selected roles as children of the organizational role, or click **Cancel**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Users

Use this page to search for and select one or more users to become owners of the role.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Users table

Lists the users matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

Name

Identifies a value for distinguishing a user, such as the user's full name. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the user's e-mail address.

Last Name

Identifies the user's last name.

Business Unit

Identifies the business unit. Click the business unit name to view details about the organization.

Status

Identifies the user's status.

Users are either active or inactive. A user must be active to log in to the system. Users become inactive when they are suspended. The suspended users still exist, but they cannot access the system. System administrators can restore inactive users.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Roles

Use this page to search for and select one or more roles to become owners of the role.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Role name or description searches for roles that contain text that is entered in the **Search information** field as a role name or description.

Business unit searches for roles that contain text that is entered in the **Search information** field as a business unit name in which the role is located.

Roles table

Lists the role members matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box adjacent to the role. To select all roles, select the check box at the top of the column.

Name

Identifies a value for distinguishing the role.

Description

Provides additional information about the role.

Business Unit

Identifies the business unit in which the role is located.

Role Type

Indicates whether the role is static or dynamic.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.

- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Definition (Rule)

Use this notebook page to specify the rule that selects members of a dynamic role.

Definition (Rule)

Type an LDAP filter rule to define the attributes of users who receive this role. For example, type (departmentnumber=audit123) to select all members in an auditing department that is named audit123.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule

Use this notebook page to schedule a request.

Immediate

Runs the request immediately.

Effective date

Runs the request at a day and hour that you specify. After you select this option, click the calendar icon to specify the scheduled day and click the clock icon to specify the scheduled hour.

Click **Finish** when you are done with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule

Use this page to schedule a request.

Immediate

Runs the request immediately.

Effective date

Runs the request at a day and hour that you specify. After you select this option, click the calendar icon to specify the scheduled day and click the clock icon to specify the scheduled hour.

Click **Finish** when you are done with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Set Assignment Values

Use this page to add or delete values for the role assignment attribute.

Add

To add a value, enter text in the text field. Click **Add**. When you click **Add**, the value is displayed in the text box below the input field. You can add more than one value.

Delete

Select an existing entry in the text box. Click **Delete** to remove the value.

When you have finished making changes, click **OK**.

Enable Access

You can control access by granting access to selected roles.

Enable as Common Access

Enables the role as common access.

Select an access type that you want to grant to all the specified roles

Specifies the access type that you want to grant for the selected roles.

Access Type

Select an access type for a role. The default access type for a role is **Role**. If **Role** is removed as an access type, the first access type is the default option.

Roles table

Lists the available roles that you can select and the associated access details. The table contains the following columns:

Role Name

Specifies the name of the role.

Description

Specifies the associated description for the role.

Access Type

Specifies the assigned access type for the role. For example: Role

You can use the following buttons:

Enable

Click to enable access for the displayed roles.

Cancel

Click to cancel any changes.

Manage Services

Select a Service

Use the **Select a Service** page to find the service that you want to manage.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Service searches for service names or descriptions that contain the text that is entered in the **Search information** field.

Business unit searches for business units in which the business unit name contains the text that is entered in the **Search information** field.

Service type

Select a service type from the list. The items in the list contain the service types that are installed by the administrator. Select **All** from the list to show all of the services that are managed by IBM Security Identity Manager.

Status

Specify the status value for the search. The items in the list contain possible status values for each service. Status values:

All

Include status values for all services.

Alive

Services that are functioning with no known issues.

Failed

Services that encountered a problem. For example, a connection test might fail, or a request was not completed on a remote endpoint.

Attempting recovery

Services that encountered a problem, and for which the server is attempting to process a previously blocked request.

Locked

Services that are locked because a reconciliation process is running.

Unknown

Services that never attempted a connection test or received and processed a request.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Services table

Lists the services that match the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box next to the service. To select all services, select the check box at the top of the column.


Status

Specifies the status of the service. Each status is represented by an icon. The icons correspond to the options in the service status list in the search criteria. Click the icon to get to detailed service status information. If the service is in Alive status, the column does not contain an icon.

Service Name

Identifies the name of the service.

Click the name of the service to change the service information.

Click the icon () next to the service to show the tasks that can be completed on the service. The task that you can complete is dependent on the type of service.

Use these menu items to complete a task on the selected service:

Set Up Reconciliation

Defines a reconciliation schedule. Reconciliation can be done immediately or scheduled for a later time. You can schedule a reconciliation to occur regularly.

Configure Policy Enforcement

Defines policy enforcement options for non-compliant accounts.

Manage Groups

Creates, modifies, or deletes groups, adds and removes membership, and defines access on a group.

Request Accounts

Requests the accounts on the service.

Accounts

Lists the accounts that use the service.

Customize Account Form

Use this action to create or modify a customized account form for the service instance.

Delete Account Form

Use this action to delete a customized account form for the service instance and reset to the default account form.

Account Recertification Status

Identifies the recertification status for accounts on a service.

Account Defaults

Defines defaults to be used by accounts that use the service.

Reconcile Now

Run a reconciliation immediately.

Enforce Policy

Reevaluate the governing provisioning policies for the service.

Retry Blocked Requests

Attempt a connection to the remote endpoint and try again any outstanding requests that are found. When you complete fixes to a service and bring the service online, you can then use this action to try again the requests.

Description

Identifies a brief description of the service.

Service Type

Identifies the type of service.

Note: Accesses that are defined on the original service are not available for the hosted service, and those accesses cannot be requested by users in different organizations.

Business Unit

Identifies the business unit in which the service is created.

Access Name

The access name of the corresponding service. If access is undefined, the field is empty.

Access Status

The status of the corresponding service. Access status displays the following value:

Access Enabled

Access is defined and enabled.

Access Disabled

Access is disabled or undefined.

Note: For HRFeed services, the column is always empty.

Access Type

The access type for the corresponding service. If access is undefined, the field is empty.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a service.

Change

Click to change the information for the selected service.

Delete

Click to delete the selected service and remove all accounts on that particular service from the system. The accounts are not removed from the resource. Deleting a service automatically removes it from all provisioning policies, identity policies, password policies, adoption policies, and recertification policies that currently reference it. In addition, if all services that are referenced by a policy are deleted by this operation, the entire policy is also deleted.

Export Access Data

Click to open the **Export Access Data** page, and export the service access data. The **Export Access Data** button is not active until you select some accesses to activate it. Only the service access that you selected are exported.

Import Access Data

Click to open the **Import Access Data** page to import the access data for a service access. You can also import access data for a set of services.

Enable Access

Click to enable access for the service.

Disable Access

Click to disable access for the service.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Export access data

Use the **Export Access Data** page to export the service access data. The access data is specified in a comma-separated value (CSV) file. IBM Security Identity Manager uses the settings that are indicated in the CSV file.

The **Export Access Data** page is displayed after you click **Export Access Data** in the **Select a Service** page.

After you submit the export request, a process status indicates the progress of the export operation.

Download Exported Data

Click to download the exported data for the service access. Download the file on your local system by using your web browser settings.

The exported data contains information such as Service DN, Service name, Define as Access, Access name, Access type, Access description, Icon URL, Search terms, Additional information, and Badges.

Download Export Log File

Click to view any error or log information about the export operation. This button is displayed only if the submitted export operation contains any log information or encountered any errors.

Cancel

Click to cancel the export operation. The operation is discontinued if you cancel it during an active export session.

Close

Click to close the **Export Access Data** page. The operation fails if you close the **Export Access Data** page during an active export session.

Related information

For more information, see the [IBM Knowledge Center](#).

Import access data

Use the **Import Access Data** page to import the service access data. The access data is specified in a comma-separated value (CSV) file. IBM Security Identity Manager uses the settings that are indicated in the CSV file.

File to Upload (.CSV)

Displays the name of the CSV file that contains all the service access data. This field is required.

Browse

Click to locate and upload the CSV file for import. You can also type the complete and correct path to the file on your workstation along with the file name.

Import

Click to immediately import the CSV file.

After you submit the import request, a process status indicates the progress of the import operation.

Note: If you click **Import** with an invalid file format, a message is displayed to inform you that the file format is not valid.

Cancel

Click to cancel the import operation. The operation is discontinued if you cancel it during an active import session.

Download Import Log File

Click to view any error or log information about the import operation. This button is displayed only if the submitted import operation contains any log information or encountered any errors.

Close

Click to close the **Import Access Data** page. The operation fails if you close the **Import Access Data** page during an active import session.

Related information

For more information, see the [IBM Knowledge Center](#).

Enable Access

You can control access by granting access to selected services.

Use service description for the access description

Lets you use the same service description for the access description.

Note: If selected, the service description overrides the existing access description.

Select an access type that you want to grant to all the specified services

Specifies the access type that you want to grant for the selected services.

Access Types

Select an access type for a service. The default access type for a service is **Application**. If **Application** is removed as an access type, the first access type is the default option.

Services table

Lists the available services and the access details that are assigned to the service. The table contains the following columns:

Service Name

Name of the service.

Description

A short description for the service.

Access Name

The assigned access name.

Access Type

The type of access assigned to the service. For example: Application.

You can use the following buttons:

Enable

Click to enable access for the displayed services.

Cancel

Click to cancel any changes.

Service Status Information

Use this page to review status information for the selected service.

Service name

The name of the service as shown on the administration console.

Service description

Description of the service as entered by the system administrator.

Status

Current operational status of the service. Possible values are:

Alive

Services that are functioning with no known issues.

Failed

Services that encountered a problem. For example, a connection test might fail, or a request did not complete on a remote endpoint.

Attempting recovery

Services that encountered a problem, and for which the server is attempting to run a previously blocked request.

Locked

Services that are locked because a reconciliation process is running.

Unknown

Services which never attempted a connection test or attempted to run a request.

Number of blocked requests

Number of requests that are blocked, waiting for the service to return to Active status.

Failed since date

Timestamp describing when this service was placed in Failed status

Last attempt date

Timestamp describing the last time the system attempted to make a connection to the service.

Oldest blocked request id

Process ID of the oldest request that is blocked because this service is in any status other than Alive. This ID can be useful when a request fails repeatedly. You can go to View Requests and use this value to identify the process ID to cancel.

Oldest blocked request date

Timestamp describing when the oldest pending request ID was originally processed by the system.

Last failing server

Describes the WebSphere cell, node, and server which last tried to connect to the service. This information can be useful in determining whether a particular server in a WebSphere cluster installation is having trouble processing requests.

Last failure reason

A detailed message that describes the reason for failure of the most recent attempt to connect to the service.

Actions**Close**

Closes the status information window and returns to the Manage Services page.

Refresh

Retrieves the most recent status information for the service.

Create a Service

Use this wizard to create a service. The tabs available vary depending on the type of service you are creating.

Related information

For more information, see the [IBM Knowledge Center](#).

Select the Type of Service

Use this page to select the service type for the service that you want to create.

Business unit

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Service Type table

Lists the available service types. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the service type for the service that you want to create.

Service Type

Identifies the type of service.

Description

Contains a brief description of the service type.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Service Information

Use this page to specify information about a service instance. The fields that are displayed on this page of the wizard vary based on the type of service that you selected in the previous panel.

You can specify a service instance for a managed resource. You provide information that IBM Security Identity Manager associates with a service instance. For example, an attribute might represent the administrative user ID and administrative password on a managed resource, or the Universal Resource Locator (URL) of the resource.

Alternatively, you can specify a service instance for activities that import identity data. You provide information that IBM Security Identity Manager uses during the data import, such as a file name or the data naming context.

Click **Test Connection** when the fields are complete, to test the connection to the managed resource. For manual services, the **Test Connection** button is not available.

If the connection is successful and SSL is configured, an informational message is displayed, indicating a successful connection. If the connection is successful and SSL is *not* configured, a warning message is displayed. If the connection fails, a warning message is displayed. You can continue with the wizard, even if the connection is not successful.

Related information

For more information, see the [IBM Knowledge Center](#).

Hosted Service: Service Information

Use this page to specify information about the hosted service.

Note: Accesses that are defined on the original service are not available for the hosted service, and those accesses cannot be requested by users in different organizations.

If you select a service profile for a hosted service, complete these fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance.

Description

Specify additional information about the service instance.

Service

Click **Search** to specify an existing service instance.

Click **Clear** to remove the currently specified service.

Service prerequisite

Click **Search** to specify an existing service instance or function that the hosted service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user can only receive a new account if they have an existing account on the service prerequisite.

Owner

Specify the existing user ID of the service owner that administers the service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user be used in administering the service instance

Click **Finish** when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

DSML Identity Feed: Service Information

Use this page to specify information about the Directory Services Markup Language (DSML) identity feed.

If you select a service profile to import identity data using DSML, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

User ID

Specify the administrative user ID for the service instance.

Password

Specify the administrative password for the service instance. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

File name

Specify the file name, including the path name, that contains the user information.

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

IDI Data Feed: Service Information

Use this page to specify information about the Initial Domain Identifier (IDI) identity feed.

If you select a service profile for activities that use IBM Security Directory Integrator to import identity data, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the name of the principal to authenticate clients using the Java Naming and Directory Interface (JNDI) application programming interface.

Password

Specify the password to authenticate clients using the JNDI application programming interface. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Name attribute

Select an attribute, such as uid, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

INetOrgPerson Identity Feed: Service Information

Use this page to specify information about the INetOrgPerson identity feed.

If you select a service profile to import identity data using LDAP, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the distinguished name (DN) of the administrator who is authorized to access the LDAP server that provides the identity information. For example, the user ID on LDAP is `cn=Administrator,cn=users,dc=itimcv,dc=com`, where *itimcv* is the domain name.

Password

Specify the password for the administrator who is authorized to access the LDAP server that provides the identity feed. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Attribute mapping file name

Specify the absolute path and file name of the file that contains attribute mapping between the identity feed source schema and specified user type schema. The mapping file contains key value pairs that identify the source and target attribute mapping.

Name attribute

Select an attribute, such as uid, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

AD OrganizationalPerson Identity Feed: Service Information

Use this page to specify information about the Active Directory OrganizationalPerson identity feed.

If you select a service profile to import identity data using Active Directory, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the distinguished name (DN) of the administrator who is authorized to access the LDAP server that provides the identity information. For example, the user ID on LDAP is `cn=Administrator,cn=users,dc=itimcv,dc=com`, where *itimcv* is the domain name.

Password

Specify the password for the administrator who is authorized to access the LDAP server that provides the identity feed. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Attribute mapping file name

Specify the absolute path and file name of the file that contains attribute mapping between the identity feed source schema and specified user type schema. The mapping file contains key value pairs that identify the source and target attribute mapping.

Name attribute

Select an attribute, such as uid, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

CSV Identity Feed: Service Information

Use this page to specify information about the comma-separated value (CSV) identity feed.

The comma-separated value (CSV) file cannot contain binary attributes. If you include multivalued attributes, they must be represented by using multiple columns with the same attribute name. You must list all required attributes in the CSV file before you list optional attributes.

If you select a service profile for activities that use a CSV format to import identity data, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

File name

Specify the file name, including the path name, of the CSV file.

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Name attribute

Select an attribute, such as `uid`, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP Profile: Service Information

Use this page to specify information about the Lightweight Directory Access Protocol (LDAP) service instance.

The LDAP service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

LDAP service**Service name**

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the LDAP service instance runs.

Description

Specify additional information about the LDAP service instance.

Connection mode

This option is available only if the `erconnectionmode` attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`. Where *ip-address* is the Security Directory Integrator host and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Directory server location

Specify the location and port number of the LDAP Adapter. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `ldap://[address]:port number`.

Use SSL communication with LDAP?

Select this check box to use secure communication with the LDAP service instance.

Administrator name

Specify the administrative user ID, such as `cn=root`, for the LDAP service instance. The name must be a distinguished name (DN).

Password

Specify the administrative password for the LDAP service instance. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Directory server name

Choose a directory server from the list.

Owner

Click **Search** to specify the existing user ID of the service owner that administers the LDAP service instance.

Click **Clear** to remove the currently specified user.

Service prerequisite

Click **Search** to specify an existing service instance or function that the LDAP service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user can only receive a new account if they have an existing account on the service prerequisite.

Users and groups**User base DN**

Specify the distinguished name (DN) of the container or base point where the users are stored.

RDN attribute

Specify the required relative distinguished name (RDN) attribute for the LDAP service instance.

Group base DN

Specify the DN of the container or base point where the groups are stored.

Initial group member

Specifies a DN used to create the LDAP group. It is prefilled with cn=TIM Adapter. Optionally, you can customize this initial group member.

Group object class name

Select the group object class for example GroupOfNames.

Group membership attribute

Select the group membership attribute for example member.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Vault Service: Service Information

Specify information about the vault service.

The vault service type creates a service where the privileged accounts are only for vault use. There is no connection to the endpoint service. These accounts are created locally and loaded into the credential vault so that they can be shared.

If you select a service profile for a vault service, complete the following fields to connect to the server where the service is located:

Service name

Specify a name that helps you identify the service instance.

Description

Specify more information about the service instance.

Service

Click **Search** to specify an existing service instance. You can have only one vault service for every remote service.

Click **Clear** to remove the currently specified service.

Owner

Specify the existing user ID of the service owner that administers the service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user can administer the service instance.

Uniform Resource Identifier

Enter one or more URIs that identify the vault.

Click **Add** to add the URI to the list.

Click **Clear** to remove the URI from the list.

Click **Finish** when you are finished with this task.

General Information

Use this page to specify information about a service instance. The fields that are displayed on this page of the wizard vary based on the type of service that you selected in the previous panel.

You can specify a service instance for a managed resource. You provide information that IBM Security Identity Manager associates with a service instance. For example, an attribute might represent the administrative user ID and administrative password on a managed resource, or the Universal Resource Locator of the resource.

Alternatively, you can specify a service instance for activities that import identity data. You provide information that IBM Security Identity Manager uses during the data import, such as a file name or the data naming context.

Click **Test Connection** when the fields are complete, to test the connection to the managed resource. For manual services, the **Test Connection** button is not available.

If the connection is successful and SSL is configured, an informational message is displayed, indicating a successful connection. If the connection is successful and SSL is *not* configured, a warning message is displayed. If the connection fails, a warning message is displayed. You can continue with the wizard, even if the connection is not successful.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Solaris Profile: General Information

Use this page to specify information about the Solaris service instance.

The Solaris service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the Solaris service instance runs.

Description

Specify additional information about the Solaris service instance.

Connection mode

This option is available only if the `erconnectionmode` attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the Solaris resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the Solaris server when the account is deleted.

Ensure that you also set the home directory permissions, which by default are none. If no permissions are set, the home directory is not deleted when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the Solaris service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user be used in administering the service instance

Service prerequisite

Specify an existing service instance or function that the Solaris service instance requires.

Click **Search** to specify an existing service instance or function that the Linux service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Linux Profile: General Information

Use this page to specify information about the Linux service instance.

The Linux service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service is:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the Linux service instance runs.

Description

Specify additional information about the Linux service instance.

Connection mode

This option is available only if the *erconnectionmode* attribute is added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:1099/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the Linux resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

RXA Internet Command TimeOut

The RXA library is used for the internal communication between the adapter and the managed resource. By default, when RXA issues a command, it expects a response within 5000 milliseconds. This property is only used when the managed resource takes more than default time to respond and the RXA call fails with timeout error.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the Linux server when the account is deleted.

Ensure that you also set the home directory permissions, which by default are none. If no permissions are set, the home directory is not deleted when the account is deleted.

Use a shadow file?

Select this check box if you want to use an access-restricted ASCII system file that stores users' encrypted passwords and related information. This field is unique to the UNIX service types.

Return sudo privileges?

If checked, the adapter returns the sudo privileges granted to users and groups during reconciliation.

Path to the sudoers file

If it is not the default location `/etc/sudoers` on the resource, enter the directory path to the sudoers file.

Owner

Specify the existing user ID of the service owner that administers the Linux service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify to use any user in administering the service instance

Service prerequisite

Specify an existing service instance or function that the Linux service instance requires.

Click **Search** to specify an existing service instance or function that the Linux service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX HP-UX Profile: General Information

Use this page to specify information about the HP-UX service instance.

The HP-UX service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the HP-UX service instance runs.

Description

Specify additional information about the HP-UX service instance.

Connection mode

This option is available only if the `erconnectionmode` attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the HP-UX resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

Use a shadow file?

Select this check box to use an access-restricted ASCII system file that stores users' encrypted passwords and related information. This field is unique to the UNIX service types.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the HP-UX server when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the HP-UX service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify to use any user in administering the service instance.

Service prerequisite

Click **Search** to specify an existing service instance or function that the HP-UX service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX AIX Profile: General Information

Use this page to specify information about the AIX® service instance.

The AIX service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the AIX service instance runs.

Description

Specify additional information about the AIX service instance.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the AIX resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

User registry

Specify how to manage and authenticate users.

- Leave Blank if the users on the service are to be managed only through the `/etc/password` file.
- Type `files` if this is a mixed setup and the users are to be managed through the `/etc/password` file.
- Type LDAP if this is a mixed setup and the users are to be managed through LDAP.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the AIX server when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the AIX service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user be used in administering the service instance

Service prerequisite

Specify an existing service instance or function that the AIX service instance requires.

If a service has another service defined as a service prerequisite, a user can only receive a new account if they have an existing account on the service prerequisite.

Related information

For more information, see the [IBM Knowledge Center](#).

Authentication

Use this page to configure authentication for the service. This page is displayed only if you are creating a POSIX service instance.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Solaris Profile: Authentication

Use this page to configure authentication for the Solaris service instance.

Administrator name

Specify the administrative user ID, such as `root`, for the Solaris server.

Is sudo user?

Select this check box if the administrator has `sudo` capability on the Solaris server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the Solaris server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the key store containing the private key of the client. This key store must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Linux Profile: Authentication

Use this page to configure authentication for the Linux service instance.

Administrator name

Specify the administrative user ID, such as root, for the Linux server.

Is sudo user?

Select this check box if the administrator has sudo capability on the Linux server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the Linux server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the key store containing the private key of the client. This key store must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX HP-UX Profile: Authentication

Use this page to configure authentication for the HP-UX service instance.

Administrator name

Specify the administrative user ID, such as root, for the HP-UX server.

Is sudo user?

Select this check box if the administrator has sudo capability on the HP-UX server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the HP-UX server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the key store containing the private key of the client. This key store must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX AIX Profile: Authentication

Use this page to configure authentication for the AIX service instance.

Administrator name

Specify the administrative user ID, such as root, for the AIX server.

Is sudo user?

Select this check box if the administrator has sudo capability on the AIX server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the AIX server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the keystore containing the private key of the client. This keystore must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Dispatcher Attributes

Use this page to specify information about the dispatcher attributes. This page is displayed only for Directory Integrator-based services.

AL FileSystem Path

Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines received from IBM Security Identity Manager. For example, you can specify the following file path to load the assembly lines from the `profiles` directory under these operating systems:

- Windows: `c:\Files\IBM\TDI\profiles`
- UNIX and Linux: `system:/opt/IBM/TDI/profiles`

Max Connection Count

Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. For example, enter `10` when you want the dispatcher to run maximum `10` assembly lines simultaneously for the service. If you enter `0`, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.

Disable AL Caching

Select the check box to disable the assembly line caching in the dispatcher for the service. The assembly lines for add, modify, delete, and test operations are not cached.

Related information

For more information, see the [IBM Knowledge Center](#).

Status and Information

Use this page to view information about the adapter and managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. For example, ADK adapters do not include fields for TDI version and Dispatcher version, and TDI adapters do not include the ADK version field. The adapter must be running to obtain the information.

- Verify the adapter log to ensure that the IBM Security Identity Manager test request was successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify IBM Security Identity Manager service parameters for the adapter profile. For example, verify the workstation name or the IP address of the managed resource and the port.

Last status update: Date

Specifies the most recent date when the **Status and Information** tab was updated.

Last status update: Time

Specifies the most recent time of the date when the **Status and Information** tab was updated.

Managed resource status

Specifies the status of the managed resource that the adapter is connected to.

Managed resource version

Specifies the version of the managed resource.

Profile version

Specifies the version of the profile that is installed in the IBM Security Identity Manager server.

Adapter version

Specifies the version of the adapter that the IBM Security Identity Manager service uses to provision request to the managed resource.

TDI connector version

Specifies the version of the TDI connector.

Managed resource status message

Specifies the status message for the managed resource.

TDI version

Specifies the version of the Security Directory Integrator on which the adapter is deployed.

Dispatcher version

Specifies the version of the dispatcher.

ADK version

Specifies the version of the ADK that the adapter uses.

Installation platform

Specifies summary information about the operating system where the adapter is installed.

Adapter account

Specifies the account that running the adapter binary file.

Adapter up time: Date

Specifies the date when the adapter started.

Adapter up time: Time

Specifies the time of the date when the adapter started.

Adapter memory usage

Specifies the memory usage for running the adapter. If the connection fails, follow the instructions in the error message.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Access Information

Use the **Access Information** page to specify access information for a service of users, including the name, type, description, and other business metadata for accesses.

Define an Access

Select this check box to activate the fields that are required to define an access item. Clearing this check box clears the access item selection.

Note: If you clear this check box, the information that is contained in the fields is cleared only when the operation is completed.

Access name

Type a name to identify an access item.

Select access type

Select an access type from the **Access Types** tree structure.

Access Types

Expand or collapse a node in the tree to view and select an access type. For example, Application, Role, and other access types.

Access description

Provide more information about the access item.

Icon URL

Provide a uniform resource identifier (URI) string for the icon. A preview of the icon is displayed that is based on the following conditions:

- If an icon URL is not specified, and the category image exists, then the preview displays the category image. An information message is displayed that this image is used.
- If an icon URL is not specified, and the category image does not exist, then the preview displays a message that there is no image.
- If an icon URL is specified, then the referenced image is displayed.

For more information, see the [Customizing an access card in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Search terms

Type the search strings that you want to add to return specific search terms. You can use multiple values for the search terms.

Use these buttons for the search terms:

Add

Click to add a search term.


Delete

Click to delete one or more search terms.

Additional information

Displays information about the access card by default. It is a free form information about the access item that the administrator considers useful.

Badges

Specify one or more badges for an access item that is associated with this service. Click the twistie icon  next to **Badges** to specify one or more badges. You can add a maximum of five badges for an access item.

Use these buttons for the badges:

Add

Click to add a badge. The button becomes inactive after a maximum of five badges are assigned to an access item.

Remove

Click to remove a badge. The button is not active until a badge is added.

Select a check box next to a badge to modify or delete it.

Badge text

Type a short text string for the badge. For example, High risk.

To customize the value of a badge text, add a \$ prefix to it. For example, \$Risk. You can customize only the value of a badge text when it is prefixed with \$. For example, \$Risk=High Risk. You cannot customize a badge text if it is not prefixed with \$.

You might want to configure the `CustomLabels.properties` file to customize the value for the badge text. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Badge class

Select a specific CSS class from the list to apply to the badge text. You can customize a badge class, where you can specify your own styles to be displayed in the **Badge class** list. For example, a CSS class can consist of font type, size, color, or other formatting styles, which you can apply to the specified badge text.

You might want to customize a badge CSS style to suit your requirements. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Preview

A preview displays the badge text that is based on the badge class you selected.

Configure Policy

Use this page to configure a provisioning policy that makes the service available to users. The page is not displayed if you are creating a service for an identity feed.

You can generate a policy that is automatically used or manually configured. Alternatively, you can manually configure the policy at a later time. Generating a policy that is automatically used makes the service available to all users, and the Default Account Request Workflow is associated with the provisioning policy.

Specify whether or not to generate a policy for all users.

Yes, create a policy for manually requesting accounts

Select this option to require that users manually request account entitlement.

Yes, create a policy to automatically create accounts, and later enable the policy

Select this option to allow for automatic provisioning of new accounts to users. You must subsequently enable the policy to provision new accounts.

Yes, create a policy to automatically create accounts as soon as the policy exists

Select this option to allow for automatic provisioning of new accounts to users. Provisioning of new accounts occurs as soon as the policy exists, and the Default Account Request Workflow is associated with the provisioning policy.

No, I will manually configure a policy later

Select this option if you want to configure a provisioning policy at a later time.

You might manually configure a provisioning policy if you need to set up account defaults or identity policies for this service. Later, you can change the provisioning to automatic.

Related information

For more information, see the [IBM Knowledge Center](#).

Reconcile Supporting Data

Use this page to schedule an account reconciliation for the service. This page is displayed only if you are creating an LDAP service instance or a POSIX service instance.

Perform a supporting data reconciliation now

Select this check box to start reconciliation immediately after you click **OK**.

Schedule supporting data reconciliation

The fields displayed vary, depending on the scheduling option that is selected. Select one of these schedule intervals to reconcile accounts for this service:

Daily

Reconciles accounts every day. After you select this option, click the clock icon to specify a time in the **At this time** field.

Weekly

Reconciles accounts once a week. After you select this option, select a day from the **On this day of the week** list, and then click the clock icon to specify a time in the **At this time** field.

Monthly

Reconciles accounts once a month. After you select this option, select a date from the **On this day of the month** list, and then click the clock icon to specify a time in the **At this time** field.

Hourly

Reconciles accounts once an hour. After you select this option, select a time from the **At this minute** list.

Annually - On a specific day of the year

Reconciles accounts on a specific date and time. After you select this option, select a month from the **Month** list. Then select a date from the **On this day of the month** list, and then click the clock icon to specify a time in the **At this time** field.

During a specific month

Reconciles accounts on a specific month, day, and time. After you select this option, select a month from the **Month** list. Then select a day from the **On this day of the week** list, and then click the clock icon to specify a time in the **At this time** field.

Never

Never reconciles accounts.

Click **Finish** when you are done with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Participants

Use this page to specify participant information. This page is displayed only if you are creating a manual service.

Participant type

Indicates the type of participant that you select. Possible participant types include:

- Administrator
- Service owner
- Manager
- User
- Group

Person name

Displays the person's name. This field is displayed only when the **User** participant type is selected.

Group name

Displays the group's name. This field is displayed only when the **Group** participant type is selected.

Escalation time in days

The amount of time in days the participant has to perform an activity before the activity is escalated.

Escalation participant type

Indicates the type of escalation participant that you select. Possible escalation participant types include:

- Administrator
- Service owner
- Manager
- User
- Group

Person name

Displays the person's name. This field is displayed only when the **User** escalation participant type is selected.

Group name

Displays the group's name. This field is displayed only when the **Group** escalation participant type is selected.

Click **Finish** when you are done with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Messages

Optionally, use this page to change the contents of an email message to send when corresponding operations are performed. This page is displayed only for manual services.

This **Messages** page is available only when you select **Manual** from **Connection mode**. For information about Connection mode, see [“POSIX Solaris Profile: General Information” on page 80](#)

Messages table

Lists the email messages to send when corresponding operations are performed. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates the message that is selected.

Operation

Identifies the operation that must be performed to send the email message.

Subject

Identifies the subject of the email message.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Change** to change the contents of the selected message.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Reconciliation

Optionally, use this page to specify a reconciliation file. This page is displayed only if you are creating a manual service.

Reconcile supporting data only

Select this check box to reconcile only supporting data from the inputted CSV file. No account data is reconciled. Group information is added or updated in IBM Security Identity Manager, but accounts are not added or updated.

Reconciliation file

Identifies the name of the reconciliation file that you select. The file cannot contain binary attributes. If you include multivalued attributes, they must be represented by using multiple columns with the same attribute name.

You can use these buttons:

Browse

Click to navigate to the reconciliation file.

Upload file

Click to upload the reconciliation file to the system.

Click **Finish** when you are done with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Search Results

Use this page to view information found for your search. Both the title of the page and the data in the table vary, depending on the field that you selected in the previous panel.

Lists the objects matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates the object that is selected.

Name

Identifies the name of the object to locate, based on the field that you selected in the previous panel.

Description

Describes the object. This column of information occurs if you previously customized an account request to include a group description and this panel is generated by a group search on account request.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Change a Service

Use this page to change information about a service instance. The tabs available vary depending on the type of service you are creating.

Click **Test Connection** when the fields are complete, to test the connection to the managed resource.

Related information

For more information, see the [IBM Knowledge Center](#).

Service Information

Use this page to change information about a service instance. The fields that are displayed on this page of the wizard vary based on the type of service that you selected in the previous panel.

You can specify a service instance for a managed resource. You provide information that IBM Security Identity Manager associates with a service instance. For example, an attribute might represent the administrative user ID and administrative password on a managed resource, or the Universal Resource Locator (URL) of the resource.

Alternatively, you can specify a service instance for activities that import identity data. You provide information that IBM Security Identity Manager uses during the data import, such as a file name or the data naming context.

Click **Test Connection** when the fields are complete, to test the connection to the managed resource. For manual services, the **Test Connection** button is not available.

If the connection is successful and SSL is configured, an informational message is displayed, indicating a successful connection. If the connection is successful and SSL is *not* configured, a warning message is displayed. If the connection fails, a warning message is displayed. You can continue with the wizard, even if the connection is not successful.

ITIM Service

Use this page to specify information about the ITIM Service.

If you select a service profile for an ITIM Service, complete these fields to connect to the server where the service resides:

Service name

Specifies a name that helps you identify the service instance.

Owner

Specifies the existing user ID of the service owner that administers the service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that the service instance does not have an assigned owner.

WebSphere account repository

Specifies the existing account repository used by IBM Security Identity Manager for authentication.

- If IBM Security Identity Manager is installed and configured to use its own custom registry, the default value for the service is *ITIM Service*.
- If IBM Security Identity Manager is installed to use an external user registry that is used by WebSphere Application Server, then:
 - If the external user registry is a service that is managed by IBM Security Identity Manager, click **Search** to locate and specify the service.

Note: You must create a service for the user registry before you enter the name of the service in this field. If you have not created the service, see the topic *Creating services* in the *IBM Security Identity Manager Administration Guide*.

- If the external user registry is *not* a service that is managed by IBM Security Identity Manager, this field must be empty. Click **Clear** to remove any value that is in the field.

- If IBM Security Identity Manager is installed to use its own custom registry, but you want to change the configuration to use an external user registry, you must reconfigure IBM Security Identity Manager before you modify the value of this field:
 1. Complete the instructions in the topic *Reconfiguration for authentication with an external user registry* in the *IBM Security Identity Manager Installation Guide*. You can view this document on the IBM Security Identity Manager information center
 2. After you complete the reconfiguration:
 - If the external user registry is a service that is managed by IBM Security Identity Manager, click **Search** to locate and specify the service.

Note: You must create a service for the user registry before you enter the name of the service in this field. If you have not created the service, see the topic *Creating services* in the *IBM Security Identity Manager Administration Guide*.
 - If the external user registry is *not* a service that is managed by IBM Security Identity Manager, this field must be empty. Click **Clear** to remove any value that is in the field.

Usage notes:

- If the value of **WebSphere account repository** is not set, or if the value is anything other than **ITIM Service**, then you cannot change the Identity Manager account password.
- If you change the value of **WebSphere account repository**, you might need to wait a few minutes for the profile of the Identity Manager account to be refreshed in order to see the effective change. In WebSphere cluster environments, the changed value may not be propagated to each node until the next refresh interval of the profiles. If you change **WebSphere account repository** from ITIM Service to another service, or to no value, the disabling of the password change feature does not take effect until the profile is refreshed.
- This property relates to both forgotten password enablement and the WebSphere user registry configuration under which IBM Security Identity Manager is deployed. For the forgotten password feature to function correctly, set this value to the service that corresponds to the configured user repository in WebSphere. This setting determines the account password to change after the challenge questions are answered successfully. If the WebSphere Application Server account repository value is not set, the forgotten password option is not enabled regardless of the setting on the **Configure Forgotten Password** page and the forgotten password option is not available on the **Login** page.

Hosted Service: Service Information

Use this page to specify information about the hosted service.

Note: Accesses that are defined on the original service are not available for the hosted service, and those accesses cannot be requested by users in different organizations.

If you select a service profile for a hosted service, complete these fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance.

Description

Specify additional information about the service instance.

Service

Click **Search** to specify an existing service instance.

Click **Clear** to remove the currently specified service.

Service prerequisite

Click **Search** to specify an existing service instance or function that the hosted service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user can only receive a new account if they have an existing account on the service prerequisite.

Owner

Specify the existing user ID of the service owner that administers the service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user be used in administering the service instance

Click **Finish** when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

DSML Identity Feed: Service Information

Use this page to specify information about the Directory Services Markup Language (DSML) identity feed.

If you select a service profile to import identity data using DSML, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

User ID

Specify the administrative user ID for the service instance.

Password

Specify the administrative password for the service instance. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

File name

Specify the file name, including the path name, that contains the user information.

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

IDI Data Feed: Service Information

Use this page to specify information about the Initial Domain Identifier (IDI) identity feed.

If you select a service profile for activities that use IBM Security Directory Integrator to import identity data, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the name of the principal to authenticate clients using the Java Naming and Directory Interface (JNDI) application programming interface.

Password

Specify the password to authenticate clients using the JNDI application programming interface. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Name attribute

Select an attribute, such as `uid`, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

INetOrgPerson Identity Feed: Service Information

Use this page to specify information about the INetOrgPerson identity feed.

If you select a service profile to import identity data using LDAP, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the distinguished name (DN) of the administrator who is authorized to access the LDAP server that provides the identity information. For example, the user ID on LDAP is `cn=Administrator,cn=users,dc=itimcv,dc=com`, where *itimcv* is the domain name.

Password

Specify the password for the administrator who is authorized to access the LDAP server that provides the identity feed. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Attribute mapping file name

Specify the absolute path and file name of the file that contains attribute mapping between the identity feed source schema and specified user type schema. The mapping file contains key value pairs that identify the source and target attribute mapping.

Name attribute

Select an attribute, such as `uid`, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

AD OrganizationalPerson Identity Feed: Service Information

Use this page to specify information about the Active Directory OrganizationalPerson identity feed.

If you select a service profile to import identity data using Active Directory, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the distinguished name (DN) of the administrator who is authorized to access the LDAP server that provides the identity information. For example, the user ID on LDAP is `cn=Administrator,cn=users,dc=itimcv,dc=com`, where *itimcv* is the domain name.

Password

Specify the password for the administrator who is authorized to access the LDAP server that provides the identity feed. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Attribute mapping file name

Specify the absolute path and file name of the file that contains attribute mapping between the identity feed source schema and specified user type schema. The mapping file contains key value pairs that identify the source and target attribute mapping.

Name attribute

Select an attribute, such as uid, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

CSV Identity Feed: Service Information

Use this page to specify information about the comma-separated value (CSV) identity feed.

The comma-separated value (CSV) file cannot contain binary attributes. If you include multivalued attributes, they must be represented by using multiple columns with the same attribute name. You must list all required attributes in the CSV file before you list optional attributes.

If you select a service profile for activities that use a CSV format to import identity data, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

File name

Specify the file name, including the path name, of the CSV file.

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Name attribute

Select an attribute, such as uid, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP Profile: Service Information

Use this page to specify information about the Lightweight Directory Access Protocol (LDAP) service instance.

The LDAP service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

LDAP service**Service name**

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the LDAP service instance runs.

Description

Specify additional information about the LDAP service instance.

Connection mode

This option is available only if the `erconnectionmode` attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`. Where *ip-address* is the Security Directory Integrator host and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Directory server location

Specify the location and port number of the LDAP Adapter. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `ldap://[address]:port number`.

Use SSL communication with LDAP?

Select this check box to use secure communication with the LDAP service instance.

Administrator name

Specify the administrative user ID, such as `cn=root`, for the LDAP service instance. The name must be a distinguished name (DN).

Password

Specify the administrative password for the LDAP service instance. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Directory server name

Choose a directory server from the list.

Owner

Click **Search** to specify the existing user ID of the service owner that administers the LDAP service instance.

Click **Clear** to remove the currently specified user.

Service prerequisite

Click **Search** to specify an existing service instance or function that the LDAP service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user can only receive a new account if they have an existing account on the service prerequisite.

Users and groups**User base DN**

Specify the distinguished name (DN) of the container or base point where the users are stored.

RDN attribute

Specify the required relative distinguished name (RDN) attribute for the LDAP service instance.

Group base DN

Specify the DN of the container or base point where the groups are stored.

Initial group member

Specifies a DN used to create the LDAP group. It is prefilled with cn=TIM Adapter. Optionally, you can customize this initial group member.

Group object class name

Select the group object class for example GroupOfNames.

Group membership attribute

Select the group membership attribute for example member.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

General Information

Use this page to specify information about a service instance. The fields that are displayed on this page of the wizard vary based on the type of service that you selected in the previous panel.

You can specify a service instance for a managed resource. You provide information that IBM Security Identity Manager associates with a service instance. For example, an attribute might represent the administrative user ID and administrative password on a managed resource, or the Universal Resource Locator of the resource.

Alternatively, you can specify a service instance for activities that import identity data. You provide information that IBM Security Identity Manager uses during the data import, such as a file name or the data naming context.

Click **Test Connection** when the fields are complete, to test the connection to the managed resource. For manual services, the **Test Connection** button is not available.

If the connection is successful and SSL is configured, an informational message is displayed, indicating a successful connection. If the connection is successful and SSL is *not* configured, a warning message is displayed. If the connection fails, a warning message is displayed. You can continue with the wizard, even if the connection is not successful.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Solaris Profile: General Information

Use this page to specify information about the Solaris service instance.

The Solaris service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the Solaris service instance runs.

Description

Specify additional information about the Solaris service instance.

Connection mode

This option is available only if the `erconnectionmode` attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the Solaris resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the Solaris server when the account is deleted.

Ensure that you also set the home directory permissions, which by default are none. If no permissions are set, the home directory is not deleted when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the Solaris service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user be used in administering the service instance

Service prerequisite

Specify an existing service instance or function that the Solaris service instance requires.

Click **Search** to specify an existing service instance or function that the Linux service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Linux Profile: General Information

Use this page to specify information about the Linux service instance.

The Linux service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service is:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the Linux service instance runs.

Description

Specify additional information about the Linux service instance.

Connection mode

This option is available only if the *erconnectionmode* attribute is added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:1099/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the Linux resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

RXA Internet Command TimeOut

The RXA library is used for the internal communication between the adapter and the managed resource. By default, when RXA issues a command, it expects a response within 5000 milliseconds. This property is only used when the managed resource takes more than default time to respond and the RXA call fails with timeout error.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the Linux server when the account is deleted.

Ensure that you also set the home directory permissions, which by default are none. If no permissions are set, the home directory is not deleted when the account is deleted.

Use a shadow file?

Select this check box if you want to use an access-restricted ASCII system file that stores users' encrypted passwords and related information. This field is unique to the UNIX service types.

Return sudo privileges?

If checked, the adapter returns the sudo privileges granted to users and groups during reconciliation.

Path to the sudoers file

If it is not the default location `/etc/sudoers` on the resource, enter the directory path to the sudoers file.

Owner

Specify the existing user ID of the service owner that administers the Linux service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify to use any user in administering the service instance

Service prerequisite

Specify an existing service instance or function that the Linux service instance requires.

Click **Search** to specify an existing service instance or function that the Linux service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX HP-UX Profile: General Information

Use this page to specify information about the HP-UX service instance.

The HP-UX service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the HP-UX service instance runs.

Description

Specify additional information about the HP-UX service instance.

Connection mode

This option is available only if the `erconnectionmode` attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the HP-UX resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

Use a shadow file?

Select this check box to use an access-restricted ASCII system file that stores users' encrypted passwords and related information. This field is unique to the UNIX service types.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the HP-UX server when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the HP-UX service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify to use any user in administering the service instance.

Service prerequisite

Click **Search** to specify an existing service instance or function that the HP-UX service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX AIX Profile: General Information

Use this page to specify information about the AIX service instance.

The AIX service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the AIX service instance runs.

Description

Specify additional information about the AIX service instance.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the AIX resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

User registry

Specify how to manage and authenticate users.

- Leave Blank if the users on the service are to be managed only through the `/etc/password` file.
- Type `files` if this is a mixed setup and the users are to be managed through the `/etc/password` file.
- Type LDAP if this is a mixed setup and the users are to be managed through LDAP.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the AIX server when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the AIX service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user be used in administering the service instance

Service prerequisite

Specify an existing service instance or function that the AIX service instance requires.

If a service has another service defined as a service prerequisite, a user can only receive a new account if they have an existing account on the service prerequisite.

Related information

For more information, see the [IBM Knowledge Center](#).

Authentication

Use this page to configure authentication for the service. This page is displayed only if you are creating a POSIX service instance.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Solaris Profile: Authentication

Use this page to configure authentication for the Solaris service instance.

Administrator name

Specify the administrative user ID, such as root, for the Solaris server.

Is sudo user?

Select this check box if the administrator has sudo capability on the Solaris server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the Solaris server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the key store containing the private key of the client. This key store must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Linux Profile: Authentication

Use this page to configure authentication for the Linux service instance.

Administrator name

Specify the administrative user ID, such as root, for the Linux server.

Is sudo user?

Select this check box if the administrator has sudo capability on the Linux server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the Linux server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the key store containing the private key of the client. This key store must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX HP-UX Profile: Authentication

Use this page to configure authentication for the HP-UX service instance.

Administrator name

Specify the administrative user ID, such as root, for the HP-UX server.

Is sudo user?

Select this check box if the administrator has sudo capability on the HP-UX server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the HP-UX server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the key store containing the private key of the client. This key store must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX AIX Profile: Authentication

Use this page to configure authentication for the AIX service instance.

Administrator name

Specify the administrative user ID, such as root, for the AIX server.

Is sudo user?

Select this check box if the administrator has sudo capability on the AIX server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the AIX server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the keystore containing the private key of the client. This keystore must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Dispatcher Attributes

Use this page to specify information about the dispatcher attributes. This page is displayed only for Directory Integrator-based services.

AL FileSystem Path

Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines received from IBM Security Identity Manager. For example, you can specify the following file path to load the assembly lines from the profiles directory under these operating systems:

- Windows: c:\Files\IBM\TDI\profiles
- UNIX and Linux: system:/opt/IBM/TDI/profiles

Max Connection Count

Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. For example, enter 10 when you want the dispatcher to run maximum 10 assembly lines simultaneously for the service. If you enter 0, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.

Disable AL Caching

Select the check box to disable the assembly line caching in the dispatcher for the service. The assembly lines for add, modify, delete, and test operations are not cached.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Information

Use the **Access Information** page to specify access information for a service of users, including the name, type, description, and other business metadata for accesses.

Define an Access

Select this check box to activate the fields that are required to define an access item. Clearing this check box clears the access item selection.

Note: If you clear this check box, the information that is contained in the fields is cleared only when the operation is completed.

Access name

Type a name to identify an access item.

Select access type

Select an access type from the **Access Types** tree structure.

Access Types

Expand or collapse a node in the tree to view and select an access type. For example, Application, Role, and other access types.

Access description

Provide more information about the access item.

Icon URL

Provide a uniform resource identifier (URI) string for the icon. A preview of the icon is displayed that is based on the following conditions:

- If an icon URL is not specified, and the category image exists, then the preview displays the category image. An information message is displayed that this image is used.
- If an icon URL is not specified, and the category image does not exist, then the preview displays a message that there is no image.
- If an icon URL is specified, then the referenced image is displayed.

For more information, see the [Customizing an access card in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Search terms

Type the search strings that you want to add to return specific search terms. You can use multiple values for the search terms.

Use these buttons for the search terms:

Add

Click to add a search term.


Delete

Click to delete one or more search terms.

Additional information

Displays information about the access card by default. It is a free form information about the access item that the administrator considers useful.

Badges

Specify one or more badges for an access item that is associated with this service. Click the twistie icon  next to **Badges** to specify one or more badges. You can add a maximum of five badges for an access item.

Use these buttons for the badges:

Add

Click to add a badge. The button becomes inactive after a maximum of five badges are assigned to an access item.

Remove

Click to remove a badge. The button is not active until a badge is added.

Select a check box next to a badge to modify or delete it.

Badge text

Type a short text string for the badge. For example, High risk.

To customize the value of a badge text, add a \$ prefix to it. For example, \$Risk. You can customize only the value of a badge text when it is prefixed with \$. For example, \$Risk=High Risk. You cannot customize a badge text if it is not prefixed with \$.

You might want to configure the `CustomLabels.properties` file to customize the value for the badge text. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Badge class

Select a specific CSS class from the list to apply to the badge text. You can customize a badge class, where you can specify your own styles to be displayed in the **Badge class** list. For example, a CSS class can consist of font type, size, color, or other formatting styles, which you can apply to the specified badge text.

You might want to customize a badge CSS style to suit your requirements. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Preview

A preview displays the badge text that is based on the badge class you selected.

Status and Information

Use this page to view information about the adapter and managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. For example, ADK adapters do not include fields for TDI version and Dispatcher version, and TDI adapters do not include the ADK version field. The adapter must be running to obtain the information.

- Verify the adapter log to ensure that the IBM Security Identity Manager test request was successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify IBM Security Identity Manager service parameters for the adapter profile. For example, verify the workstation name or the IP address of the managed resource and the port.

Last status update: Date

Specifies the most recent date when the **Status and Information** tab was updated.

Last status update: Time

Specifies the most recent time of the date when the **Status and Information** tab was updated.

Managed resource status

Specifies the status of the managed resource that the adapter is connected to.

Managed resource version

Specifies the version of the managed resource.

Profile version

Specifies the version of the profile that is installed in the IBM Security Identity Manager server.

Adapter version

Specifies the version of the adapter that the IBM Security Identity Manager service uses to provision request to the managed resource.

TDI connector version

Specifies the version of the TDI connector.

Managed resource status message

Specifies the status message for the managed resource.

TDI version

Specifies the version of the Security Directory Integrator on which the adapter is deployed.

Dispatcher version

Specifies the version of the dispatcher.

ADK version

Specifies the version of the ADK that the adapter uses.

Installation platform

Specifies summary information about the operating system where the adapter is installed.

Adapter account

Specifies the account that running the adapter binary file.

Adapter up time: Date

Specifies the date when the adapter started.

Adapter up time: Time

Specifies the time of the date when the adapter started.

Adapter memory usage

Specifies the memory usage for running the adapter. If the connection fails, follow the instructions in the error message.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Participants

Use this page to specify participant information. This page is displayed only if you are changing a manual service.

Participant type

Indicates the type of participant that you select. Possible participant types include:

- Administrator
- Service owner
- Manager
- User
- Group

Person name

Indicates the person's name. This field is displayed only when the **User** participant type is selected.

Group name

Indicates the group's name. This field is displayed only when the **Group** participant type is selected.

Escalation time in days

The amount of time in days the participant has to perform an activity before the activity is escalated.

Escalation participant type

Indicates the type of escalation participant that you select. Possible escalation participant types include:

- Administrator
- Service owner
- Manager
- User
- Group

Person name

Indicates the person's name. This field is displayed only when the **User** escalation participant type is selected.

Group name

Indicates the group's name. This field is displayed only when the **Group** escalation participant type is selected.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Messages

Optionally, use this page to change the contents of an email message to send when corresponding operations are performed. This page is displayed only for manual services.

This **Messages** page is available only when you select **Manual** from **Connection mode**. For information about Connection mode, see [“POSIX Solaris Profile: General Information” on page 80](#)

Messages table

Lists the email messages to send when corresponding operations are performed. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates the message that is selected.

Operation

Identifies the operation that must be performed to send the email message.

Subject

Identifies the subject of the email message.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Change** to change the contents of the selected message.

Click other tabs to specify additional information.

Related information

For more information, see [the IBM Knowledge Center](#).

Participants

Use this page to specify participant information. This page is displayed only if you are changing a manual service.

Participant type

Indicates the type of participant that you select. Possible participant types include:

- Administrator
- Service owner
- Manager
- User
- Group

Person name

Indicates the person's name. This field is displayed only when the **User** participant type is selected.

Group name

Indicates the group's name. This field is displayed only when the **Group** participant type is selected.

Escalation time in days

The amount of time in days the participant has to perform an activity before the activity is escalated.

Escalation participant type

Indicates the type of escalation participant that you select. Possible escalation participant types include:

- Administrator
- Service owner
- Manager
- User

- Group

Person name

Indicates the person's name. This field is displayed only when the **User** escalation participant type is selected.

Group name

Indicates the group's name. This field is displayed only when the **Group** escalation participant type is selected.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Reconciliation

Optionally, use this page to specify a reconciliation file. This page is displayed only if you are changing a manual service.

Reconcile supporting data only

Select this check box to reconcile only supporting data from the inputted CSV file. No account data is reconciled. Group information is added or updated in IBM Security Identity Manager, but accounts are not added or updated.

Reconciliation file

Identifies the name of the reconciliation file that you select. The file cannot contain binary attributes. If you include multivalued attributes, they must be represented by using multiple columns with the same attribute name.

You can use these buttons:

Browse

Click to navigate to the reconciliation file.

Upload file

Click to upload the reconciliation file to the system.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Change a Manual Service

Use this page to change the general information, participants, e-mail messages, and reconciliation file for a manual service instance.

Related information

For more information, see the [IBM Knowledge Center](#).

General Information

Use this page to specify general information about the manual service.

The fields that are displayed on this page vary, depending on the way you configured the service type that was used to create this manual service.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Information

Use the **Access Information** page to specify access information for a service of users, including the name, type, description, and other business metadata for accesses.

Define an Access

Select this check box to activate the fields that are required to define an access item. Clearing this check box clears the access item selection.

Note: If you clear this check box, the information that is contained in the fields is cleared only when the operation is completed.

Access name

Type a name to identify an access item.

Select access type

Select an access type from the **Access Types** tree structure.

Access Types

Expand or collapse a node in the tree to view and select an access type. For example, Application, Role, and other access types.

Access description

Provide more information about the access item.

Icon URL

Provide a uniform resource identifier (URI) string for the icon. A preview of the icon is displayed that is based on the following conditions:

- If an icon URL is not specified, and the category image exists, then the preview displays the category image. An information message is displayed that this image is used.
- If an icon URL is not specified, and the category image does not exist, then the preview displays a message that there is no image.
- If an icon URL is specified, then the referenced image is displayed.

For more information, see the [Customizing an access card in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Search terms

Type the search strings that you want to add to return specific search terms. You can use multiple values for the search terms.

Use these buttons for the search terms:

Add

Click to add a search term.


Delete

Click to delete one or more search terms.

Additional information

Displays information about the access card by default. It is a free form information about the access item that the administrator considers useful.

Badges

Specify one or more badges for an access item that is associated with this service. Click the twistie icon  next to **Badges** to specify one or more badges. You can add a maximum of five badges for an access item.

Use these buttons for the badges:

Add

Click to add a badge. The button becomes inactive after a maximum of five badges are assigned to an access item.

Remove

Click to remove a badge. The button is not active until a badge is added.

Select a check box next to a badge to modify or delete it.

Badge text

Type a short text string for the badge. For example, High risk.

To customize the value of a badge text, add a \$ prefix to it. For example, \$Risk. You can customize only the value of a badge text when it is prefixed with \$. For example, \$Risk=High Risk. You cannot customize a badge text if it is not prefixed with \$.

You might want to configure the `CustomLabels.properties` file to customize the value for the badge text. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Badge class

Select a specific CSS class from the list to apply to the badge text. You can customize a badge class, where you can specify your own styles to be displayed in the **Badge class** list. For example, a CSS class can consist of font type, size, color, or other formatting styles, which you can apply to the specified badge text.

You might want to customize a badge CSS style to suit your requirements. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Preview

A preview displays the badge text that is based on the badge class you selected.

Participants

Use this page to specify participant information. This page is displayed only if you are changing a manual service.

Participant type

Indicates the type of participant that you select. Possible participant types include:

- Administrator
- Service owner
- Manager
- User
- Group

Person name

Indicates the person's name. This field is displayed only when the **User** participant type is selected.

Group name

Indicates the group's name. This field is displayed only when the **Group** participant type is selected.

Escalation time in days

The amount of time in days the participant has to perform an activity before the activity is escalated.

Escalation participant type

Indicates the type of escalation participant that you select. Possible escalation participant types include:

- Administrator
- Service owner
- Manager
- User
- Group

Person name

Indicates the person's name. This field is displayed only when the **User** escalation participant type is selected.

Group name

Indicates the group's name. This field is displayed only when the **Group** escalation participant type is selected.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Messages

Optionally, use this page to change the contents of an email message to send when corresponding operations are performed. This page is displayed only for manual services.

This **Messages** page is available only when you select **Manual** from **Connection mode**. For information about Connection mode, see [“POSIX Solaris Profile: General Information” on page 80](#)

Messages table

Lists the email messages to send when corresponding operations are performed. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates the message that is selected.

Operation

Identifies the operation that must be performed to send the email message.

Subject

Identifies the subject of the email message.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Change** to change the contents of the selected message.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Reconciliation

Optionally, use this page to specify a reconciliation file. This page is displayed only if you are changing a manual service.

Reconcile supporting data only

Select this check box to reconcile only supporting data from the inputted CSV file. No account data is reconciled. Group information is added or updated in IBM Security Identity Manager, but accounts are not added or updated.

Reconciliation file

Identifies the name of the reconciliation file that you select. The file cannot contain binary attributes. If you include multivalued attributes, they must be represented by using multiple columns with the same attribute name.

You can use these buttons:

Browse

Click to navigate to the reconciliation file.

Upload file

Click to upload the reconciliation file to the system.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Change Message: Operation

Use this page to modify the contents of an e-mail message to send to the selected operation.

Subject

Specify the subject of the e-mail message.

Plaintext body

Specify the main content of the notification message in plaintext format. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Specify the XHTML body of the notification message. The content in this section can include images and hyperlinks.

Related information

For more information, see the [IBM Knowledge Center](#).

Set Up Account Reconciliation

Use this page to create, change, or delete a scheduled reconciliation.

Lists the reconciliation schedules for a service. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a schedule. To select one or more schedules, select the check box adjacent to the schedule. To select all schedules, select the check box at the top of the column.

Name

Identifies the name of a schedule. Click the name of the schedule to view or change its details.

Schedule

Provides interval and date information about a scheduled reconciliation.

Description

Provides additional information about the schedule.

Check policy during reconciliation

Indicates whether the policy is enforced on an account during reconciliation.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new schedule.

Change

Click to change the information for the selected schedule.

Delete

Click to delete the selected schedule.

Related information

For more information, see the [IBM Knowledge Center](#).

Set Up Account Reconciliation

Use this notebook to define account reconciliation information, schedule, and query a service. The tabs that are available for this notebook vary, depending on the service type.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to specify reconciliation information for a service.

Display name

Identifies the name of the reconciliation schedule for display purposes.

Description

Provides a description of the reconciliation schedule.

Lock service during reconciliation

Indicates whether other provisioning requests are queued until an active reconciliation completes.

Maximum duration (minutes)

Indicates the maximum amount of time in minutes that a reconciliation can run.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule

Use this page to schedule a reconciliation for the accounts on the managed resource.

The fields displayed vary, depending on the scheduling option that is selected. Select one of these schedule intervals to reconcile accounts for this service:

Daily

Reconciles accounts every day. After you select this option, click the clock icon to specify a time in the **At this time** field.

Weekly

Reconciles accounts once a week. After you select this option, select a day from the **On this day of the week** list, and then click the clock icon to specify a time in the **At this time** field.

Monthly

Reconciles accounts once a month. After you select this option, select a date from the **On this day of the month** list, and then click the clock icon to specify a time in the **At this time** field.

Hourly

Reconciles accounts once an hour. After you select this option, select a time from the **At this minute** list.

Annually - On a specific day of the year

Reconciles accounts on a specific date and time. After you select this option, select a month from the **Month** list. Then select a date from the **On this day of the month** list, and then click the clock icon to specify a time in the **At this time** field.

During a specific month

Reconciles accounts on a specific month, day, and time. After you select this option, select a month from the **Month** list. Then select a day from the **On this day of the week** list, and then click the clock icon to specify a time in the **At this time** field.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Query

Use this page to specify a reconciliation query.

Reconcile supporting data only

Indicates whether to reconcile supporting data from the managed resource instead of the actual accounts on the resource. For example, supporting data might be a list of groups defined on the resource.

Reconcile accounts that match this filter

Indicates valid LDAP search filter statements that select a list of accounts to reconcile.

Available attributes

Identifies attributes that are not processed during reconciliation.

Selected attributes

Identifies attributes that are included in processing during reconciliation.

You can use these buttons:

Add

Click to add an attribute to the query.

Remove

Click to remove an attribute from the query.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Query

Use this page to select a reconciliation query to reconcile all accounts or selected accounts.

Query

None

Includes all accounts in the reconciliation.

Use query from existing schedule

Select a query for the reconciliation from an existing schedule. The **Reconciliation Schedule** table displays the reconciliation schedules for a service. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the schedule that you want to use.

Name

Identifies the name of a schedule.

Schedule

Provides interval and date information about a scheduled reconciliation.

Description

Provides additional information about the schedule.

Define query

Specify an LDAP search filter for account attributes to include in a query.

Reconcile supporting data only

Indicates whether to reconcile supporting data from the managed resource instead of the actual accounts on the resource. For example, supporting data might be a list of groups defined on the resource.

Reconcile accounts that match this filter

Indicates valid LDAP search filter statements that select a list of accounts to reconcile.

Available attributes

Identifies attributes that are not processed during reconciliation.

Selected attributes

Identifies attributes that are included in processing during reconciliation.

You can use these buttons:

Add

Click to add an attribute to the query.

Remove

Click to remove an attribute from the query.

Click **Submit** to submit your request.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Action

Use this page to specify the policy enforcement action that occurs for an account that has a noncompliant attribute.

Mark

Sets a mark on an account that has a noncompliant attribute.

Suspend

Suspends an account that has a noncompliant attribute.

Correct

Replaces a noncompliant attribute on an account with the correct attribute.

Alert

Issues an alert for an account that has a noncompliant attribute.

Use Global Enforcement Action: <action>

Specifies a global enforcement action for an account that has a noncompliant attribute. The current global setting is displayed.

You can use these buttons:

Submit

Click to save the selection and continue to the next page. This button is displayed when **Mark, Suspend, Correct, or Use Global Enforcement Action** is selected as the enforcement action.

Continue

Click to save the selection and continue to the next page. This button is displayed only when **Alert** is selected as the enforcement action.

Related information

For more information, see the [IBM Knowledge Center](#).

Configure Policy Enforcement

Use this notebook to configure policy enforcement for a service.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to specify an alert, including participants, escalation intervals, and process types.

Alert name

Type a name to identify the alert.

Send compliance alert to

Select the participant type you want to receive the unattended compliance alert to-do items. Depending on which type of participant you select, one of these fields might be displayed:

User (with ITIM Account) name

Specify the user name for the participant. Click **Browse** to navigate to a list of user names, or click **Clear** to remove the currently specified user name.

This field is displayed only when you select **User (with ITIM Account) name** in the previous field.

Organizational role name

Specify the organizational role name for the participant. Click **Browse** to navigate to a list of role names, or click **Clear** to remove the currently specified role name.

This field is displayed only when you select **Organizational Role** in the previous field.

Custom participant script

Type an LDAP search filter. The search filter is the search criteria for getting the participants.

This field is displayed only when you select **Custom-Defined Participant** in the previous field.

Number of days to wait before escalating compliance alert

Type the number of days to elapse before the unattended compliance alert to-do items are escalated and sent to the escalation participant.

Escalate compliance alert to

Select the second-level participant type you want to receive the unattended compliance alert to-do items. Depending on which type of participant you select, one of these fields might be displayed:

User (with ITIM Account) name

Specify the user name for the participant. Click **Browse** to navigate to a list of user names, or click **Clear** to remove the currently specified user name.

This field is displayed only when you select **User (with ITIM Account) name** in the previous field.

Organizational role name

Specify the organizational role name for the participant. Click **Browse** to navigate to a list of role names, or click **Clear** to remove the currently specified role name.

This field is displayed only when you select **Organizational Role** in the previous field.

Custom participant script

Type an LDAP search filter. The search filter is the search criteria for getting the participants.

This field is displayed only when you select **Custom-Defined Participant** in the previous field.

Number of days after which the system will take corrective action

Type the maximum number of days that the compliance alert to-do items can remain unanswered. When the number of days specified in this field is reached, the associated accounts are automatically corrected with the suggested values in the compliance alert to-do item.

Process Types table

Lists the processes that generate a compliance alert. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Generate Alert

Specifies a process type. To select one or more process types, select the check box adjacent to the process type. To select all process types, select the check box at the top of the column.

If the process type is checked, an alert is generated. Otherwise, the noncompliance is automatically corrected. Correction can result in either the account being modified to a compliance state, or deletion of the account if no entitlement is defined for the owner of the account.

Process Type

Indicates the type of workflow process that generates a compliance alert to-do item.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click other tabs to specify additional information. Then, click **Submit** to submit your request.

Related information

For more information, see the [IBM Knowledge Center](#).

E-mail

Use this page to specify an alert e-mail.

Use default template

Select this check box to use the default e-mail template instead of the custom fields for the alert. If this option is selected, the custom fields are read-only.

Subject

Type the subject line of the e-mail notification.

Plain text body

Type the plain text body of the e-mail notification.

XHTML body

Specify the XHTML dynamic content of the e-mail notification.

Click other tabs to specify additional information. Then, click **Submit** to submit your request.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Groups on Service

Use this page to search for a group or access definition.

Group information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Group searches for groups in which the group name contains the text that is entered in the **Group information** field.

Access searches for the name of the access definition that is associated with the group that is entered in the **Group information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Groups and Access table

Lists the groups matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group or access definition to which the **Define Access** button applies. To select one or more group or access definitions, select the check box adjacent to the group or access definition. To select all groups or access definitions, select the check box at the top of the column.

Common Access

Specifies whether the access defined for the group is visible to users. If no access is defined, or if the group is not enabled for access, the column is empty. Your selection is saved immediately.

Group Name

Identifies the group's name.

Click the name of the group to view the group details.

Click the icon () adjacent to the group to show the tasks that can be performed on the group.

Use these menu items to perform a task on the selected group:

Define Access

Defines the group as an access.

Group Membership

Enables you to add users to, or remove users from, group membership.

Access Recertification Status

Identifies the recertification status for access definitions for the group.

Group Type

Displays the type of group, based on the group profile. For example, AIX types include AIX groups and AIX AIX.

Description

Displays information about the intended purpose of the group.

Access Name

Identifies the name of the access for the group. Click the access name for details about the access.

Access Type

Identifies the type of access, such as a shared folder.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Define Access

Click to define the group as an access.

Clear Access

Click to remove the group as an access.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Define Access

Use this notebook to define access for a group of users.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Information

Use the **Access Information** page to specify general information about the access, including the name, type, description, owner, and other business metadata for accesses.

Access name

Type a name to identify the access.

Access type

Select the type of access that is defined by the group.

Description

Provide more information about the access.

Access owner

Specify the user who has access ownership. To see a list of owners, click **Search**.

Display in Access List

Select this check box to include the access in the access list.

Display in Common Access list

Select this check box to include the access in a common access list that is visible to users.

Icon URL

Provide a uniform resource identifier (URI) string for the icon. A preview of the icon is displayed that is based on the following conditions:

- If an icon URL is not specified, and the category image exists, then the preview displays the category image. An information message is displayed that this image is used.
- If an icon URL is not specified, and the category image does not exist, then the preview displays a message that there is no image.
- If an icon URL is specified, then the referenced image is displayed.

For more information, see the [Customizing an access card in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Search terms

Type the search strings that you want to add to return specific search terms. You can use multiple values for the search terms.

Use these buttons for the search terms:

Add

Click to add a search term.


Delete

Click to delete one or more search terms.

Additional information

Displays information about the access card by default. It is a free form information about the access item that the administrator considers useful.

Badges

Specify one or more badges for an access item that is associated with this group. Click the twistie icon  next to **Badges** to specify one or more badges. You can add a maximum of five badges for an access item.

Use these buttons for the badges:

Add

Click to add a badge. The button becomes inactive after a maximum of five badges are assigned to an access item.

Remove

Click to remove a badge. The button is not active until a badge is added.

Select a check box next to a badge to modify or delete it.

Badge text

Type a short text string for the badge. For example, High risk.

To customize the value of a badge text, add a \$ prefix to it. For example, \$Risk. You can customize only the value of a badge text when it is prefixed with \$. For example, \$Risk=High Risk. You cannot customize a badge text if it is not prefixed with \$.

You might want to configure the `CustomLabels.properties` file to customize the value for the badge text. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Badge class

Select a specific CSS class from the list to apply to the badge text. You can customize a badge class, where you can specify your own styles to be displayed in the **Badge class** list. For example, a CSS class can consist of font type, size, color, or other formatting styles, which you can apply to the specified badge text.

You might want to customize a badge CSS style to suit your requirements. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Preview

A preview displays the badge text that is based on the badge class you selected.

Click other tabs to specify more information.

Related information

For more information, see the [IBM Knowledge Center](#).

Provisioning Options

Use this page to specify access approval and notification options.

Approval workflow

Specify whether no approval or specific approval is required to grant access.

Notify users when access is provisioned and available for use

Select this check box to ensure that users are notified when access is provisioned.

Notify users when access is de-provisioned

Select this check box to ensure that users are notified when access is de-provisioned.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Group Members

Use this page to add or remove accounts that are associated with a group.

Account information

Type the user ID or name of the user who owns the account in this field. If you do not know the name of the account that you want to find, you can type a portion of the name to display a list of accounts. If you do not type a value in this field or if you type an asterisk (*), and then click **Search**, the entire list of accounts is displayed as long as the number of accounts does not exceed the search limit.

Search by

Select the search category.

User ID searches for accounts with user IDs that contain the text that is entered in the **Search information** field.

Owner searches for accounts in which the full name of the account owner contains the text that is entered in the **Account information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Accounts table

Lists the accounts that match the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box next to the account. To select all accounts, select the check box at the top of the column.

State

Indicates the state of the group.

User ID

Identifies the user ID that is associated with the group. Click the user ID to review the account information.

Owner

Identifies the full name of the user who owns the account that is associated with the group. Click the name of the owner to view the personal profile of the user.

Ownership Type

Identifies the ownership of the account. The ownership type can be a default type of Device, Individual, System, or Vendor, or a custom ownership type.

Status

Indicates whether the account is active or inactive.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add accounts to the group.

Remove

Click to remove the selected accounts from the group

Add to Vault

Click to add the sponsored account to the credential vault so that the account can be shared. This function is available only if the Shared Access Module is installed.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Add Members

Use this page to add a group that has access to a specified account.

Account information

Type the user ID or name of the user who owns the account in this field. If you do not know the name of the account that you want to find, you can type a portion of the name to display a list of accounts. If you do not type a value in this field or if you type an asterisk (*), and then click **Search**, the entire list of accounts is displayed as long as the number of accounts does not exceed the search limit.

Search by

Select the search category.

User ID searches for accounts with user IDs that contain the text that is entered in the **Search information** field.

Owner searches for accounts in which the account owner's full name contains the text that is entered in the **Account information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Accounts table

Lists the accounts matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box adjacent to the account. To select all accounts, select the check box at the top of the column.

State

Indicates the state of the group.

User ID

Identifies the user ID that is associated with the group. Click the user ID to review the account information.

Owner

Identifies the full name of the user who owns the account that is associated with the group. Click the name of the owner to view the user's personal profile.

Status

Indicates whether the account is active or inactive.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Group Membership

Use this page to add or remove accounts that are associated with a group.

Account information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

User ID searches for accounts with user IDs that contain the text that is entered in the **Search information** field.

Owner searches for accounts in which the account owner's full name contains the text that is entered in the **Account information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Accounts table

Lists the accounts matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box adjacent to the account. To select all accounts, select the check box at the top of the column.

State

Indicates the state of the group.

User ID

Identifies the user ID that is associated with the group. Click the user ID to review the account information.

Owner

Identifies the full name of the user who owns the account that is associated with the group. Click the name of the owner to view the user's personal profile.

Status

Indicates whether the account is active or inactive.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add accounts to the group.

Remove

Click to remove the selected accounts from the group.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Recertification Status

Use this page to locate and recertify access to accounts that are associated with a group.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

User ID searches for access definitions with user IDs that contain the text that is entered in the **Search information** field.

Owner searches for access definitions in which the access owner's full name contains the text that is entered in the **Search information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Access table

Lists the current access definitions for the group. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an access definition. To select one or more access definitions, select the check box adjacent to the access definition. To select all access definitions, select the check box at the top of the column. Access definitions that have a status of Recertified or Admin Recertified cannot be selected.

User ID

Identifies the user ID for the access.

Owner

Identifies the name of the owner of the access. Click the name of the owner to view the user's personal profile.

Status

Indicates whether the access is active or inactive.

Recertification Status

Identifies the recertification status of the access. The possible recertification status values of the access definitions are:

- Recertified
- Admin Recertified
- Rejected and marked
- Never Recertified

Recertification Status Date

Indicates the date on which the recertification status of the access was last updated.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Recertify** to change the status of an access to Administrator Recertified.

Related information

For more information, see the [IBM Knowledge Center](#).

Account Information

Use this page to request an account for another user.

The pages that are displayed vary, depending on the type of service that you selected and by the authority that the system administrator has granted you.

The fields that are displayed on these pages also vary, depending on the type of service that you selected and by the authority that the system administrator has granted you.

The following topics define the default service attributes for the default services. For information about other service attributes, see your system administrator.

Related information

For more information, see the [IBM Knowledge Center](#).

AIX Default Attributes

For the AIX service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Access information page

UNIX Shell

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the read, write, and execute permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the access used by the account as a default change file mode value for the user home directory.

Administration choices(1) page

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as the secondary group of the user.

Groups that can use the su command on this user

Specify the name of the group that can use the UNIX **su** command on the user.

Groups to be administered

Specify the groups to administer.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before the date that a password expires that a warning is issued to the user.

Administrative roles

Specify the administrative roles for the user.

Additional mandatory methods for authenticating the user

Specify other mandatory authentication methods.

Additional optional methods for authenticating the user

Specify other optional authentication methods.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices(2) page**Audit class**

Specify the list of audit classes for the user.

Allow user to execute daemon process?

Select this check box to enable the user to run daemon processes on the system.

Allow user to log in to the system?

Select this check box to enable the user to log directly into the system.

Allow user to remotely login to the system?

Select this check box to enable the user to log into the system remotely.

Can another user switch user to this user?

Select this check box to enable another user to use the UNIX **su** command on this user.

Is this user an administrator?

Select this check box to designate the user as an administrator of the system.

Trusted path status

Select the default trusted path status for the account.

always

Specifies that the user that is confined to the trusted path.

/notsh

Specifies that the user session ends if the secure attention key (SAK) signal is detected.

nosak

Specifies that the SAK key is disabled.

on

Specifies that the standard trusted path management is used.

Soft limit for largest core size

Specify the soft limit for the largest core file that the user's process can create.

Soft limit for maximum amount of CPU utilization

Specify the soft limit for the largest amount of system unit time (in seconds) that the user's process can use.

Soft limit for largest data segment

Specify the soft limit for the largest process data segment for the user's process.

Soft limit for largest file size

Specify the soft limit for the largest file that the user's process can create or extend.

Soft limit for largest stack segment

Specify the soft limit for the largest process stack segment for the user's process.

Largest core size

Specify the largest core file that the user's process can create.

Maximum CPU utilization

Specify the largest amount of system unit time (in seconds) that the user's process can use.

Largest data segment

Specify the largest process data segment for the user's process.

Largest file size

Specify the largest file that the user's process can create or extend.

Largest stack segment

Specify the largest amount of physical memory that the user's process can allocate.

Allowed login time

Specify the days and times that the user is allowed to access the system.

Allowed number of login retries before locking the account

Specify the number of failed login attempts before the account is locked.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in weeks) that the account can remain active after the password for the account has expired.

Minimum alphabetic characters in password

Specify the minimum number of alphabetic characters that must be included in the password for the account.

Minimum difference between the current and last password

Specify the minimum number of characters that are required in a new password that were not in the old password.

Maximum number of characters that can be repeated in a password

Specify the maximum number of characters in a password that can be repeated.

Minimum length of the password

Specify the minimum length of the password.

Password restriction methods

Specify password restriction methods to the account.

Password dictionaries used to restrict passwords

Specify the password dictionary files that are used to restrict which passwords can be used by the account.

Number of previous passwords that cannot be reused

Specify the number of passwords to be kept in the password history.

Account last accessed on

Specify a value for the last access date and time.

Valid terminals allowed to access the account

Specify which terminals can log in using this account.

System authentication mechanism for the user

Specify the authentication mechanism the system uses to authenticate the user.

Authentication registry where the user is administered

Specify the registry that is used for authenticating the user.

Related information

For more information, see the [IBM Knowledge Center](#).

HP-UX Default Attributes

For the HP-UX service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX Shell**

Specify a default command shell for the account.

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the names of the groups to use as secondary groups of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices page**Password warning age**

Specify the number of days before the date that a password expires that a warning is sent to the user.

Maximum number of days (weeks for AIX) the account can remain valid after the password expires

Specify the maximum time that the account can remain active after the password for the account has expired.

Number of days the account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allowed number of login retries before locking the account

Specify the number of login attempts that can occur before the account is locked.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Although you can specify a time, this feature is disabled and you can only set an account expiration date. Alternatively, select **Never** to set the account to never expire.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP Default Attributes

For the LDAP service type, IBM Security Identity Manager provides a set of default attributes.

User page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

User Container

Click **Search** to search for the location in the LDAP tree where you want to add the user.

Full name

Type a value for distinguishing users, for example, the full name of the user.

Preferred user ID

Type the user ID. This determines the default user ID that new accounts and access use when they are created.

Last name

Type the last name of the user.

First name

Type the first name of the user.

Initials

Type the initials of the user.

E-mail address

Type the e-mail address of the user.

Display name

Type the name of the user that you want to be displayed in the IBM Security Identity Manager interface.

Description

Type information about the intended purpose of the account.

Home telephone number

Type the home telephone number of the user.

Mobile telephone number

Type the mobile telephone number of the user.

Pager

Type the pager number of the user.

Business page

Title

Type the business title of the user.

Employee number

Type the employee number of the user.

Employee type

Type the employment specification of the user, such as regular, contractor, or business partner.

Manager

Type the name of the manager of the user.

Administrative assistant

Type the name of the assistant of the user.

Business category

Type the business category type of the user.

Department number

Type the department number of the user.

Telephone number

Type the business telephone number of the user.

Fax number

Type the business fax number of the user.

Postal address

Type the business postal address of the user.

Office number

Type the office location of the user.

Location name

Type the locale of the user.

Address page**Registered address**

Type the registered address of the user.

Street

Type the street name of the registered address.

State

Type the state in which the user resides.

Destination indicator

Type an applicable destination indicator.

Physical delivery office name

Type the name of the physical address.

Home address

Type the home address of the user.

Postal code

Type the postal code of the user.

Post office box

Type the post office box number of the user.

Preferred delivery method

Type the preferred method of delivery of the user.

Other page**Driver license**

Type the driver's license number of the user.

Preferred language

Type the preferred language of the user.

Teletex terminal ID

Type the teletex terminal ID of the user.

Telex number

Type the teletex number of the user.

Related information

[For more information, see the IBM Knowledge Center.](#)

Linux Default Attributes

For the Linux service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page

UNIX shell

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

This field is not supported for Linux operating systems.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices pages

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Password warning age

Specify the number of days before expiration that a password expiration warning is issued to the user.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in days) that the account can remain active after the password for the account has expired.

Related information

For more information, see the [IBM Knowledge Center](#).

Solaris Default Attributes

For the Solaris service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX Shell**

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices page**Force a password change?**

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before expiration that a password expiration warning is issued to the user.

Number of days account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allow at jobs?

Select this check box to allow this account to run an *at* job.

Allow cron jobs?

Select this check box to allow this account to run a *cron* job.

Related information

For more information, see the [IBM Knowledge Center](#).

Accounts

Use this page to find the account that you want to manage.

Account information

Type the user ID or name of the user who owns the account in this field. If you do not know the name of the account that you want to find, you can type a portion of the name to display a list of accounts. If you do not type a value in this field or if you type an asterisk (*), and then click **Search**, the entire list of accounts is displayed as long as the number of accounts does not exceed the search limit.

Search by

Select the search category.

User ID searches for user IDs that contain the text that is entered in the **Account information** field.

Owner searches for owner names that contain the text that is entered in the **Account information** field.

Ownership type

Select an ownership type from the list to display accounts with that ownership type. The list contains default and custom ownership types. If you select an ownership type, the search is based on that ownership type.

All searches for all the accounts.

Device searches for the device accounts.

Individual searches for the individual accounts.

System searches for the system accounts.

Vendor searches for the vendor accounts.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Accounts table

Lists the accounts that match the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box next to the account. To select all accounts, select the check box at the top of the column.

State

Indicates the compliancy state of the account.

Blank (no symbol)

Indicates that the account is compliant.



Indicates that the account was returned from a reconciliation, which means it was not checked against the existing provisioning policies.



Indicates that the account can exist for the user, but that one or more of the account attributes does not comply with the existing provisioning policies.



Indicates either of the following:


The account is not supposed to exist because the user is not allowed to have access to the specified resource.

The provisioning policy is not defined for the resource.

User ID

Identifies the user ID for the account.

Click the user ID to review the account information.

Click the icon () next to the account to show the tasks that can be performed on the account.

Use these menu items to perform a task on the selected account:

Change

Changes the information for the selected account.

Delete

Deletes the selected account.

Change Password

Changes the password for the account. The account must be assigned to a user for this option to be available.

Suspend

Suspends the selected account. The account must be active for this option to be available.

Restore

Restores the selected account. The account must be inactive for this option to be available. Depending on how your system administrator configured the system, you might be prompted to enter a password.

Assign to User

Assigns the selected account to a specified user. A value of None in the **Owner** column indicates that the account is an orphan account.

Orphan

Makes the account an orphan account. The account must be already assigned to a user for this option to be available.

Add to Vault

Click to add the sponsored account to the credential vault so that the account can be shared. This function is available only if the Shared Access Module is installed. This function is disabled if the credentials exist in the vault. You cannot add individual, inactive, or orphan accounts to the credential vault.

Owner

Identifies the name of the owner of the account. Click the name of the owner to view the user personal profile. A value of None indicates that the account is an orphan account.

Ownership Type

Identifies the ownership type of the account. A value of None is displayed if no owner is assigned to the account. To assign or change the ownership type, use the **Assign to User** task. After selecting an owner, you will be prompted to select Ownership Type if the selected user is entitled for more than one ownership type.

Status

Identifies the status of the account. Accounts can be active or inactive. Contact your help desk assistant, the service owner, or your system administrator to restore an inactive account.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Request

Click to request an account.

Change

Click to change the information for the selected account.

Delete

Click to delete the selected account.

Suspend

Click to suspend the selected account.

Restore

Click to restore the selected account. Depending on how your system administrator configured the system, you might be prompted to enter a password.

Assign to User

Click to assign the selected account to a specified user.

Add to Vault

Click to add the sponsored account to the credential vault so that the account can be shared. This function is available only if the Shared Access Module is installed.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Noncompliant Account Attributes

Use this page to view an account that has one or more attributes with values that do not comply with an existing policy.

Attribute

Identifies the name of an attribute.

Non-Compliant Value

Provides the value that does not comply with an existing policy. If an attribute value is empty, the suggested value is used. If there is no suggested value, the noncompliant value is removed when you change the account.

Suggested Value

Provides the compliant value for the attribute based on the policy evaluation.

Related information

For more information, see the [IBM Knowledge Center](#).

Change an Account

Use this notebook to change an account for another user.

The pages that are displayed in the notebook vary, depending on the type of service that you selected and by the authority that the system administrator has granted you. For example, for the AIX service, the Account information, Access information, and Administration choices pages might be displayed.

The fields that are displayed on these pages also vary, depending on the type of service that you selected and by the authority that the system administrator has granted you.

Actions

Submit Now

Click **Submit Now** to implement your changes.

Schedule Submission

Click **Schedule Submission** to specify a date and time for the changes to take effect.

Cancel

Click **Cancel** to discard any changes you made.

Default service attributes for default services

The following topics define the default service attributes for the default services. For information about other service attributes, see your system administrator.

Related information

For more information, see the [IBM Knowledge Center](#).

AIX Default Attributes

For the AIX service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Access information page

UNIX Shell

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the read, write, and execute permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the access used by the account as a default change file mode value for the user home directory.

Administration choices(1) page

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as the secondary group of the user.

Groups that can use the su command on this user

Specify the name of the group that can use the UNIX **su** command on the user.

Groups to be administered

Specify the groups to administer.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before the date that a password expires that a warning is issued to the user.

Administrative roles

Specify the administrative roles for the user.

Additional mandatory methods for authenticating the user

Specify other mandatory authentication methods.

Additional optional methods for authenticating the user

Specify other optional authentication methods.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices(2) page

Audit class

Specify the list of audit classes for the user.

Allow user to execute daemon process?

Select this check box to enable the user to run daemon processes on the system.

Allow user to log in to the system?

Select this check box to enable the user to log directly into the system.

Allow user to remotely login to the system?

Select this check box to enable the user to log into the system remotely.

Can another user switch user to this user?

Select this check box to enable another user to use the UNIX **su** command on this user.

Is this user an administrator?

Select this check box to designate the user as an administrator of the system.

Trusted path status

Select the default trusted path status for the account.

always

Specifies that the user that is confined to the trusted path.

/notsh

Specifies that the user session ends if the secure attention key (SAK) signal is detected.

nosak

Specifies that the SAK key is disabled.

on

Specifies that the standard trusted path management is used.

Soft limit for largest core size

Specify the soft limit for the largest core file that the user's process can create.

Soft limit for maximum amount of CPU utilization

Specify the soft limit for the largest amount of system unit time (in seconds) that the user's process can use.

Soft limit for largest data segment

Specify the soft limit for the largest process data segment for the user's process.

Soft limit for largest file size

Specify the soft limit for the largest file that the user's process can create or extend.

Soft limit for largest stack segment

Specify the soft limit for the largest process stack segment for the user's process.

Largest core size

Specify the largest core file that the user's process can create.

Maximum CPU utilization

Specify the largest amount of system unit time (in seconds) that the user's process can use.

Largest data segment

Specify the largest process data segment for the user's process.

Largest file size

Specify the largest file that the user's process can create or extend.

Largest stack segment

Specify the largest amount of physical memory that the user's process can allocate.

Allowed login time

Specify the days and times that the user is allowed to access the system.

Allowed number of login retries before locking the account

Specify the number of failed login attempts before the account is locked.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in weeks) that the account can remain active after the password for the account has expired.

Minimum alphabetic characters in password

Specify the minimum number of alphabetic characters that must be included in the password for the account.

Minimum difference between the current and last password

Specify the minimum number of characters that are required in a new password that were not in the old password.

Maximum number of characters that can be repeated in a password

Specify the maximum number of characters in a password that can be repeated.

Minimum length of the password

Specify the minimum length of the password.

Password restriction methods

Specify password restriction methods to the account.

Password dictionaries used to restrict passwords

Specify the password dictionary files that are used to restrict which passwords can be used by the account.

Number of previous passwords that cannot be reused

Specify the number of passwords to be kept in the password history.

Account last accessed on

Specify a value for the last access date and time.

Valid terminals allowed to access the account

Specify which terminals can log in using this account.

System authentication mechanism for the user

Specify the authentication mechanism the system uses to authenticate the user.

Authentication registry where the user is administered

Specify the registry that is used for authenticating the user.

Related information

For more information, see the [IBM Knowledge Center](#).

HP-UX Default Attributes

For the HP-UX service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX Shell**

Specify a default command shell for the account.

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the names of the groups to use as secondary groups of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices page**Password warning age**

Specify the number of days before the date that a password expires that a warning is sent to the user.

Maximum number of days (weeks for AIX) the account can remain valid after the password expires

Specify the maximum time that the account can remain active after the password for the account has expired.

Number of days the account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allowed number of login retries before locking the account

Specify the number of login attempts that can occur before the account is locked.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Although you can specify a time, this feature is disabled and you can only set an account expiration date. Alternatively, select **Never** to set the account to never expire.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP Default Attributes

For the LDAP service type, IBM Security Identity Manager provides a set of default attributes.

User page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

User Container

Click **Search** to search for the location in the LDAP tree where you want to add the user.

Full name

Type a value for distinguishing users, for example, the full name of the user.

Preferred user ID

Type the user ID. This determines the default user ID that new accounts and access use when they are created.

Last name

Type the last name of the user.

First name

Type the first name of the user.

Initials

Type the initials of the user.

E-mail address

Type the e-mail address of the user.

Display name

Type the name of the user that you want to be displayed in the IBM Security Identity Manager interface.

Description

Type information about the intended purpose of the account.

Home telephone number

Type the home telephone number of the user.

Mobile telephone number

Type the mobile telephone number of the user.

Pager

Type the pager number of the user.

Business page**Title**

Type the business title of the user.

Employee number

Type the employee number of the user.

Employee type

Type the employment specification of the user, such as regular, contractor, or business partner.

Manager

Type the name of the manager of the user.

Administrative assistant

Type the name of the assistant of the user.

Business category

Type the business category type of the user.

Department number

Type the department number of the user.

Telephone number

Type the business telephone number of the user.

Fax number

Type the business fax number of the user.

Postal address

Type the business postal address of the user.

Office number

Type the office location of the user.

Location name

Type the locale of the user.

Address page**Registered address**

Type the registered address of the user.

Street

Type the street name of the registered address.

State

Type the state in which the user resides.

Destination indicator

Type an applicable destination indicator.

Physical delivery office name

Type the name of the physical address.

Home address

Type the home address of the user.

Postal code

Type the postal code of the user.

Post office box

Type the post office box number of the user.

Preferred delivery method

Type the preferred method of delivery of the user.

Other page**Driver license**

Type the driver's license number of the user.

Preferred language

Type the preferred language of the user.

Teletex terminal ID

Type the teletex terminal ID of the user.

Telex number

Type the teletex number of the user.

Related information

For more information, see the [IBM Knowledge Center](#).

Linux Default Attributes

For the Linux service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX shell**

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

This field is not supported for Linux operating systems.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices pages

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Password warning age

Specify the number of days before expiration that a password expiration warning is issued to the user.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in days) that the account can remain active after the password for the account has expired.

Related information

For more information, see the [IBM Knowledge Center](#).

Solaris Default Attributes

For the Solaris service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page

UNIX Shell

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices page**Force a password change?**

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before expiration that a password expiration warning is issued to the user.

Number of days account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allow at jobs?

Select this check box to allow this account to run an *at* job.

Allow cron jobs?

Select this check box to allow this account to run a *cron* job.

Related information

For more information, see the [IBM Knowledge Center](#).

Account Recertification Status

Use this page to view the recertification status of accounts and to override the recertification state, if required. For example, accounts that have been rejected through normal recertification processes can be set to the Admin Recertified state.

Account information

Type the user ID or name of the user who owns the account in this field. If you do not know the name of the account that you want to find, you can type a portion of the name to display a list of accounts. If you do not type a value in this field or if you type an asterisk (*), and then click **Search**, the entire list of accounts is displayed as long as the number of accounts does not exceed the search limit.

Search by

Select the search category.

User ID searches for accounts with user IDs that contain the text that is entered in the **Account information** field.

Owner searches for accounts in which the account owner's full name contains the text that is entered in the **Account information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Accounts table

Lists the accounts matching the specified search criteria. This table also displays related information and recertification status of accounts. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box adjacent to the account. To select all accounts, select the check box at the top of the column.. Accounts that have a status of Recertified or Admin Recertified cannot be selected.

User ID

Identifies the user ID for the account. Click the user ID to view the account information for the user ID.

Owner

Identifies the name of the owner of the account. Click the name of the owner to view the personal, business, and contact information for the user.

Status

Indicates whether the account is active or inactive.

Recertification Status

Identifies the recertification status of the account. The possible recertification status values of the accounts are:

- Recertified
- Admin Recertified
- Rejected and suspended
- Rejected and marked
- Never Recertified

Recertification Status Date

Indicates the date on which the recertification status of the account was last updated.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Recertify

Click to change the status of an account to Admin Recertified.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Confirm

Use this page to confirm recertification of the selected accounts.

Specify a justification for performing the administrative recertification of the accounts in the **Justification** field. This information is stored in a log that can be reported on at a later date.

Click **Recertify** to perform the recertification action on the accounts.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Account Defaults

Select an Account Attribute

Use this page to add, change, or remove the default account attributes for a service instance.

When you define account defaults for a service, any defaults that are defined for that service's type are pre-populated into the table. After the account defaults are saved for the service, they override the account defaults that are defined for the service's type.

Use the global account defaults for the service type

Select this check box to use the global account defaults for the service type instead of adding an attribute default to the service type.

Account Attributes table

Lists the attributes that are associated with the account for the given service instance. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account attribute. To select one or more account attributes, select the check box adjacent to the account attribute. To select all account attributes, select the check box at the top of the column.

Account Attribute

Identifies the name of the attributes associated with the service.

Template Value

Indicates the default value of the account attribute.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add an attribute default to the service type.

Change (Basic)

Click to change the selected attribute.

Change (Advanced)

Click to change the selected attribute using JavaScript to define the account default.

Remove

Click to remove the selected attribute.

Related information

For more information, see the [IBM Knowledge Center](#).

Select an Attribute to Default

Use this page to specify default values for attributes that are associated with an account.

Attributes table

Lists the attributes that are associated with the account for the given service instance. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates the account attribute to which the **Add** and **Add (Advanced)** buttons apply.

Attribute name

Identifies the name of the attribute.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a default value for the selected attribute.

Add (Advanced)

Click to add a script that specifies a default value for the selected attribute.

Related information

For more information, see the [IBM Knowledge Center](#).

Set Default for Attribute Name

Use this page to specify or change the default value of an attribute. The default value applies to accounts associated with the specified service instance.

The fields that are displayed on this page vary, depending on the type of the attribute as specified in the Form Designer.

This page might not display the existing default value for the attribute if the default is an advanced value. Click **OK** to replace the existing value with the value on this page.

Attributes are validated against constraints in the Form Designer. However, an attribute that is a text area or text field, such as a description or comment attribute, is not validated. For example, in AIX, the Gecos (comments) attribute is not validated.

Related information

For more information, see the [IBM Knowledge Center](#).

AIX Default Attributes

For the AIX service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Access information page**UNIX Shell**

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the read, write, and execute permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the access used by the account as a default change file mode value for the user home directory.

Administration choices(1) page

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as the secondary group of the user.

Groups that can use the su command on this user

Specify the name of the group that can use the UNIX **su** command on the user.

Groups to be administered

Specify the groups to administer.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before the date that a password expires that a warning is issued to the user.

Administrative roles

Specify the administrative roles for the user.

Additional mandatory methods for authenticating the user

Specify other mandatory authentication methods.

Additional optional methods for authenticating the user

Specify other optional authentication methods.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices(2) page

Audit class

Specify the list of audit classes for the user.

Allow user to execute daemon process?

Select this check box to enable the user to run daemon processes on the system.

Allow user to log in to the system?

Select this check box to enable the user to log directly into the system.

Allow user to remotely login to the system?

Select this check box to enable the user to log into the system remotely.

Can another user switch user to this user?

Select this check box to enable another user to use the UNIX **su** command on this user.

Is this user an administrator?

Select this check box to designate the user as an administrator of the system.

Trusted path status

Select the default trusted path status for the account.

always

Specifies that the user that is confined to the trusted path.

/notsh

Specifies that the user session ends if the secure attention key (SAK) signal is detected.

nosak

Specifies that the SAK key is disabled.

on

Specifies that the standard trusted path management is used.

Soft limit for largest core size

Specify the soft limit for the largest core file that the user's process can create.

Soft limit for maximum amount of CPU utilization

Specify the soft limit for the largest amount of system unit time (in seconds) that the user's process can use.

Soft limit for largest data segment

Specify the soft limit for the largest process data segment for the user's process.

Soft limit for largest file size

Specify the soft limit for the largest file that the user's process can create or extend.

Soft limit for largest stack segment

Specify the soft limit for the largest process stack segment for the user's process.

Largest core size

Specify the largest core file that the user's process can create.

Maximum CPU utilization

Specify the largest amount of system unit time (in seconds) that the user's process can use.

Largest data segment

Specify the largest process data segment for the user's process.

Largest file size

Specify the largest file that the user's process can create or extend.

Largest stack segment

Specify the largest amount of physical memory that the user's process can allocate.

Allowed login time

Specify the days and times that the user is allowed to access the system.

Allowed number of login retries before locking the account

Specify the number of failed login attempts before the account is locked.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in weeks) that the account can remain active after the password for the account has expired.

Minimum alphabetic characters in password

Specify the minimum number of alphabetic characters that must be included in the password for the account.

Minimum difference between the current and last password

Specify the minimum number of characters that are required in a new password that were not in the old password.

Maximum number of characters that can be repeated in a password

Specify the maximum number of characters in a password that can be repeated.

Minimum length of the password

Specify the minimum length of the password.

Password restriction methods

Specify password restriction methods to the account.

Password dictionaries used to restrict passwords

Specify the password dictionary files that are used to restrict which passwords can be used by the account.

Number of previous passwords that cannot be reused

Specify the number of passwords to be kept in the password history.

Account last accessed on

Specify a value for the last access date and time.

Valid terminals allowed to access the account

Specify which terminals can log in using this account.

System authentication mechanism for the user

Specify the authentication mechanism the system uses to authenticate the user.

Authentication registry where the user is administered

Specify the registry that is used for authenticating the user.

Related information

For more information, see the [IBM Knowledge Center](#).

HP-UX Default Attributes

For the HP-UX service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX Shell**

Specify a default command shell for the account.

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the names of the groups to use as secondary groups of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices page**Password warning age**

Specify the number of days before the date that a password expires that a warning is sent to the user.

Maximum number of days (weeks for AIX) the account can remain valid after the password expires

Specify the maximum time that the account can remain active after the password for the account has expired.

Number of days the account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allowed number of login retries before locking the account

Specify the number of login attempts that can occur before the account is locked.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Although you can specify a time, this feature is disabled and you can only set an account expiration date. Alternatively, select **Never** to set the account to never expire.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP Default Attributes

For the LDAP service type, IBM Security Identity Manager provides a set of default attributes.

User page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

User Container

Click **Search** to search for the location in the LDAP tree where you want to add the user.

Full name

Type a value for distinguishing users, for example, the full name of the user.

Preferred user ID

Type the user ID. This determines the default user ID that new accounts and access use when they are created.

Last name

Type the last name of the user.

First name

Type the first name of the user.

Initials

Type the initials of the user.

E-mail address

Type the e-mail address of the user.

Display name

Type the name of the user that you want to be displayed in the IBM Security Identity Manager interface.

Description

Type information about the intended purpose of the account.

Home telephone number

Type the home telephone number of the user.

Mobile telephone number

Type the mobile telephone number of the user.

Pager

Type the pager number of the user.

Business page**Title**

Type the business title of the user.

Employee number

Type the employee number of the user.

Employee type

Type the employment specification of the user, such as regular, contractor, or business partner.

Manager

Type the name of the manager of the user.

Administrative assistant

Type the name of the assistant of the user.

Business category

Type the business category type of the user.

Department number

Type the department number of the user.

Telephone number

Type the business telephone number of the user.

Fax number

Type the business fax number of the user.

Postal address

Type the business postal address of the user.

Office number

Type the office location of the user.

Location name

Type the locale of the user.

Address page**Registered address**

Type the registered address of the user.

Street

Type the street name of the registered address.

State

Type the state in which the user resides.

Destination indicator

Type an applicable destination indicator.

Physical delivery office name

Type the name of the physical address.

Home address

Type the home address of the user.

Postal code

Type the postal code of the user.

Post office box

Type the post office box number of the user.

Preferred delivery method

Type the preferred method of delivery of the user.

Other page**Driver license**

Type the driver's license number of the user.

Preferred language

Type the preferred language of the user.

Teletex terminal ID

Type the teletex terminal ID of the user.

Telex number

Type the teletex number of the user.

Related information

For more information, see the [IBM Knowledge Center](#).

Linux Default Attributes

For the Linux service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX shell**

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

This field is not supported for Linux operating systems.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices pages

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Password warning age

Specify the number of days before expiration that a password expiration warning is issued to the user.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in days) that the account can remain active after the password for the account has expired.

Related information

For more information, see the [IBM Knowledge Center](#).

Solaris Default Attributes

For the Solaris service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page

UNIX Shell

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices page**Force a password change?**

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before expiration that a password expiration warning is issued to the user.

Number of days account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allow at jobs?

Select this check box to allow this account to run an *at* job.

Allow cron jobs?

Select this check box to allow this account to run a *cron* job.

Related information

For more information, see the [IBM Knowledge Center](#).

Set Default for Attribute Name

Use this page to specify a script that defines the account default.

Script

Type the JavaScript code used to define the account default.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a User Attribute

Use this page to select attributes for the account.

User Type

Select a user type from the list. Available user types are Person and Business Partner Person.

Attributes table

Lists the attributes that are associated with the account. The list of attributes varies, depending on the type of user that you select.

Select

Indicates the user attribute that is selected.

Attribute

Identifies the name of the attribute.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select an Ownership Type

Use this page to select an ownership type or account category for the account you want to request.

Ownership Type table

Lists the ownership types. The table contains these columns:

Select

Select to specify an ownership type.

Ownership Type

Identifies the ownership type for an account, such as:

Device

Individual

Individual/Category1

System

Vendor

Note: The provisioning policy entitlements control the ownership types that are available for the account.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Organization Structure

Manage Organization Structure

Use this page to create, change, or delete business units, locations, and other components in the business structure tree.

Click the expand (+) icon to expand any subordinate elements in the **Root Organization** tree. Click the icon (▸) adjacent to each element to see tasks that are available. Click an element in the tree to view more details, or change the element. You must be authorized to see details or change an element. The tree contains these available types:

Organization

Identifies the top of an organizational hierarchy, which might contain subsidiary entities such as organization units, business partner organization units, and locations. This is the parent node at the top of the node tree.

Organization Unit

Identifies a subsidiary part of an organization, such as a division or department. An organization unit can be subordinate to any other container, such as organization, organization unit, location, and business partner organization.

Business Partner Organization Unit

Identifies a business partner organization, which is typically a company outside your organization that has an affiliation, such as a supplier, customer, or contractor.

Location

Identifies a container that is different geographically, but contained within an organization entity.

Admin Domain

Identifies a subsidiary part of an organization as a separate entity with its own policies, services, and access control items, including an administrator whose actions and views are restricted to that domain.

You can use these choices:

Create Organization

Click to create the highest node in the organization tree.

Create Admin Domain

Click to create an administrative domain.

Create Business Partner Unit

Click to create a subordinate business partner unit.

Create Location

Click to create a location.

Create Organizational Unit

Click to create a subordinate business unit.

Change

Click to change the specifications for a target node in the tree.

Delete

Click to delete a target node in the tree. You cannot delete a node that has child nodes.

Transfer

Click to transfer a business unit. You can transfer a business unit to an existing organization unit that is under the same organization root. Optionally, you can also create a new business unit and then transfer an existing business unit for people and roles. Following are a few restrictions for business unit transfer activity:

- Business unit cannot be transferred across different organization hierarchy.
- Business unit that contains objects that are related to services and policies cannot be transferred.
- Business unit that contains customized Access Control Item (ACI), cannot be transferred.
- Business unit to be transferred must contain an ACI granted for the Modify operation.
- Business unit cannot be transferred to a child of original business unit to be transferred.
- Business unit that contains a subtree, cannot be transferred.

Related information

For more information, see the [IBM Knowledge Center](#).

Organization Details

Use this page to specify an organization as the parent node in a hierarchy.

Organization name

Type the name of the organization.

Description

Type additional information to identify the organization.

Related information

For more information, see the [IBM Knowledge Center](#).

Admin Domain Details

Use this page to specify the name and other details for an admin domain in the organization.

The fields you use to specify an admin domain vary, depending on your site customization. If you do not have access control item permission to change a field, its value is in read-only mode.

Admin domain name

Type the domain name of the dependent unit.

Description

Type additional information to identify the purpose of the dependent unit.

Administrator

Select the administrator who is responsible for the unit. Click **Search** to locate an administrator.

Related information

[For more information, see the IBM Knowledge Center.](#)

Business Partner Unit Details

Use this page to specify the name and other details for a business partner unit in the organization.

The fields you use to specify a business partner unit vary, depending on your site customization. If you do not have access control item permission to change a field, its value is in read-only mode.

Business partner name

Type the name of the dependent unit.

Sponsor

Select the appropriate sponsor for the unit. Click **Search** to locate a person who is a sponsor.

Related information

[For more information, see the IBM Knowledge Center.](#)

Location Details

Use this page to specify the name and other details for a location within the organization.

The fields you use to specify a location vary, depending on your site customization. If you do not have access control item permission to change a field, its value is in read-only mode.

Location name

Type the location of the dependent unit.

Description

Type additional information to identify the purpose of the dependent unit.

Supervisor

Select the supervisor who is responsible for the unit. Click **Search** to locate a supervisor.

Related information

[For more information, see the IBM Knowledge Center.](#)

Organizational Unit Details

Use this page to specify the name and other details for an organizational unit within the organization.

The fields you use to specify an organization unit vary, depending on your site customization. If you do not have access control item permission to change a field, its value is in read-only mode.

Organizational unit name

Type the name of the dependent unit.

Description

Type additional information to identify the purpose of the dependent unit.

Supervisor

Select the supervisor who is responsible for the unit. Click **Search** to locate a person who is a supervisor.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Users

Select a User

Use this page to search for a user that you want to manage.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select an attribute from the list. All searchable attributes and the personal profile are included in this list. If you select an attribute, the search is based on that attribute. If you select **Entire profile**, the search is based on all attributes associated with the user.

Last Name searches for the user's last name.

Full Name searches for the user's full name.

E-mail Address searches for the user's e-mail address.

Entire Profile searches all attributes associated with the user.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Include individual accounts when suspending, restoring, or deleting users

Select the check box to suspend, restore, or delete all of the individual accounts associated with the user that you select. Sponsored accounts associated with the user must be handled through the accounts table.

If the user is deleted only the individual accounts associated with the user are deleted. The associated sponsored accounts are not deleted. The sponsored accounts become orphaned accounts. You can access these orphaned accounts through the Manage Services utility.

The Restore option is disabled when:

- More than one user is selected.
- A single user is selected and the password rules for the user accounts conflict.


Users table

Lists the users matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box next to the user. To select all users, select the check box at the top of the column.

Name

Identifies a value for distinguishing a user, such as the user's full name. Click the name of the user to view the user's personal profile. Click the icon () next to the name to display a menu containing tasks that can be performed for the user. The menu can contain these functions, depending on the system configuration:

Change

Click to change the personal profile for the selected user.

Delete

Click to remove the selected user from the system. All ITIM Service accounts associated with the user are deleted. All other accounts associated with the user become orphan accounts.

Change Passwords

Click to change the passwords for the selected user.

Reset Passwords

Click to reset the passwords for the selected user.

Suspend

Click to make the selected user inactive. Suspension does not remove the user from the system.

Restore

Click to make the selected inactive user active. Depending on how your system administrator has configured the system, you might be prompted to enter a password.

Delegate Activities

Click to delegate activities to the selected user.

Request Accounts

Click to request accounts for the selected user.

Accounts

Click to view and change accounts for the selected user.

Request Access

Click to request access for the selected user.

Access

Click to view and change access for the selected user.

Recertify

Click to run a recertification policy for the selected user. Only system administrators can perform this task.

E-mail Address

Identifies the user e-mail address.

Custom Display

Identifies a custom display attribute.

Business Unit

Identifies the business unit. Click the link for more information about the business unit.

Status

Identifies the user status.

Users are either active or inactive. A user must be active to log in to the system. A user becomes inactive when they are suspended. The suspended user still exists, but cannot access the system. System administrators can restore inactive users.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a user.

Change

Click to change the personal profile for the selected user.

Delete

Click to remove the selected user from the system.

Suspend

Click to make the selected user inactive. Suspending does not remove the user from the system.

Restore

Click to make the selected inactive user active. Depending on how your system administrator has configured the system, you might be prompted to enter a password.

Transfer

Click to transfer the selected user to a particular business unit.

Refresh

Click to update items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Select User Type

Use this page to select the type of user you want to create. For example, a user type might be a business partner.

Business unit

Select the business unit. The types of users that are displayed in the table depend on the business unit you have selected. To select a business unit, click **Search**.

User Type table

Lists the exclusion rules. The table contains these columns:

Select

Select to specify a user type.

User Type

Identifies the name of a type of user, such as a person or a business partner.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Create a User

Use this page or notebook to define the personal profile for the user that you are creating.

The profile contains personal, business, and contact information about who the user is, how to contact the user, and so on. Your ability to change and view profile information is determined by the authority your system administrator has granted to you.

The default profile contains tabs that you can click to specify additional information. Depending on the user type, some or all of the default tabs might not be displayed.

You can use these buttons to submit your request, which are displayed only if the administrator does not require you to enter a password:

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request for a later date and time.

Related information

For more information, see the [IBM Knowledge Center](#).

Personal Information

Use this notebook page to specify personal information about the user that you are creating.

Your ability to change and view profile information is determined by the authority your system administrator has granted to you. Contact your help desk or system administrator for information about profiles. The following fields are the default fields:

Last name

Type the user's last name or family name.

Full name

Identifies a value for distinguishing users, such as the user's full name.

Preferred user ID

Type the user ID. This determines the default user ID that new accounts and access use when they are created.

First name

Contains the user's first name or given name.

Initials

Contains the user's initials.

Home address

Contains the user's postal address at home.

Shared secret

Contains a value to use to retrieve a new password when the password is reset.

Organizational roles

Assign an organizational role. To select a role, click **Search**. For information about organizational roles, contact your system administrator. To remove an organizational role from the list, select the role and click **Delete**. If you do not have the appropriate authority, this field is read-only.

If you are an administrator, use caution if you assign persons to membership in groups so you can prevent unwanted assignments.

Click other tabs to specify additional information.

You can use these buttons:

Submit Now

Click to submit your request immediately. This button is not displayed if your administrator requires you to enter a password.

Schedule Submission

Click to schedule your request. This button is not displayed if your administrator requires you to enter a password.

Related information

For more information, see the [IBM Knowledge Center](#).

Business Information

Use this notebook page to specify business information for the user that you are creating.

Your ability to change and view profile information is determined by the authority your system administrator has granted to you. Contact your help desk or system administrator for information about profiles. The following fields are the default fields:

Office number

Type the office number.

Employee number

Type the employee number. This information is a numeric or alphanumeric identifier assigned to a person by the business.

Title

Type the title.

Manager

To edit this field, click **Search** to search for the manager of the user.

Postal address

Type the postal address at work.

Administrative assistant

To edit this field, click **Search** to search for a personal or department administrative assistant.

Click other tabs to specify additional information.

You can use these buttons:

Clear

Click to remove a user from the selected field.

Submit Now

Click to submit your request immediately. This button is not displayed if your administrator requires you to enter a password.

Schedule Submission

Click to schedule your request. This button is not displayed if your administrator requires you to enter a password.

Related information

For more information, see the [IBM Knowledge Center](#).

Contact Information

Use this notebook page to specify the contact information for the user that you are creating.

Your ability to change and view profile information is determined by the authority your system administrator has granted to you. Contact your help desk or system administrator for information about profiles. The following fields are the default fields:

E-mail address

Contains the e-mail address. If no e-mail address exists, the user does not receive a password for a new account in an e-mail message and must call the help desk or contact a manager.

Telephone number

Contains the work telephone number.

Mobile telephone number

Contains the mobile telephone number.

Pager

Contains the pager number.

Home telephone number

Contains the home telephone number.

Aliases

Contains the alias associated with the user ID. Aliases are sometimes used to determine account ownership for unowned accounts by matching up with user IDs for those accounts. To add an alias to the list of aliases, click **Add**. To delete an alias from the list, select the alias and click **Delete**. If you do not have the proper authority, this field is read-only. If you have authority and are unsure of what to put in this field, contact your help desk or administrator for assistance.

Click other tabs to specify additional information.

You can use these buttons:

Add

Click to add an alias.

Delete

Click to remove an alias from the alias list, if any exist.

Submit Now

Click to submit your request immediately. This button is not displayed if your administrator requires you to enter a password.

Schedule Submission

Click to schedule your request. This button is not displayed if your administrator requires you to enter a password.

Related information

For more information, see the [IBM Knowledge Center](#).

Assignment Attributes

Use this notebook page to specify values for the role assignment attributes for the user that you are creating.

You can specify values for attributes if you assigned a role to this user, and the role or its parent role contains assignment attributes.

You cannot specify values on this panel if:

- You did not assign a role.
- You assigned a role, but neither the role nor its parent role has assignment attributes.

Note: You cannot use this console panel to create a new assignment attribute. You can only specify values for existing assignment attributes.

The table on this page shows the list of assigned roles that have assignment attributes on the roles or its parent role. This table has the following fields:

Name

A link to the role associated with the user. Click the link to view or update the assignment attribute values for the role or its parent role.

Business Unit

The name of the business unit associated with the role.

When you have finished assigning values to attributes, select one of the following actions:

Submit Now

Click **Submit Now** to immediately submit the completed user profile.

Schedule Submission

Click **Schedule Submission** to specify a date and time for the submission of the completed user profile.

Associate role assignment attributes

Use this page to view the assignment attributes, and to select attributes for which you want to specify values.

The role assignment attributes table displays the attributes associated with this user.

Name

A link to the attribute. Each link consists of an attribute name combined with the name of the role. Click the link to modify the values.

Some attributes might have the name of a role that is different than the role you assigned to the user. This difference indicates that the role inherited the attributes from a parent role.

Value

The current values for the attribute. You can specify more than one value for each attribute. Attributes are not required to have a value.

When you have completed modification of values for the attributes, click **OK**.

Set assignment values

Use this page to add or delete values for a role assignment attribute.

Add

To add a value, enter text in the text field. Click **Add**. When you click **Add**, the value is displayed in the text box below the input field. You can add more than one value.

Delete

Select an existing entry in the text box. Click **Delete** to remove the value.

When you have finished making changes, click **OK**.

User Information

Use this page to define the profile for the business partner user that you are creating.

This page contains profile information about who the business partner user is, how to contact the user, and other information. The information in the profile is determined by the authority your system administrator has granted to you.

Full name

Identifies a value for distinguishing users, such as the user's full name.

Last name

Type the user's last name or family name.

E-mail address

Type the user's e-mail address.

Sponsor

Select a sponsor. To find and select a sponsor, click **Search**. To remove a sponsor, click **Clear**.

Organizational roles

Assign an organizational role. To select a role, click **Search**. For information about organizational roles, contact your system administrator. To remove an organizational role from the list, select the role and click **Delete**. If you do not have the appropriate authority, this field is read-only.

If you are an administrator, use caution if you assign persons to membership in groups so you can prevent unwanted assignments.

Aliases

Contains the alias associated with the user ID. Aliases are sometimes used to determine account ownership for unowned accounts by matching up with user IDs for those accounts. To add an alias to the list of aliases, click **Add**. To delete an alias from the list, select the alias and click **Delete**. If you do not have the proper authority, this field is read-only. If you have authority and are unsure of what to put in this field, contact your help desk or administrator for assistance.

You can use these buttons, which are displayed only if the administrator does not require you to enter a password:

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request for a later date and time.

Related information

For more information, see the [IBM Knowledge Center](#).

Change Profile

Use this page to change the profile for a business partner user. This page contains profile information about who the business partner user is, how to contact the user, and other information. The information in the profile is determined by the authority your system administrator has granted to you. After you view or specify information, choose an option to save any changes you made and complete your request.

Full name

Identifies a value for distinguishing users, such as the user's full name.

Last name

Type the user's last name or family name.

E-mail address

Type the user's e-mail address.

Sponsor

Select a sponsor. To find and select a sponsor, click **Search**. To remove a sponsor, click **Clear**.

Organizational roles

Assign an organizational role. To select a role, click **Search**. For information about organizational roles, contact your system administrator. To remove an organizational role from the list, select the role and click **Delete**. If you do not have the appropriate authority, this field is read-only.

If you are an administrator, use caution if you assign persons to membership in groups so you can prevent unwanted assignments.

Aliases

Contains the alias associated with the user ID. Aliases are sometimes used to determine account ownership for unowned accounts by matching up with user IDs for those accounts. To add an alias to the list of aliases, click **Add**. To delete an alias from the list, select the alias and click **Delete**. If you do not have the proper authority, this field is read-only. If you have authority and are unsure of what to put in this field, contact your help desk or administrator for assistance.

You can use these buttons:

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request for a later date and time.

Related information

For more information, see the [IBM Knowledge Center](#).

Change Profile

Use this page or notebook to view and change the user's personal profile information.

The profile contains personal, business, and contact information about who the user is, how to contact the user, and so on. Your ability to change and view profile information is determined by the authority your system administrator has granted to you.

Click any available tabs to view or specify additional information. After you view or specify information in any available tabs, select an option to save any changes you made and complete your request.

You can use these buttons:

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request for a later date and time.

Related information

For more information, see the [IBM Knowledge Center](#).

Personal Information

Use this notebook page to view and change the user's personal information.

Your ability to change and view profile information is determined by the authority your system administrator has granted to you. Contact your help desk or system administrator for information about profiles. The following fields are the default fields:

Last name

Type the user's last name or family name.

Full name

Identifies a value for distinguishing users, such as the user's full name.

Preferred user ID

Type the user ID. This determines the default user ID that new accounts and access use when they are created.

First name

Contains the first name or given name.

Initials

Contains the initials.

Home address

Contains the postal address at home.

Shared secret

Contains a value to use to retrieve a new password when the password is reset.

Organizational roles

Assign an organizational role. To select a role, click **Search**. For information about organizational roles, contact your system administrator. To remove an organizational role from the list, select the role and click **Delete**. If you do not have the appropriate authority, this field is read-only.

If you are an administrator, use caution if you assign persons to membership in groups so you can prevent unwanted assignments.

Click other tabs to specify additional information.

You can use these buttons:

Add

Click to add an organizational role.

Delete

Click to remove a role from the organizational role list, if any exist.

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request.

Related information

For more information, see the [IBM Knowledge Center](#).

Business Information

Use this notebook page to view and change the user's business information.

Your ability to change and view profile information is determined by the authority your system administrator has granted to you. Contact your help desk or system administrator for information about profiles. The following fields are the default fields:

Office number

Contains the office number.

Employee number

Contains the employee number. This information is a numeric or alphanumeric identifier assigned to the user by the business.

Title

Contains the job title.

Manager

Contains the name of the manager for the user. If you have permission to edit this field, click **Search** to search for the manager.

Postal address

Contains the postal address at work.

Administrative assistant

To edit this field, click **Search** to search for a personal or departmental administrative assistant.

Click other tabs to specify additional information.

Clear

Click to remove a user from the selected field.

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request.

Related information

For more information, see the [IBM Knowledge Center](#).

Contact Information

Use this notebook page to view and change the user's contact information.

Your ability to change and view profile information is determined by the authority your system administrator has granted to you. Contact your help desk or system administrator for information about profiles. The following fields are the default fields:

E-mail address

Contains the e-mail address. If no e-mail address exists, the user does not receive a password for a new account in an e-mail message and must call the help desk or contact a manager.

Telephone number

Contains the work telephone number.

Mobile telephone number

Contains the mobile telephone number.

Pager

Contains the pager number.

Home telephone number

Contains the home telephone number.

Aliases

Contains the alias associated with the user ID. Aliases are sometimes used to determine account ownership for unowned accounts by matching up with user IDs for those accounts. To add an alias to the list of aliases, click **Add**. To delete an alias from the list, select the alias and click **Delete**. If you do not have the proper authority, this field is read-only. If you have authority and are unsure of what to put in this field, contact your help desk or administrator for assistance.

Click other tabs to specify additional information.

You can use these buttons:

Add

Click to add an alias.

Delete

Click to remove an alias from the alias list, if any exist.

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request.

Related information

For more information, see the [IBM Knowledge Center](#).

Assignment attributes

Use this notebook page to specify values for the role assignment attributes for the user that you are modifying.

You can specify values for attributes if you assigned a role to this user, and the role or its parent role contains assignment attributes.

You cannot specify values on this panel if:

- You did not assign a role.
- You assigned a role, but neither the role nor its parent role has assignment attributes.

Note: You cannot use this console panel to create a new assignment attribute. You can only specify values for existing assignment attributes.

The table on this page shows the list of assigned roles that have assignment attributes on the roles or its parent role. This table has the following fields:

Name

A link to the role associated with the user. Click the link to view or update the assignment attribute values for the role or its parent role.

Business Unit

The name of the business unit associated with the role.

When you have finished assigning values to attributes, select one of the following actions:

Submit Now

Click **Submit Now** to immediately submit the completed user profile.

Schedule Submission

Click **Schedule Submission** to specify a date and time for the submission of the completed user profile.

Associate role assignment attributes

Use this page to view the assignment attributes, and to select attributes for which you want to specify values.

The role assignment attributes table displays the attributes associated with this user.

Name

A link to the attribute. Each link consists of an attribute name combined with the name of the role. Click the link to modify the values.

Some attributes might have the name of a role that is different than the role you assigned to the user. This difference indicates that the role inherited the attributes from a parent role.

Value

The current values for the attribute. You can specify more than one value for each attribute. Attributes are not required to have a value.

When you have completed modification of values for the attributes, click **OK**.

Set assignment values

Use this page to add or delete values for a role assignment attribute.

Add

To add a value, enter text in the text field. Click **Add**. When you click **Add**, the value is displayed in the text box below the input field. You can add more than one value.

Delete

Select an existing entry in the text box. Click **Delete** to remove the value.

When you have finished making changes, click **OK**.

Change Profile

Use this page to change the profile for a business partner user. This page contains profile information about who the business partner user is, how to contact the user, and other information. The information in the profile is determined by the authority your system administrator has granted to you. After you view or specify information, choose an option to save any changes you made and complete your request.

Full name

Identifies a value for distinguishing users, such as the user's full name.

Last name

Type the user's last name or family name.

E-mail address

Type the user's e-mail address.

Sponsor

Select a sponsor. To find and select a sponsor, click **Search**. To remove a sponsor, click **Clear**.

Organizational roles

Assign an organizational role. To select a role, click **Search**. For information about organizational roles, contact your system administrator. To remove an organizational role from the list, select the role and click **Delete**. If you do not have the appropriate authority, this field is read-only.

If you are an administrator, use caution if you assign persons to membership in groups so you can prevent unwanted assignments.

Aliases

Contains the alias associated with the user ID. Aliases are sometimes used to determine account ownership for unowned accounts by matching up with user IDs for those accounts. To add an alias to the list of aliases, click **Add**. To delete an alias from the list, select the alias and click **Delete**. If you do not have the proper authority, this field is read-only. If you have authority and are unsure of what to put in this field, contact your help desk or administrator for assistance.

You can use these buttons:

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request for a later date and time.

Related information

[For more information, see the IBM Knowledge Center.](#)

Change Passwords

Use this page to change the password for one or more accounts that belong to another user. You can change the password only when password editing is enabled.

Generate a password for me

Select this option to allow the system to generate a new password for you.

Allow me to type a password

Select this option to specify a password for the account.

Password

Type a new password for the account in this field. Asterisks (*) are displayed as you type. To edit this field, select the **Allow me to type a password** option.


Confirm password

Type the new password again. Asterisks (*) are displayed as you type. To edit this field, select the **Allow me to type a password** option.

Note: For some accounts, you cannot specify a password, even if you select **Allow me to type a password**. For these accounts, passwords must be generated. For example, some accounts are put into the credential vault. If the credentials for the account are configured to require check out and check in, you cannot specify the password, even if you select **Allow me to type a password**. The system generates a different password for these accounts. For these accounts, you must check out its credential to view the password.

If you have multiple accounts, and you select **Allow me to type a password**, your password is only applied to the accounts that permit a user-specified password.

Password strength rules

Click the  icon next to **View password strength rules** to display a list of password strength rules that must be applied for this account. The new password must conform to the password strength rules for the

account, or the password is not changed. The password strength rules vary for an account, based on your organization guidelines.

Password Rule table

Lists the rules that the password policy has defined.

Password Rule

Identifies the password rule.

Setting

Identifies the value for password rule.

If no password policy has been set, the **Password Rule** table might not be displayed.

Selecting accounts

Accounts table

Lists the accounts, including your IBM Security Identity Manager login account. Each account is represented by the service that hosts the account and the user ID for the account. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account.

If password synchronization is not enabled, the check box next to the accounts are preselected. The password change applies only to selected accounts. If you cannot change the password for an account, the check box is disabled.

If password synchronization is enabled, the table displays a list of individual accounts whose passwords are automatically changed by this action. The Select column is not displayed when password synchronization is enabled.

Service Name

Identifies the name of the service that hosts the account. Click the name of the service to view information about the service.


User ID

Identifies the user ID for the account. Click the user ID to view the details about the account.

Ownership Type

Identifies the ownership type for an account. This column is displayed when password synchronization is disabled.

Scheduling your request

If you want to schedule your request for a later date and time, click the  icon next to **Schedule**.

Immediate

Runs the request immediately after you click **Submit**. This option is selected by default.

Effective Date

Runs the request at a day and hour that you specify. After you select this option, click the calendar icon to specify the scheduled day and the clock icon to specify the scheduled hour.

Submitting your request

Click **Submit** to submit your request. If password synchronization is not enabled, you must select an account before clicking **Submit**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a User

Use this page to search for and select a user whose password you want to change.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select an attribute from the list. All searchable attributes and the personal profile are included in this list. If you select an attribute, the search is based on that attribute. If you select **Entire profile**, the search is based on all attributes associated with the user.

Last Name searches for the user's last name.

Full Name searches for the user's full name.

E-mail Address searches for the user's e-mail address.

Entire Profile searches all attributes associated with the user.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Users table

Lists the users matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

Name

Identifies a value for distinguishing a user, such as the user's full name. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the user's e-mail address.

Last Name

Identifies the user's last name.

Business Unit

Identifies the business unit. Click to view details about the organization.

Status

Identifies the user's status.

Users are either active or inactive. A user must be active to log in to the system. Users become inactive when they are suspended. The suspended users still exist, but they cannot access the system. System administrators can restore inactive users.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Reset Passwords

Use this page to reset the password for one or more accounts that belong to another user. Use this page when password editing is not enabled.

Accounts table

Lists the accounts. Each account is represented by the service that hosts the account and the user ID for the account. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account.

If password synchronization is not enabled, the check box next to the account is preselected. The password change applies only to that current account. If you cannot change the password for an account, the check box is disabled.


If password synchronization is enabled, the table displays a list of individual accounts whose passwords are automatically changed by this action. The Select column is not displayed when password synchronization is enabled.

Service Name

Identifies the name of the service that hosts the account.

User ID

Identifies the user ID for the account.

If you want to schedule your request for a later date and time, click the  icon next to **Schedule**.

Immediate

Runs the request immediately after you click the button to complete the task.

Effective date

Runs the request at a day and hour that you specify. After you select this option, click the calendar icon to specify the scheduled day, and click the clock icon to specify the scheduled hour.

Click **Reset** to perform the password reset. If password synchronization is disabled, you must select an account before clicking **Reset**.

Note: For some accounts, the generated passwords are not displayed. For example, the administrator might have placed some of the accounts in the credential vault. The credentials for these accounts can be configured to require check out and check in. For each account of this type, a separate password is generated. The generated passwords are not displayed when the password reset completes.

Related information

For more information, see the [IBM Knowledge Center](#).

Accounts

Use this page to find and view all the accounts that are associated with a specific user ID.

Account information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

User ID searches for user IDs that contain the text that is entered in the **Account information** field.

Service searches for services that contain the text that is entered in the **Account information** field.

Ownership type

Select an ownership type from the list to display accounts with that ownership type. The list contains default and custom ownership types. If you select an ownership type, the search is based on that ownership type.

- All** searches for all the accounts.
- Device** searches for the device accounts.
- Individual** searches for the individual accounts.
- System** searches for the system accounts.
- Vendor** searches for the vendor accounts.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Accounts table

Lists the accounts that are associated with the specified user ID. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box next to the account. To select all accounts, select the check box at the top of the column.

State

Indicates the compliancy state of the account.

Blank (no symbol)

Blank indicates the account is compliant.



Indicates that the account was returned from a reconciliation, which means it was not checked against the existing provisioning policies.




Indicates that the account can exist for the user, but that one or more of the account attributes do not comply with the existing provisioning policies.



Indicates either that the account is not supposed to exist because the user is not allowed to have access to the specified resource, or that a provisioning policy is not defined for the resource.

User ID

Identifies the user ID associated with the account. To view the details of the account, click the user ID. Click the icon () next to the user ID to show the tasks that can be performed on this account. The menu has these functions:

Change

Click to change the selected account.

Delete

Click to delete the selected account.

Change Password

Click to change the password for the selected account.

Reset Password

Click to reset the password for the selected account.

Suspend

Click to suspend the selected account.

Restore

Click to restore the selected account.

Add to Vault

Click to add the sponsored account to the credential vault so that the account can be shared. This function is only available if the Shared Access Module is installed. This function is disabled if the credentials exist in the vault.

Change Category

Click to add or remove account category from an account. Account categories are defined by the System Administrator.

Service Name

Identifies the name of the service. To view the details for the service, click the service name.

Ownership type

Identifies the ownership type of the account.

Status

Identifies the status of the account. Accounts can be active or inactive.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Request

Click to request an account.

Change

Click to change the information for the selected account.

Delete

Click to delete the selected account.

Suspend

Click to suspend the selected account.

Restore

Click to restore the selected account. Depending on how your system administrator has configured the system, you might be prompted to enter a password.

Add to Vault

Click to add the sponsored account to the credential vault so that the account can be shared. This function is only available if the Shared Access Module is installed.

Refresh

Click to update items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Account category

Use this page to find and view all the accounts that are associated with a specific user ID.

Account category table

Lists the account categories. The table contains these columns:

Select

Select to specify an account category.

Account Category

Identifies the category for an account, valid categories are defined by your system administrator.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Request an Account

Use this page to request an account for another user.

The pages that are displayed in the notebook vary, depending on the type of service that you selected and by the authority that the system administrator has granted you. For example, for the AIX service, the Account information, Access information, and Administration choices pages might be displayed.

The fields that are displayed on these pages also vary, depending on the type of service that you selected and by the authority that the system administrator has granted you.

The following topics define the default service attributes for the default services. For information about other service attributes, see your system administrator.

Related information

For more information, see the [IBM Knowledge Center](#).

AIX Default Attributes

For the AIX service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Access information page

UNIX Shell

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the read, write, and execute permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the access used by the account as a default change file mode value for the user home directory.

Administration choices(1) page

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as the secondary group of the user.

Groups that can use the su command on this user

Specify the name of the group that can use the UNIX **su** command on the user.

Groups to be administered

Specify the groups to administer.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before the date that a password expires that a warning is issued to the user.

Administrative roles

Specify the administrative roles for the user.

Additional mandatory methods for authenticating the user

Specify other mandatory authentication methods.

Additional optional methods for authenticating the user

Specify other optional authentication methods.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices(2) page**Audit class**

Specify the list of audit classes for the user.

Allow user to execute daemon process?

Select this check box to enable the user to run daemon processes on the system.

Allow user to log in to the system?

Select this check box to enable the user to log directly into the system.

Allow user to remotely login to the system?

Select this check box to enable the user to log into the system remotely.

Can another user switch user to this user?

Select this check box to enable another user to use the UNIX **su** command on this user.

Is this user an administrator?

Select this check box to designate the user as an administrator of the system.

Trusted path status

Select the default trusted path status for the account.

always

Specifies that the user that is confined to the trusted path.

/notsh

Specifies that the user session ends if the secure attention key (SAK) signal is detected.

nosak

Specifies that the SAK key is disabled.

on

Specifies that the standard trusted path management is used.

Soft limit for largest core size

Specify the soft limit for the largest core file that the user's process can create.

Soft limit for maximum amount of CPU utilization

Specify the soft limit for the largest amount of system unit time (in seconds) that the user's process can use.

Soft limit for largest data segment

Specify the soft limit for the largest process data segment for the user's process.

Soft limit for largest file size

Specify the soft limit for the largest file that the user's process can create or extend.

Soft limit for largest stack segment

Specify the soft limit for the largest process stack segment for the user's process.

Largest core size

Specify the largest core file that the user's process can create.

Maximum CPU utilization

Specify the largest amount of system unit time (in seconds) that the user's process can use.

Largest data segment

Specify the largest process data segment for the user's process.

Largest file size

Specify the largest file that the user's process can create or extend.

Largest stack segment

Specify the largest amount of physical memory that the user's process can allocate.

Allowed login time

Specify the days and times that the user is allowed to access the system.

Allowed number of login retries before locking the account

Specify the number of failed login attempts before the account is locked.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in weeks) that the account can remain active after the password for the account has expired.

Minimum alphabetic characters in password

Specify the minimum number of alphabetic characters that must be included in the password for the account.

Minimum difference between the current and last password

Specify the minimum number of characters that are required in a new password that were not in the old password.

Maximum number of characters that can be repeated in a password

Specify the maximum number of characters in a password that can be repeated.

Minimum length of the password

Specify the minimum length of the password.

Password restriction methods

Specify password restriction methods to the account.

Password dictionaries used to restrict passwords

Specify the password dictionary files that are used to restrict which passwords can be used by the account.

Number of previous passwords that cannot be reused

Specify the number of passwords to be kept in the password history.

Account last accessed on

Specify a value for the last access date and time.

Valid terminals allowed to access the account

Specify which terminals can log in using this account.

System authentication mechanism for the user

Specify the authentication mechanism the system uses to authenticate the user.

Authentication registry where the user is administered

Specify the registry that is used for authenticating the user.

Related information

For more information, see the [IBM Knowledge Center](#).

HP-UX Default Attributes

For the HP-UX service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX Shell**

Specify a default command shell for the account.

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the names of the groups to use as secondary groups of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices page**Password warning age**

Specify the number of days before the date that a password expires that a warning is sent to the user.

Maximum number of days (weeks for AIX) the account can remain valid after the password expires

Specify the maximum time that the account can remain active after the password for the account has expired.

Number of days the account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allowed number of login retries before locking the account

Specify the number of login attempts that can occur before the account is locked.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Although you can specify a time, this feature is disabled and you can only set an account expiration date. Alternatively, select **Never** to set the account to never expire.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP Default Attributes

For the LDAP service type, IBM Security Identity Manager provides a set of default attributes.

User page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

User Container

Click **Search** to search for the location in the LDAP tree where you want to add the user.

Full name

Type a value for distinguishing users, for example, the full name of the user.

Preferred user ID

Type the user ID. This determines the default user ID that new accounts and access use when they are created.

Last name

Type the last name of the user.

First name

Type the first name of the user.

Initials

Type the initials of the user.

E-mail address

Type the e-mail address of the user.

Display name

Type the name of the user that you want to be displayed in the IBM Security Identity Manager interface.

Description

Type information about the intended purpose of the account.

Home telephone number

Type the home telephone number of the user.

Mobile telephone number

Type the mobile telephone number of the user.

Pager

Type the pager number of the user.

Business page**Title**

Type the business title of the user.

Employee number

Type the employee number of the user.

Employee type

Type the employment specification of the user, such as regular, contractor, or business partner.

Manager

Type the name of the manager of the user.

Administrative assistant

Type the name of the assistant of the user.

Business category

Type the business category type of the user.

Department number

Type the department number of the user.

Telephone number

Type the business telephone number of the user.

Fax number

Type the business fax number of the user.

Postal address

Type the business postal address of the user.

Office number

Type the office location of the user.

Location name

Type the locale of the user.

Address page**Registered address**

Type the registered address of the user.

Street

Type the street name of the registered address.

State

Type the state in which the user resides.

Destination indicator

Type an applicable destination indicator.

Physical delivery office name

Type the name of the physical address.

Home address

Type the home address of the user.

Postal code

Type the postal code of the user.

Post office box

Type the post office box number of the user.

Preferred delivery method

Type the preferred method of delivery of the user.

Other page

Driver license

Type the driver's license number of the user.

Preferred language

Type the preferred language of the user.

Teletex terminal ID

Type the teletex terminal ID of the user.

Telex number

Type the teletex number of the user.

Related information

For more information, see the [IBM Knowledge Center](#).

Linux Default Attributes

For the Linux service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page

UNIX shell

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

This field is not supported for Linux operating systems.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices pages

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Password warning age

Specify the number of days before expiration that a password expiration warning is issued to the user.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in days) that the account can remain active after the password for the account has expired.

Related information

For more information, see the [IBM Knowledge Center](#).

Solaris Default Attributes

For the Solaris service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX Shell**

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices page

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before expiration that a password expiration warning is issued to the user.

Number of days account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allow at jobs?

Select this check box to allow this account to run an *at* job.

Allow cron jobs?

Select this check box to allow this account to run a *cron* job.

Related information

For more information, see the [IBM Knowledge Center](#).

Change an Account

Use this notebook to change an account associated with the selected user ID.

The pages that are displayed in the notebook vary, depending on the type of service that you selected and by the authority that the system administrator has granted you. For example, for the AIX service, the Account information, Access information, and Administration choices pages might be displayed.

The fields that are displayed on these pages also vary, depending on the type of service that you selected and by the authority that the system administrator has granted you.

The following topics define the default service attributes for the default services. For information about other service attributes, see your system administrator.

Related information

For more information, see the [IBM Knowledge Center](#).

AIX Default Attributes

For the AIX service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Access information page**UNIX Shell**

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the read, write, and execute permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the access used by the account as a default change file mode value for the user home directory.

Administration choices(1) page**Force a password change?**

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as the secondary group of the user.

Groups that can use the su command on this user

Specify the name of the group that can use the UNIX **su** command on the user.

Groups to be administered

Specify the groups to administer.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before the date that a password expires that a warning is issued to the user.

Administrative roles

Specify the administrative roles for the user.

Additional mandatory methods for authenticating the user

Specify other mandatory authentication methods.

Additional optional methods for authenticating the user

Specify other optional authentication methods.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices(2) page

Audit class

Specify the list of audit classes for the user.

Allow user to execute daemon process?

Select this check box to enable the user to run daemon processes on the system.

Allow user to log in to the system?

Select this check box to enable the user to log directly into the system.

Allow user to remotely login to the system?

Select this check box to enable the user to log into the system remotely.

Can another user switch user to this user?

Select this check box to enable another user to use the UNIX **su** command on this user.

Is this user an administrator?

Select this check box to designate the user as an administrator of the system.

Trusted path status

Select the default trusted path status for the account.

always

Specifies that the user that is confined to the trusted path.

/notsh

Specifies that the user session ends if the secure attention key (SAK) signal is detected.

nosak

Specifies that the SAK key is disabled.

on

Specifies that the standard trusted path management is used.

Soft limit for largest core size

Specify the soft limit for the largest core file that the user's process can create.

Soft limit for maximum amount of CPU utilization

Specify the soft limit for the largest amount of system unit time (in seconds) that the user's process can use.

Soft limit for largest data segment

Specify the soft limit for the largest process data segment for the user's process.

Soft limit for largest file size

Specify the soft limit for the largest file that the user's process can create or extend.

Soft limit for largest stack segment

Specify the soft limit for the largest process stack segment for the user's process.

Largest core size

Specify the largest core file that the user's process can create.

Maximum CPU utilization

Specify the largest amount of system unit time (in seconds) that the user's process can use.

Largest data segment

Specify the largest process data segment for the user's process.

Largest file size

Specify the largest file that the user's process can create or extend.

Largest stack segment

Specify the largest amount of physical memory that the user's process can allocate.

Allowed login time

Specify the days and times that the user is allowed to access the system.

Allowed number of login retries before locking the account

Specify the number of failed login attempts before the account is locked.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in weeks) that the account can remain active after the password for the account has expired.

Minimum alphabetic characters in password

Specify the minimum number of alphabetic characters that must be included in the password for the account.

Minimum difference between the current and last password

Specify the minimum number of characters that are required in a new password that were not in the old password.

Maximum number of characters that can be repeated in a password

Specify the maximum number of characters in a password that can be repeated.

Minimum length of the password

Specify the minimum length of the password.

Password restriction methods

Specify password restriction methods to the account.

Password dictionaries used to restrict passwords

Specify the password dictionary files that are used to restrict which passwords can be used by the account.

Number of previous passwords that cannot be reused

Specify the number of passwords to be kept in the password history.

Account last accessed on

Specify a value for the last access date and time.

Valid terminals allowed to access the account

Specify which terminals can log in using this account.

System authentication mechanism for the user

Specify the authentication mechanism the system uses to authenticate the user.

Authentication registry where the user is administered

Specify the registry that is used for authenticating the user.

Related information

For more information, see the [IBM Knowledge Center](#).

HP-UX Default Attributes

For the HP-UX service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page

UNIX Shell

Specify a default command shell for the account.

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the names of the groups to use as secondary groups of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices page

Password warning age

Specify the number of days before the date that a password expires that a warning is sent to the user.

Maximum number of days (weeks for AIX) the account can remain valid after the password expires

Specify the maximum time that the account can remain active after the password for the account has expired.

Number of days the account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allowed number of login retries before locking the account

Specify the number of login attempts that can occur before the account is locked.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Although you can specify a time, this feature is disabled and you can only set an account expiration date. Alternatively, select **Never** to set the account to never expire.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP Default Attributes

For the LDAP service type, IBM Security Identity Manager provides a set of default attributes.

User page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

User Container

Click **Search** to search for the location in the LDAP tree where you want to add the user.

Full name

Type a value for distinguishing users, for example, the full name of the user.

Preferred user ID

Type the user ID. This determines the default user ID that new accounts and access use when they are created.

Last name

Type the last name of the user.

First name

Type the first name of the user.

Initials

Type the initials of the user.

E-mail address

Type the e-mail address of the user.

Display name

Type the name of the user that you want to be displayed in the IBM Security Identity Manager interface.

Description

Type information about the intended purpose of the account.

Home telephone number

Type the home telephone number of the user.

Mobile telephone number

Type the mobile telephone number of the user.

Pager

Type the pager number of the user.

Business page**Title**

Type the business title of the user.

Employee number

Type the employee number of the user.

Employee type

Type the employment specification of the user, such as regular, contractor, or business partner.

Manager

Type the name of the manager of the user.

Administrative assistant

Type the name of the assistant of the user.

Business category

Type the business category type of the user.

Department number

Type the department number of the user.

Telephone number

Type the business telephone number of the user.

Fax number

Type the business fax number of the user.

Postal address

Type the business postal address of the user.

Office number

Type the office location of the user.

Location name

Type the locale of the user.

Address page**Registered address**

Type the registered address of the user.

Street

Type the street name of the registered address.

State

Type the state in which the user resides.

Destination indicator

Type an applicable destination indicator.

Physical delivery office name

Type the name of the physical address.

Home address

Type the home address of the user.

Postal code

Type the postal code of the user.

Post office box

Type the post office box number of the user.

Preferred delivery method

Type the preferred method of delivery of the user.

Other page**Driver license**

Type the driver's license number of the user.

Preferred language

Type the preferred language of the user.

Teletex terminal ID

Type the teletex terminal ID of the user.

Telex number

Type the teletex number of the user.

Related information

[For more information, see the IBM Knowledge Center.](#)

Linux Default Attributes

For the Linux service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX shell**

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

This field is not supported for Linux operating systems.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices pages**Force a password change?**

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Password warning age

Specify the number of days before expiration that a password expiration warning is issued to the user.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in days) that the account can remain active after the password for the account has expired.

Related information

For more information, see the [IBM Knowledge Center](#).

Solaris Default Attributes

For the Solaris service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX Shell**

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices page**Force a password change?**

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before expiration that a password expiration warning is issued to the user.

Number of days account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allow at jobs?

Select this check box to allow this account to run an *at* job.

Allow cron jobs?

Select this check box to allow this account to run a *cron* job.

Related information

For more information, see the [IBM Knowledge Center](#).

Noncompliant Value

Use this page to change an account that has one or more attributes with values that do not comply with an existing policy.

Select

Specifies a noncompliant attribute. To select or deselect one or more noncompliant attributes, select the check box adjacent to the noncompliant attribute. To select or deselect all noncompliant attributes, select the check box at the top of the column. If the policy enforcement setting for the service is set to Correct or Suspend, you cannot deselect any attributes.

Attribute Name

Identifies the name of an attribute.

Noncompliant Value

Provides the value that does not comply with an existing policy. If an attribute value is empty, the suggested value is used. If there is no suggested value, the noncompliant value is removed when you change the account.

Suggested Value

Provides the compliant value for the attribute based on the policy evaluation.

Access

Provides the name of the access related to the noncompliant attribute value.

Click **Back with correction** to bring the suggested value back to the account form.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Access

Use this page to request or remove access.

Select

Select this radio button to select an access.

State

Indicates the compliancy state of the access. Compliance states do not occur for organizational role access entitlements.

Blank (no symbol)

Blank indicates the access is compliant.



Indicates that the access was returned from a reconciliation, which means it was not checked against the existing provisioning policies.



Indicates that the access can exist for the user, but that one or more attributes do not comply with the existing provisioning policies.



Indicates either that the access is not supposed to exist or that a provisioning policy is not defined for the resource.

Access Name

Identifies the name of the access.

Access Type

Identifies the type of access, such as an application, email group, shared folder, or role.

User ID

Identifies the user who has the access. To ensure that this is the correct user ID, click the name to see details about the user. This field is left blank for organizational roles.

Service Name

Identifies the name of a service instance. This field is blank for organizational roles.

Status

Identifies the current status of the access. An access can be active or inactive. This field is blank for organizational roles.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Request

Click to request an access.

Delete

Click to delete the selected access.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Details

Use this page to review the details related to the selected access. All fields are read-only.

Access name

Identifies the access name.

Access type

Identifies the type of access, such as an application, e-mail group, shared folder, or role.

Access description

Provides a description of the access.

Access owner

Identifies the name of the access owner.

Select Access

Use this page to find and request an access.

Access information

Select an access type from the list. The contents of the list are defined by the system administrator.

The search is based on the access type that you select from the list. The list items might vary, depending on which access type you selected from the **Access type** list. For example, if you select **Application**, a new list with its dependent access types is displayed. Similarly, if you select **All**, no new list is displayed.

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Access type

Select an access type from the list. Select **All** to display all of the accesses dependent on an access type and click **Search**.

Access table

Lists the commonly used access items matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an access. Select an option to select an access.

Access Name

Identifies the name of the access.

Service Name

Identifies the name of a managed resource associated with the access.

Access Type

Identifies the category of the access, and consists of these types:

- Application
- AccessRole
- MailGroup
- SharedFolder
- A custom-defined access type

The column displays the access type hierarchy in a colon-separated string format. For example, Application:ERP Application:Supplier or AccessRole:Manager:Finance.

Access Description

Provides a description of the access.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Accounts

Use this page to grant access to accounts that you want the user to access.

Select Accounts table

Lists the accounts that the user has for a specific access. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box adjacent to the account. To select all accounts, select the check box at the top of the column. If the check box is not visible, the user already has access to the account.

User ID

Identifies the user who has the account. To ensure that this is the correct user ID, click the name to see details about the user.

Service Name

Identifies the name of the managed resource.

Status

Identifies whether the account is active or inactive.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Request Access Confirmation

Use this page to submit your request immediately or schedule the request for a future time. If password synchronization is off, you can also specify a password for the new accounts that you want the user to access.

Password

Enter the password for accounts on the managed resource.

Generate a password for me

Select to have the system generate a password for the account.

Allow me to type a password

Select to specify a password for the account.

Password

Type a new password for the account in this field. The password is encrypted when it is saved.

Confirm password

Type the new password again.

Password Strength Rules table

Lists the rules that the new password must conform to for this account. If the password does not conform to these password strength rules, an error message is displayed, and you must specify a new password. This field might not be displayed if no password rules have been defined.

Password Rule

Displays the password rules.

Setting

Displays the value that is required for the password rule.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

One Time Schedule

Click the  icon adjacent to **One Time Schedule** to schedule your request.

Immediate

Runs the request immediately after you click **Submit**.

Effective date

Runs the request at a date and time that you specify. After you select this option, click the calendar and clock icons to specify the scheduled date and time.

Click **Submit** to submit your request.

Related information

For more information, see the [IBM Knowledge Center](#).

Remove Access

Use this page to remove access to accounts immediately or schedule the request to remove access for a future time.

One Time Schedule

Click **One Time Schedule** to schedule your request.

Immediate

Runs the request immediately after you click **Submit**.

Effective date

Runs the request at a date and time that you specify. After you select this option, click the calendar and clock icons to specify the scheduled date and time.

Click **Submit** to submit your request.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a Recertification Policy

Use this page to run a recertification policy for a specific user. Only user recertification policies that are enabled can be searched. Only system administrators can perform this task.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Name or description searches for recertification policy names or descriptions that contain the text that is entered in the **Search information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Recertification Policies table

Lists the recertification policies matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a recertification policy. To select one or more recertification policies, select the check box adjacent to the recertification policy. To select all recertification policies, select the check box at the top of the column.

Name

Identifies the name of the recertification policy. Click the name to view or change the recertification policy.

Description

Provides a brief description of the recertification policy.

Business Unit

Indicates the business unit in which the recertification policy is defined.

Targets

Identifies the users to which the recertification policy applies.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Run** to immediately run the selected recertification policy.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a Service

Use this page to find the service that you want.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Service searches for service names that contain the text that is entered in the **Search information** field.

Business unit searches for business units in which the business unit name contains the text that is entered in the **Search information** field.

Service type

Select a service type from the list.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Services table

Lists the services that match the search criteria that you specified. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box next to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view the service details.

Description

Identifies a brief description of the service.

Service Type

Identifies the type of service.

Business Unit

Identifies the business unit associated with the service.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a User

Use this page to search for a user.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select an attribute from the list. All searchable attributes and the personal profile are included in this list. If you select an attribute, the search is based on that attribute. If you select **Entire profile**, the search is based on all attributes associated with the user.

Last Name searches for the user's last name.

Full Name searches for the user's full name.

E-mail Address searches for the user's e-mail address.

Entire Profile searches all attributes associated with the user.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Users table

Lists the users matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

Name

Identifies a value for distinguishing a user, such as the user's full name. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the user's e-mail address.

Custom Display

Identifies a custom display attribute.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

Status

Identifies the user's status.

Users are either active or inactive. A user must be active to log in to the system. Users become inactive when they are suspended. The suspended users still exist, but they cannot access the system. System administrators can restore inactive users.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Success

This page confirms that you have successfully completed your task.

Click a related task you might want to perform.

Related information

For more information, see the [IBM Knowledge Center](#).

Confirm

Use this page to verify that you want to complete the requested action. The **Confirm** page is displayed for requests that can have a detrimental effect on your system.

Verify that the action specified in the message displayed is what you want to be done and click the appropriate button.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Services

Select a Service

Use the **Select a Service** page to find the service that you want to manage.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Service searches for service names or descriptions that contain the text that is entered in the **Search information** field.

Business unit searches for business units in which the business unit name contains the text that is entered in the **Search information** field.

Service type

Select a service type from the list. The items in the list contain the service types that are installed by the administrator. Select **All** from the list to show all of the services that are managed by IBM Security Identity Manager.

Status

Specify the status value for the search. The items in the list contain possible status values for each service. Status values:

All

Include status values for all services.

Alive

Services that are functioning with no known issues.

Failed

Services that encountered a problem. For example, a connection test might fail, or a request was not completed on a remote endpoint.

Attempting recovery

Services that encountered a problem, and for which the server is attempting to process a previously blocked request.

Locked

Services that are locked because a reconciliation process is running.

Unknown

Services that never attempted a connection test or received and processed a request.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Services table

Lists the services that match the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box next to the service. To select all services, select the check box at the top of the column.


Status

Specifies the status of the service. Each status is represented by an icon. The icons correspond to the options in the service status list in the search criteria. Click the icon to get to detailed service status information. If the service is in Alive status, the column does not contain an icon.

Service Name

Identifies the name of the service.

Click the name of the service to change the service information.

Click the icon () next to the service to show the tasks that can be completed on the service. The task that you can complete is dependent on the type of service.

Use these menu items to complete a task on the selected service:

Set Up Reconciliation

Defines a reconciliation schedule. Reconciliation can be done immediately or scheduled for a later time. You can schedule a reconciliation to occur regularly.

Configure Policy Enforcement

Defines policy enforcement options for non-compliant accounts.

Manage Groups

Creates, modifies, or deletes groups, adds and removes membership, and defines access on a group.

Request Accounts

Requests the accounts on the service.

Accounts

Lists the accounts that use the service.

Customize Account Form

Use this action to create or modify a customized account form for the service instance.

Delete Account Form

Use this action to delete a customized account form for the service instance and reset to the default account form.

Account Recertification Status

Identifies the recertification status for accounts on a service.

Account Defaults

Defines defaults to be used by accounts that use the service.

Reconcile Now

Run a reconciliation immediately.

Enforce Policy

Reevaluate the governing provisioning policies for the service.

Retry Blocked Requests

Attempt a connection to the remote endpoint and try again any outstanding requests that are found. When you complete fixes to a service and bring the service online, you can then use this action to try again the requests.

Description

Identifies a brief description of the service.

Service Type

Identifies the type of service.

Note: Accesses that are defined on the original service are not available for the hosted service, and those accesses cannot be requested by users in different organizations.

Business Unit

Identifies the business unit in which the service is created.

Access Name

The access name of the corresponding service. If access is undefined, the field is empty.

Access Status

The status of the corresponding service. Access status displays the following value:

Access Enabled

Access is defined and enabled.

Access Disabled

Access is disabled or undefined.

Note: For HRFeed services, the column is always empty.

Access Type

The access type for the corresponding service. If access is undefined, the field is empty.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a service.

Change

Click to change the information for the selected service.

Delete

Click to delete the selected service and remove all accounts on that particular service from the system. The accounts are not removed from the resource. Deleting a service automatically removes it from all provisioning policies, identity policies, password policies, adoption policies, and recertification policies that currently reference it. In addition, if all services that are referenced by a policy are deleted by this operation, the entire policy is also deleted.

Export Access Data

Click to open the **Export Access Data** page, and export the service access data. The **Export Access Data** button is not active until you select some accesses to activate it. Only the service access that you selected are exported.

Import Access Data

Click to open the **Import Access Data** page to import the access data for a service access. You can also import access data for a set of services.

Enable Access

Click to enable access for the service.

Disable Access

Click to disable access for the service.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Export access data

Use the **Export Access Data** page to export the service access data. The access data is specified in a comma-separated value (CSV) file. IBM Security Identity Manager uses the settings that are indicated in the CSV file.

The **Export Access Data** page is displayed after you click **Export Access Data** in the **Select a Service** page.

After you submit the export request, a process status indicates the progress of the export operation.

Download Exported Data

Click to download the exported data for the service access. Download the file on your local system by using your web browser settings.

The exported data contains information such as Service DN, Service name, Define as Access, Access name, Access type, Access description, Icon URL, Search terms, Additional information, and Badges.

Download Export Log File

Click to view any error or log information about the export operation. This button is displayed only if the submitted export operation contains any log information or encountered any errors.

Cancel

Click to cancel the export operation. The operation is discontinued if you cancel it during an active export session.

Close

Click to close the **Export Access Data** page. The operation fails if you close the **Export Access Data** page during an active export session.

Related information

For more information, see the [IBM Knowledge Center](#).

Import access data

Use the **Import Access Data** page to import the service access data. The access data is specified in a comma-separated value (CSV) file. IBM Security Identity Manager uses the settings that are indicated in the CSV file.

File to Upload (.CSV)

Displays the name of the CSV file that contains all the service access data. This field is required.

Browse

Click to locate and upload the CSV file for import. You can also type the complete and correct path to the file on your workstation along with the file name.

Import

Click to immediately import the CSV file.

After you submit the import request, a process status indicates the progress of the import operation.

Note: If you click **Import** with an invalid file format, a message is displayed to inform you that the file format is not valid.

Cancel

Click to cancel the import operation. The operation is discontinued if you cancel it during an active import session.

Download Import Log File

Click to view any error or log information about the import operation. This button is displayed only if the submitted import operation contains any log information or encountered any errors.

Close

Click to close the **Import Access Data** page. The operation fails if you close the **Import Access Data** page during an active import session.

Related information

For more information, see the [IBM Knowledge Center](#).

Enable Access

You can control access by granting access to selected services.

Use service description for the access description

Lets you use the same service description for the access description.

Note: If selected, the service description overrides the existing access description.

Select an access type that you want to grant to all the specified services

Specifies the access type that you want to grant for the selected services.

Access Types

Select an access type for a service. The default access type for a service is **Application**. If **Application** is removed as an access type, the first access type is the default option.

Services table

Lists the available services and the access details that are assigned to the service. The table contains the following columns:

Service Name

Name of the service.

Description

A short description for the service.

Access Name

The assigned access name.

Access Type

The type of access assigned to the service. For example: Application.

You can use the following buttons:

Enable

Click to enable access for the displayed services.

Cancel

Click to cancel any changes.

Service Status Information

Use this page to review status information for the selected service.

Service name

The name of the service as shown on the administration console.

Service description

Description of the service as entered by the system administrator.

Status

Current operational status of the service. Possible values are:

Alive

Services that are functioning with no known issues.

Failed

Services that encountered a problem. For example, a connection test might fail, or a request did not complete on a remote endpoint.

Attempting recovery

Services that encountered a problem, and for which the server is attempting to run a previously blocked request.

Locked

Services that are locked because a reconciliation process is running.

Unknown

Services which never attempted a connection test or attempted to run a request.

Number of blocked requests

Number of requests that are blocked, waiting for the service to return to Active status.

Failed since date

Timestamp describing when this service was placed in Failed status

Last attempt date

Timestamp describing the last time the system attempted to make a connection to the service.

Oldest blocked request id

Process ID of the oldest request that is blocked because this service is in any status other than Alive. This ID can be useful when a request fails repeatedly. You can go to View Requests and use this value to identify the process ID to cancel.

Oldest blocked request date

Timestamp describing when the oldest pending request ID was originally processed by the system.

Last failing server

Describes the WebSphere cell, node, and server which last tried to connect to the service. This information can be useful in determining whether a particular server in a WebSphere cluster installation is having trouble processing requests.

Last failure reason

A detailed message that describes the reason for failure of the most recent attempt to connect to the service.

Actions**Close**

Closes the status information window and returns to the Manage Services page.

Refresh

Retrieves the most recent status information for the service.

Create a Service

Use this wizard to create a service. The tabs available vary depending on the type of service you are creating.

Related information

For more information, see the [IBM Knowledge Center](#).

Select the Type of Service

Use this page to select the service type for the service that you want to create.

Business unit

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Service Type table

Lists the available service types. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the service type for the service that you want to create.

Service Type

Identifies the type of service.

Description

Contains a brief description of the service type.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Service Information

Use this page to specify information about a service instance. The fields that are displayed on this page of the wizard vary based on the type of service that you selected in the previous panel.

You can specify a service instance for a managed resource. You provide information that IBM Security Identity Manager associates with a service instance. For example, an attribute might represent the administrative user ID and administrative password on a managed resource, or the Universal Resource Locator (URL) of the resource.

Alternatively, you can specify a service instance for activities that import identity data. You provide information that IBM Security Identity Manager uses during the data import, such as a file name or the data naming context.

Click **Test Connection** when the fields are complete, to test the connection to the managed resource. For manual services, the **Test Connection** button is not available.

If the connection is successful and SSL is configured, an informational message is displayed, indicating a successful connection. If the connection is successful and SSL is *not* configured, a warning message is displayed. If the connection fails, a warning message is displayed. You can continue with the wizard, even if the connection is not successful.

Related information

For more information, see the [IBM Knowledge Center](#).

Hosted Service: Service Information

Use this page to specify information about the hosted service.

Note: Accesses that are defined on the original service are not available for the hosted service, and those accesses cannot be requested by users in different organizations.

If you select a service profile for a hosted service, complete these fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance.

Description

Specify additional information about the service instance.

Service

Click **Search** to specify an existing service instance.

Click **Clear** to remove the currently specified service.

Service prerequisite

Click **Search** to specify an existing service instance or function that the hosted service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user can only receive a new account if they have an existing account on the service prerequisite.

Owner

Specify the existing user ID of the service owner that administers the service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user be used in administering the service instance

Click **Finish** when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

DSML Identity Feed: Service Information

Use this page to specify information about the Directory Services Markup Language (DSML) identity feed.

If you select a service profile to import identity data using DSML, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

User ID

Specify the administrative user ID for the service instance.

Password

Specify the administrative password for the service instance. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

File name

Specify the file name, including the path name, that contains the user information.

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

IDI Data Feed: Service Information

Use this page to specify information about the Initial Domain Identifier (IDI) identity feed.

If you select a service profile for activities that use IBM Security Directory Integrator to import identity data, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the name of the principal to authenticate clients using the Java Naming and Directory Interface (JNDI) application programming interface.

Password

Specify the password to authenticate clients using the JNDI application programming interface. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Name attribute

Select an attribute, such as `uid`, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

InetOrgPerson Identity Feed: Service Information

Use this page to specify information about the INetOrgPerson identity feed.

If you select a service profile to import identity data using LDAP, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the distinguished name (DN) of the administrator who is authorized to access the LDAP server that provides the identity information. For example, the user ID on LDAP is `cn=Administrator,cn=users,dc=itimcv,dc=com`, where *itimcv* is the domain name.

Password

Specify the password for the administrator who is authorized to access the LDAP server that provides the identity feed. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Attribute mapping file name

Specify the absolute path and file name of the file that contains attribute mapping between the identity feed source schema and specified user type schema. The mapping file contains key value pairs that identify the source and target attribute mapping.

Name attribute

Select an attribute, such as `uid`, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

AD OrganizationalPerson Identity Feed: Service Information

Use this page to specify information about the Active Directory OrganizationalPerson identity feed.

If you select a service profile to import identity data using Active Directory, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the distinguished name (DN) of the administrator who is authorized to access the LDAP server that provides the identity information. For example, the user ID on LDAP is `cn=Administrator,cn=users,dc=itimcv,dc=com`, where *itimcv* is the domain name.

Password

Specify the password for the administrator who is authorized to access the LDAP server that provides the identity feed. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Attribute mapping file name

Specify the absolute path and file name of the file that contains attribute mapping between the identity feed source schema and specified user type schema. The mapping file contains key value pairs that identify the source and target attribute mapping.

Name attribute

Select an attribute, such as `uid`, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

CSV Identity Feed: Service Information

Use this page to specify information about the comma-separated value (CSV) identity feed.

The comma-separated value (CSV) file cannot contain binary attributes. If you include multivalued attributes, they must be represented by using multiple columns with the same attribute name. You must list all required attributes in the CSV file before you list optional attributes.

If you select a service profile for activities that use a CSV format to import identity data, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

File name

Specify the file name, including the path name, of the CSV file.

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Name attribute

Select an attribute, such as uid, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP Profile: Service Information

Use this page to specify information about the Lightweight Directory Access Protocol (LDAP) service instance.

The LDAP service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

LDAP service

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the LDAP service instance runs.

Description

Specify additional information about the LDAP service instance.

Connection mode

This option is available only if the erconnectionmode attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`. Where *ip-address* is the Security Directory Integrator host and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Directory server location

Specify the location and port number of the LDAP Adapter. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `ldap://[address]:port number`.

Use SSL communication with LDAP?

Select this check box to use secure communication with the LDAP service instance.

Administrator name

Specify the administrative user ID, such as `cn=root`, for the LDAP service instance. The name must be a distinguished name (DN).

Password

Specify the administrative password for the LDAP service instance. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Directory server name

Choose a directory server from the list.

Owner

Click **Search** to specify the existing user ID of the service owner that administers the LDAP service instance.

Click **Clear** to remove the currently specified user.

Service prerequisite

Click **Search** to specify an existing service instance or function that the LDAP service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user can only receive a new account if they have an existing account on the service prerequisite.

Users and groups**User base DN**

Specify the distinguished name (DN) of the container or base point where the users are stored.

RDN attribute

Specify the required relative distinguished name (RDN) attribute for the LDAP service instance.

Group base DN

Specify the DN of the container or base point where the groups are stored.

Initial group member

Specifies a DN used to create the LDAP group. It is prefilled with `cn=TIM Adapter`. Optionally, you can customize this initial group member.

Group object class name

Select the group object class for example `GroupOfNames`.

Group membership attribute

Select the group membership attribute for example `member`.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Vault Service: Service Information

Specify information about the vault service.

The vault service type creates a service where the privileged accounts are only for vault use. There is no connection to the endpoint service. These accounts are created locally and loaded into the credential vault so that they can be shared.

If you select a service profile for a vault service, complete the following fields to connect to the server where the service is located:

Service name

Specify a name that helps you identify the service instance.

Description

Specify more information about the service instance.

Service

Click **Search** to specify an existing service instance. You can have only one vault service for every remote service.

Click **Clear** to remove the currently specified service.

Owner

Specify the existing user ID of the service owner that administers the service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user can administer the service instance.

Uniform Resource Identifier

Enter one or more URIs that identify the vault.

Click **Add** to add the URI to the list.

Click **Clear** to remove the URI from the list.

Click **Finish** when you are finished with this task.

General Information

Use this page to specify information about a service instance. The fields that are displayed on this page of the wizard vary based on the type of service that you selected in the previous panel.

You can specify a service instance for a managed resource. You provide information that IBM Security Identity Manager associates with a service instance. For example, an attribute might represent the administrative user ID and administrative password on a managed resource, or the Universal Resource Locator of the resource.

Alternatively, you can specify a service instance for activities that import identity data. You provide information that IBM Security Identity Manager uses during the data import, such as a file name or the data naming context.

Click **Test Connection** when the fields are complete, to test the connection to the managed resource. For manual services, the **Test Connection** button is not available.

If the connection is successful and SSL is configured, an informational message is displayed, indicating a successful connection. If the connection is successful and SSL is *not* configured, a warning message is displayed. If the connection fails, a warning message is displayed. You can continue with the wizard, even if the connection is not successful.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Solaris Profile: General Information

Use this page to specify information about the Solaris service instance.

The Solaris service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the Solaris service instance runs.

Description

Specify additional information about the Solaris service instance.

Connection mode

This option is available only if the `erconnectionmode` attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the Solaris resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the Solaris server when the account is deleted.

Ensure that you also set the home directory permissions, which by default are none. If no permissions are set, the home directory is not deleted when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the Solaris service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user be used in administering the service instance

Service prerequisite

Specify an existing service instance or function that the Solaris service instance requires.

Click **Search** to specify an existing service instance or function that the Linux service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Linux Profile: General Information

Use this page to specify information about the Linux service instance.

The Linux service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service is:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the Linux service instance runs.

Description

Specify additional information about the Linux service instance.

Connection mode

This option is available only if the *erconnectionmode* attribute is added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:1099/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the Linux resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

RXA Internet Command TimeOut

The RXA library is used for the internal communication between the adapter and the managed resource. By default, when RXA issues a command, it expects a response within 5000 milliseconds. This property is only used when the managed resource takes more than default time to respond and the RXA call fails with timeout error.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the Linux server when the account is deleted.

Ensure that you also set the home directory permissions, which by default are none. If no permissions are set, the home directory is not deleted when the account is deleted.

Use a shadow file?

Select this check box if you want to use an access-restricted ASCII system file that stores users' encrypted passwords and related information. This field is unique to the UNIX service types.

Return sudo privileges?

If checked, the adapter returns the sudo privileges granted to users and groups during reconciliation.

Path to the sudoers file

If it is not the default location `/etc/sudoers` on the resource, enter the directory path to the sudoers file.

Owner

Specify the existing user ID of the service owner that administers the Linux service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify to use any user in administering the service instance

Service prerequisite

Specify an existing service instance or function that the Linux service instance requires.

Click **Search** to specify an existing service instance or function that the Linux service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX HP-UX Profile: General Information

Use this page to specify information about the HP-UX service instance.

The HP-UX service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the HP-UX service instance runs.

Description

Specify additional information about the HP-UX service instance.

Connection mode

This option is available only if the `erconnectionmode` attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the HP-UX resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

Use a shadow file?

Select this check box to use an access-restricted ASCII system file that stores users' encrypted passwords and related information. This field is unique to the UNIX service types.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the HP-UX server when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the HP-UX service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify to use any user in administering the service instance.

Service prerequisite

Click **Search** to specify an existing service instance or function that the HP-UX service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX AIX Profile: General Information

Use this page to specify information about the AIX service instance.

The AIX service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the AIX service instance runs.

Description

Specify additional information about the AIX service instance.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the AIX resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

User registry

Specify how to manage and authenticate users.

- Leave Blank if the users on the service are to be managed only through the `/etc/password` file.
- Type `files` if this is a mixed setup and the users are to be managed through the `/etc/password` file.
- Type LDAP if this is a mixed setup and the users are to be managed through LDAP.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the AIX server when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the AIX service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user be used in administering the service instance

Service prerequisite

Specify an existing service instance or function that the AIX service instance requires.

If a service has another service defined as a service prerequisite, a user can only receive a new account if they have an existing account on the service prerequisite.

Related information

For more information, see the [IBM Knowledge Center](#).

Authentication

Use this page to configure authentication for the service. This page is displayed only if you are creating a POSIX service instance.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Solaris Profile: Authentication

Use this page to configure authentication for the Solaris service instance.

Administrator name

Specify the administrative user ID, such as root, for the Solaris server.

Is sudo user?

Select this check box if the administrator has sudo capability on the Solaris server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the Solaris server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the key store containing the private key of the client. This key store must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Linux Profile: Authentication

Use this page to configure authentication for the Linux service instance.

Administrator name

Specify the administrative user ID, such as root, for the Linux server.

Is sudo user?

Select this check box if the administrator has sudo capability on the Linux server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the Linux server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the key store containing the private key of the client. This key store must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX HP-UX Profile: Authentication

Use this page to configure authentication for the HP-UX service instance.

Administrator name

Specify the administrative user ID, such as root, for the HP-UX server.

Is sudo user?

Select this check box if the administrator has sudo capability on the HP-UX server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the HP-UX server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the key store containing the private key of the client. This key store must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX AIX Profile: Authentication

Use this page to configure authentication for the AIX service instance.

Administrator name

Specify the administrative user ID, such as root, for the AIX server.

Is sudo user?

Select this check box if the administrator has sudo capability on the AIX server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the AIX server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the keystore containing the private key of the client. This keystore must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Dispatcher Attributes

Use this page to specify information about the dispatcher attributes. This page is displayed only for Directory Integrator-based services.

AL FileSystem Path

Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines received from IBM Security Identity Manager. For example, you can specify the following file path to load the assembly lines from the profiles directory under these operating systems:

- Windows: c:\Files\IBM\TDI\profiles
- UNIX and Linux: system:/opt/IBM/TDI/profiles

Max Connection Count

Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. For example, enter 10 when you want the dispatcher to run maximum 10 assembly lines simultaneously for the service. If you enter 0, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.

Disable AL Caching

Select the check box to disable the assembly line caching in the dispatcher for the service. The assembly lines for add, modify, delete, and test operations are not cached.

Related information

For more information, see the [IBM Knowledge Center](#).

Status and Information

Use this page to view information about the adapter and managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. For example, ADK adapters do not include fields for TDI version and Dispatcher version, and TDI adapters do not include the ADK version field. The adapter must be running to obtain the information.

- Verify the adapter log to ensure that the IBM Security Identity Manager test request was successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify IBM Security Identity Manager service parameters for the adapter profile. For example, verify the workstation name or the IP address of the managed resource and the port.

Last status update: Date

Specifies the most recent date when the **Status and Information** tab was updated.

Last status update: Time

Specifies the most recent time of the date when the **Status and Information** tab was updated.

Managed resource status

Specifies the status of the managed resource that the adapter is connected to.

Managed resource version

Specifies the version of the managed resource.

Profile version

Specifies the version of the profile that is installed in the IBM Security Identity Manager server.

Adapter version

Specifies the version of the adapter that the IBM Security Identity Manager service uses to provision request to the managed resource.

TDI connector version

Specifies the version of the TDI connector.

Managed resource status message

Specifies the status message for the managed resource.

TDI version

Specifies the version of the Security Directory Integrator on which the adapter is deployed.

Dispatcher version

Specifies the version of the dispatcher.

ADK version

Specifies the version of the ADK that the adapter uses.

Installation platform

Specifies summary information about the operating system where the adapter is installed.

Adapter account

Specifies the account that running the adapter binary file.

Adapter up time: Date

Specifies the date when the adapter started.

Adapter up time: Time

Specifies the time of the date when the adapter started.

Adapter memory usage

Specifies the memory usage for running the adapter. If the connection fails, follow the instructions in the error message.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Access Information

Use the **Access Information** page to specify access information for a service of users, including the name, type, description, and other business metadata for accesses.

Define an Access

Select this check box to activate the fields that are required to define an access item. Clearing this check box clears the access item selection.

Note: If you clear this check box, the information that is contained in the fields is cleared only when the operation is completed.

Access name

Type a name to identify an access item.

Select access type

Select an access type from the **Access Types** tree structure.

Access Types

Expand or collapse a node in the tree to view and select an access type. For example, Application, Role, and other access types.

Access description

Provide more information about the access item.

Icon URL

Provide a uniform resource identifier (URI) string for the icon. A preview of the icon is displayed that is based on the following conditions:

- If an icon URL is not specified, and the category image exists, then the preview displays the category image. An information message is displayed that this image is used.
- If an icon URL is not specified, and the category image does not exist, then the preview displays a message that there is no image.
- If an icon URL is specified, then the referenced image is displayed.

For more information, see the [Customizing an access card in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Search terms

Type the search strings that you want to add to return specific search terms. You can use multiple values for the search terms.

Use these buttons for the search terms:

Add

Click to add a search term.


Delete

Click to delete one or more search terms.

Additional information

Displays information about the access card by default. It is a free form information about the access item that the administrator considers useful.

Badges

Specify one or more badges for an access item that is associated with this service. Click the twistie icon  next to **Badges** to specify one or more badges. You can add a maximum of five badges for an access item.

Use these buttons for the badges:

Add

Click to add a badge. The button becomes inactive after a maximum of five badges are assigned to an access item.

Remove

Click to remove a badge. The button is not active until a badge is added.

Select a check box next to a badge to modify or delete it.

Badge text

Type a short text string for the badge. For example, High risk.

To customize the value of a badge text, add a \$ prefix to it. For example, \$Risk. You can customize only the value of a badge text when it is prefixed with \$. For example, \$Risk=High Risk. You cannot customize a badge text if it is not prefixed with \$.

You might want to configure the CustomLabels.properties file to customize the value for the badge text. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Badge class

Select a specific CSS class from the list to apply to the badge text. You can customize a badge class, where you can specify your own styles to be displayed in the **Badge class** list. For example,

a CSS class can consist of font type, size, color, or other formatting styles, which you can apply to the specified badge text.

You might want to customize a badge CSS style to suit your requirements. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Preview

A preview displays the badge text that is based on the badge class you selected.

Configure Policy

Use this page to configure a provisioning policy that makes the service available to users. The page is not displayed if you are creating a service for an identity feed.

You can generate a policy that is automatically used or manually configured. Alternatively, you can manually configure the policy at a later time. Generating a policy that is automatically used makes the service available to all users, and the Default Account Request Workflow is associated with the provisioning policy.

Specify whether or not to generate a policy for all users.

Yes, create a policy for manually requesting accounts

Select this option to require that users manually request account entitlement.

Yes, create a policy to automatically create accounts, and later enable the policy

Select this option to allow for automatic provisioning of new accounts to users. You must subsequently enable the policy to provision new accounts.

Yes, create a policy to automatically create accounts as soon as the policy exists

Select this option to allow for automatic provisioning of new accounts to users. Provisioning of new accounts occurs as soon as the policy exists, and the Default Account Request Workflow is associated with the provisioning policy.

No, I will manually configure a policy later

Select this option if you want to configure a provisioning policy at a later time.

You might manually configure a provisioning policy if you need to set up account defaults or identity policies for this service. Later, you can change the provisioning to automatic.

Related information

For more information, see the [IBM Knowledge Center](#).

Reconcile Supporting Data

Use this page to schedule an account reconciliation for the service. This page is displayed only if you are creating an LDAP service instance or a POSIX service instance.

Perform a supporting data reconciliation now

Select this check box to start reconciliation immediately after you click **OK**.

Schedule supporting data reconciliation

The fields displayed vary, depending on the scheduling option that is selected. Select one of these schedule intervals to reconcile accounts for this service:

Daily

Reconciles accounts every day. After you select this option, click the clock icon to specify a time in the **At this time** field.

Weekly

Reconciles accounts once a week. After you select this option, select a day from the **On this day of the week** list, and then click the clock icon to specify a time in the **At this time** field.

Monthly

Reconciles accounts once a month. After you select this option, select a date from the **On this day of the month** list, and then click the clock icon to specify a time in the **At this time** field.

Hourly

Reconciles accounts once an hour. After you select this option, select a time from the **At this minute** list.

Annually - On a specific day of the year

Reconciles accounts on a specific date and time. After you select this option, select a month from the **Month** list. Then select a date from the **On this day of the month** list, and then click the clock icon to specify a time in the **At this time** field.

During a specific month

Reconciles accounts on a specific month, day, and time. After you select this option, select a month from the **Month** list. Then select a day from the **On this day of the week** list, and then click the clock icon to specify a time in the **At this time** field.

Never

Never reconciles accounts.

Click **Finish** when you are done with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Participants

Use this page to specify participant information. This page is displayed only if you are creating a manual service.

Participant type

Indicates the type of participant that you select. Possible participant types include:

- Administrator
- Service owner
- Manager
- User
- Group

Person name

Displays the person's name. This field is displayed only when the **User** participant type is selected.

Group name

Displays the group's name. This field is displayed only when the **Group** participant type is selected.

Escalation time in days

The amount of time in days the participant has to perform an activity before the activity is escalated.

Escalation participant type

Indicates the type of escalation participant that you select. Possible escalation participant types include:

- Administrator
- Service owner
- Manager
- User
- Group

Person name

Displays the person's name. This field is displayed only when the **User** escalation participant type is selected.

Group name

Displays the group's name. This field is displayed only when the **Group** escalation participant type is selected.

Click **Finish** when you are done with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Messages

Optionally, use this page to change the contents of an email message to send when corresponding operations are performed. This page is displayed only for manual services.

This **Messages** page is available only when you select **Manual** from **Connection mode**. For information about Connection mode, see [“POSIX Solaris Profile: General Information” on page 80](#)

Messages table

Lists the email messages to send when corresponding operations are performed. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates the message that is selected.

Operation

Identifies the operation that must be performed to send the email message.

Subject

Identifies the subject of the email message.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Change** to change the contents of the selected message.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Reconciliation

Optionally, use this page to specify a reconciliation file. This page is displayed only if you are creating a manual service.

Reconcile supporting data only

Select this check box to reconcile only supporting data from the inputted CSV file. No account data is reconciled. Group information is added or updated in IBM Security Identity Manager, but accounts are not added or updated.

Reconciliation file

Identifies the name of the reconciliation file that you select. The file cannot contain binary attributes. If you include multivalued attributes, they must be represented by using multiple columns with the same attribute name.

You can use these buttons:

Browse

Click to navigate to the reconciliation file.

Upload file

Click to upload the reconciliation file to the system.

Click **Finish** when you are done with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Search Results

Use this page to view information found for your search. Both the title of the page and the data in the table vary, depending on the field that you selected in the previous panel.

Lists the objects matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates the object that is selected.

Name

Identifies the name of the object to locate, based on the field that you selected in the previous panel.

Description

Describes the object. This column of information occurs if you previously customized an account request to include a group description and this panel is generated by a group search on account request.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Change a Service

Use this page to change information about a service instance. The tabs available vary depending on the type of service you are creating.

Click **Test Connection** when the fields are complete, to test the connection to the managed resource.

Related information

For more information, see the [IBM Knowledge Center](#).

Service Information

Use this page to change information about a service instance. The fields that are displayed on this page of the wizard vary based on the type of service that you selected in the previous panel.

You can specify a service instance for a managed resource. You provide information that IBM Security Identity Manager associates with a service instance. For example, an attribute might represent the administrative user ID and administrative password on a managed resource, or the Universal Resource Locator (URL) of the resource.

Alternatively, you can specify a service instance for activities that import identity data. You provide information that IBM Security Identity Manager uses during the data import, such as a file name or the data naming context.

Click **Test Connection** when the fields are complete, to test the connection to the managed resource. For manual services, the **Test Connection** button is not available.

If the connection is successful and SSL is configured, an informational message is displayed, indicating a successful connection. If the connection is successful and SSL is *not* configured, a warning message is displayed. If the connection fails, a warning message is displayed. You can continue with the wizard, even if the connection is not successful.

ITIM Service

Use this page to specify information about the ITIM Service.

If you select a service profile for an ITIM Service, complete these fields to connect to the server where the service resides:

Service name

Specifies a name that helps you identify the service instance.

Owner

Specifies the existing user ID of the service owner that administers the service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that the service instance does not have an assigned owner.

WebSphere account repository

Specifies the existing account repository used by IBM Security Identity Manager for authentication.

- If IBM Security Identity Manager is installed and configured to use its own custom registry, the default value for the service is **ITIM Service**.
- If IBM Security Identity Manager is installed to use an external user registry that is used by WebSphere Application Server, then:
 - If the external user registry is a service that is managed by IBM Security Identity Manager, click **Search** to locate and specify the service.

Note: You must create a service for the user registry before you enter the name of the service in this field. If you have not created the service, see the topic *Creating services* in the *IBM Security Identity Manager Administration Guide*.
 - If the external user registry is *not* a service that is managed by IBM Security Identity Manager, this field must be empty. Click **Clear** to remove any value that is in the field.
- If IBM Security Identity Manager is installed to use its own custom registry, but you want to change the configuration to use an external user registry, you must reconfigure IBM Security Identity Manager before you modify the value of this field:
 1. Complete the instructions in the topic *Reconfiguration for authentication with an external user registry* in the *IBM Security Identity Manager Installation Guide*. You can view this document on the IBM Security Identity Manager information center
 2. After you complete the reconfiguration:
 - If the external user registry is a service that is managed by IBM Security Identity Manager, click **Search** to locate and specify the service.

Note: You must create a service for the user registry before you enter the name of the service in this field. If you have not created the service, see the topic *Creating services* in the *IBM Security Identity Manager Administration Guide*.
 - If the external user registry is *not* a service that is managed by IBM Security Identity Manager, this field must be empty. Click **Clear** to remove any value that is in the field.

Usage notes:

- If the value of **WebSphere account repository** is not set, or if the value is anything other than **ITIM Service**, then you cannot change the Identity Manager account password.
- If you change the value of **WebSphere account repository**, you might need to wait a few minutes for the profile of the Identity Manager account to be refreshed in order to see the effective change. In WebSphere cluster environments, the changed value may not be propagated to each node until the next refresh interval of the profiles. If you change **WebSphere account repository** from **ITIM Service** to another service, or to no value, the disabling of the password change feature does not take effect until the profile is refreshed.
- This property relates to both forgotten password enablement and the WebSphere user registry configuration under which IBM Security Identity Manager is deployed. For the forgotten password feature to function correctly, set this value to the service that corresponds to the configured user repository in WebSphere. This setting determines the account password to change after the challenge questions are answered successfully. If the WebSphere Application Server account repository value is not set, the forgotten password option is not enabled regardless of the setting on the **Configure Forgotten Password** page and the forgotten password option is not available on the **Login** page.

Hosted Service: Service Information

Use this page to specify information about the hosted service.

Note: Accesses that are defined on the original service are not available for the hosted service, and those accesses cannot be requested by users in different organizations.

If you select a service profile for a hosted service, complete these fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance.

Description

Specify additional information about the service instance.

Service

Click **Search** to specify an existing service instance.

Click **Clear** to remove the currently specified service.

Service prerequisite

Click **Search** to specify an existing service instance or function that the hosted service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user can only receive a new account if they have an existing account on the service prerequisite.

Owner

Specify the existing user ID of the service owner that administers the service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user be used in administering the service instance

Click **Finish** when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

DSML Identity Feed: Service Information

Use this page to specify information about the Directory Services Markup Language (DSML) identity feed.

If you select a service profile to import identity data using DSML, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

User ID

Specify the administrative user ID for the service instance.

Password

Specify the administrative password for the service instance. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

File name

Specify the file name, including the path name, that contains the user information.

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

IDI Data Feed: Service Information

Use this page to specify information about the Initial Domain Identifier (IDI) identity feed.

If you select a service profile for activities that use IBM Security Directory Integrator to import identity data, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the name of the principal to authenticate clients using the Java Naming and Directory Interface (JNDI) application programming interface.

Password

Specify the password to authenticate clients using the JNDI application programming interface. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Name attribute

Select an attribute, such as `uid`, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

InetOrgPerson Identity Feed: Service Information

Use this page to specify information about the INetOrgPerson identity feed.

If you select a service profile to import identity data using LDAP, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the distinguished name (DN) of the administrator who is authorized to access the LDAP server that provides the identity information. For example, the user ID on LDAP is `cn=Administrator,cn=users,dc=itimcv,dc=com`, where *itimcv* is the domain name.

Password

Specify the password for the administrator who is authorized to access the LDAP server that provides the identity feed. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Attribute mapping file name

Specify the absolute path and file name of the file that contains attribute mapping between the identity feed source schema and specified user type schema. The mapping file contains key value pairs that identify the source and target attribute mapping.

Name attribute

Select an attribute, such as `uid`, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

AD OrganizationalPerson Identity Feed: Service Information

Use this page to specify information about the Active Directory OrganizationalPerson identity feed.

If you select a service profile to import identity data using Active Directory, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the distinguished name (DN) of the administrator who is authorized to access the LDAP server that provides the identity information. For example, the user ID on LDAP is `cn=Administrator,cn=users,dc=itimcv,dc=com`, where *itimcv* is the domain name.

Password

Specify the password for the administrator who is authorized to access the LDAP server that provides the identity feed. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Attribute mapping file name

Specify the absolute path and file name of the file that contains attribute mapping between the identity feed source schema and specified user type schema. The mapping file contains key value pairs that identify the source and target attribute mapping.

Name attribute

Select an attribute, such as `uid`, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

CSV Identity Feed: Service Information

Use this page to specify information about the comma-separated value (CSV) identity feed.

The comma-separated value (CSV) file cannot contain binary attributes. If you include multivalued attributes, they must be represented by using multiple columns with the same attribute name. You must list all required attributes in the CSV file before you list optional attributes.

If you select a service profile for activities that use a CSV format to import identity data, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

File name

Specify the file name, including the path name, of the CSV file.

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Name attribute

Select an attribute, such as uid, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP Profile: Service Information

Use this page to specify information about the Lightweight Directory Access Protocol (LDAP) service instance.

The LDAP service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

LDAP service

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the LDAP service instance runs.

Description

Specify additional information about the LDAP service instance.

Connection mode

This option is available only if the erconnectionmode attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`. Where *ip-address* is the Security Directory Integrator host and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Directory server location

Specify the location and port number of the LDAP Adapter. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `ldap://[address]:port number`.

Use SSL communication with LDAP?

Select this check box to use secure communication with the LDAP service instance.

Administrator name

Specify the administrative user ID, such as `cn=root`, for the LDAP service instance. The name must be a distinguished name (DN).

Password

Specify the administrative password for the LDAP service instance. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Directory server name

Choose a directory server from the list.

Owner

Click **Search** to specify the existing user ID of the service owner that administers the LDAP service instance.

Click **Clear** to remove the currently specified user.

Service prerequisite

Click **Search** to specify an existing service instance or function that the LDAP service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user can only receive a new account if they have an existing account on the service prerequisite.

Users and groups**User base DN**

Specify the distinguished name (DN) of the container or base point where the users are stored.

RDN attribute

Specify the required relative distinguished name (RDN) attribute for the LDAP service instance.

Group base DN

Specify the DN of the container or base point where the groups are stored.

Initial group member

Specifies a DN used to create the LDAP group. It is prefilled with `cn=TIM Adapter`. Optionally, you can customize this initial group member.

Group object class name

Select the group object class for example `GroupOfNames`.

Group membership attribute

Select the group membership attribute for example `member`.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

General Information

Use this page to specify information about a service instance. The fields that are displayed on this page of the wizard vary based on the type of service that you selected in the previous panel.

You can specify a service instance for a managed resource. You provide information that IBM Security Identity Manager associates with a service instance. For example, an attribute might represent the administrative user ID and administrative password on a managed resource, or the Universal Resource Locator of the resource.

Alternatively, you can specify a service instance for activities that import identity data. You provide information that IBM Security Identity Manager uses during the data import, such as a file name or the data naming context.

Click **Test Connection** when the fields are complete, to test the connection to the managed resource. For manual services, the **Test Connection** button is not available.

If the connection is successful and SSL is configured, an informational message is displayed, indicating a successful connection. If the connection is successful and SSL is *not* configured, a warning message is displayed. If the connection fails, a warning message is displayed. You can continue with the wizard, even if the connection is not successful.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Solaris Profile: General Information

Use this page to specify information about the Solaris service instance.

The Solaris service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the Solaris service instance runs.

Description

Specify additional information about the Solaris service instance.

Connection mode

This option is available only if the `erconnectionmode` attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the Solaris resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the Solaris server when the account is deleted.

Ensure that you also set the home directory permissions, which by default are none. If no permissions are set, the home directory is not deleted when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the Solaris service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user be used in administering the service instance

Service prerequisite

Specify an existing service instance or function that the Solaris service instance requires.

Click **Search** to specify an existing service instance or function that the Linux service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Linux Profile: General Information

Use this page to specify information about the Linux service instance.

The Linux service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service is:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the Linux service instance runs.

Description

Specify additional information about the Linux service instance.

Connection mode

This option is available only if the *erconnectionmode* attribute is added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:1099/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the Linux resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

RXA Internet Command TimeOut

The RXA library is used for the internal communication between the adapter and the managed resource. By default, when RXA issues a command, it expects a response within 5000 milliseconds. This property is only used when the managed resource takes more than default time to respond and the RXA call fails with timeout error.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the Linux server when the account is deleted.

Ensure that you also set the home directory permissions, which by default are none. If no permissions are set, the home directory is not deleted when the account is deleted.

Use a shadow file?

Select this check box if you want to use an access-restricted ASCII system file that stores users' encrypted passwords and related information. This field is unique to the UNIX service types.

Return sudo privileges?

If checked, the adapter returns the sudo privileges granted to users and groups during reconciliation.

Path to the sudoers file

If it is not the default location `/etc/sudoers` on the resource, enter the directory path to the sudoers file.

Owner

Specify the existing user ID of the service owner that administers the Linux service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify to use any user in administering the service instance

Service prerequisite

Specify an existing service instance or function that the Linux service instance requires.

Click **Search** to specify an existing service instance or function that the Linux service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX HP-UX Profile: General Information

Use this page to specify information about the HP-UX service instance.

The HP-UX service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the HP-UX service instance runs.

Description

Specify additional information about the HP-UX service instance.

Connection mode

This option is available only if the `erconnectionmode` attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the HP-UX resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

Use a shadow file?

Select this check box to use an access-restricted ASCII system file that stores users' encrypted passwords and related information. This field is unique to the UNIX service types.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the HP-UX server when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the HP-UX service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify to use any user in administering the service instance.

Service prerequisite

Click **Search** to specify an existing service instance or function that the HP-UX service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX AIX Profile: General Information

Use this page to specify information about the AIX service instance.

The AIX service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the AIX service instance runs.

Description

Specify additional information about the AIX service instance.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and

port is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the AIX resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

User registry

Specify how to manage and authenticate users.

- Leave Blank if the users on the service are to be managed only through the `/etc/password` file.
- Type `files` if this is a mixed setup and the users are to be managed through the `/etc/password` file.
- Type LDAP if this is a mixed setup and the users are to be managed through LDAP.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the AIX server when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the AIX service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user be used in administering the service instance

Service prerequisite

Specify an existing service instance or function that the AIX service instance requires.

If a service has another service defined as a service prerequisite, a user can only receive a new account if they have an existing account on the service prerequisite.

Related information

For more information, see the [IBM Knowledge Center](#).

Authentication

Use this page to configure authentication for the service. This page is displayed only if you are creating a POSIX service instance.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Solaris Profile: Authentication

Use this page to configure authentication for the Solaris service instance.

Administrator name

Specify the administrative user ID, such as `root`, for the Solaris server.

Is sudo user?

Select this check box if the administrator has `sudo` capability on the Solaris server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the Solaris server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the key store containing the private key of the client. This key store must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Linux Profile: Authentication

Use this page to configure authentication for the Linux service instance.

Administrator name

Specify the administrative user ID, such as root, for the Linux server.

Is sudo user?

Select this check box if the administrator has sudo capability on the Linux server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the Linux server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the key store containing the private key of the client. This key store must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX HP-UX Profile: Authentication

Use this page to configure authentication for the HP-UX service instance.

Administrator name

Specify the administrative user ID, such as root, for the HP-UX server.

Is sudo user?

Select this check box if the administrator has sudo capability on the HP-UX server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the HP-UX server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the key store containing the private key of the client. This key store must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX AIX Profile: Authentication

Use this page to configure authentication for the AIX service instance.

Administrator name

Specify the administrative user ID, such as root, for the AIX server.

Is sudo user?

Select this check box if the administrator has sudo capability on the AIX server.

Authentication method

Select the authentication method.

Password Based Authentication uses a password to authenticate users.

Key Based Authentication requires the use of a passphrase and private key file to authenticate users.

Password

Specify the administrative password for the AIX server. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Passphrase (Required for key based authentication)

Enter the passphrase to use for key based authentication.

Private key file (Required for key based authentication)

Specify the full path and file name of the keystore containing the private key of the client. This keystore must be on the machine running the Tivoli Directory Integrator server.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Dispatcher Attributes

Use this page to specify information about the dispatcher attributes. This page is displayed only for Directory Integrator-based services.

AL FileSystem Path

Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines received from IBM Security Identity Manager. For

example, you can specify the following file path to load the assembly lines from the profiles directory under these operating systems:

- Windows: c:\Files\IBM\TDI\profiles
- UNIX and Linux: system:/opt/IBM/TDI/profiles

Max Connection Count

Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. For example, enter 10 when you want the dispatcher to run maximum 10 assembly lines simultaneously for the service. If you enter 0, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.

Disable AL Caching

Select the check box to disable the assembly line caching in the dispatcher for the service. The assembly lines for add, modify, delete, and test operations are not cached.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Information

Use the **Access Information** page to specify access information for a service of users, including the name, type, description, and other business metadata for accesses.

Define an Access

Select this check box to activate the fields that are required to define an access item. Clearing this check box clears the access item selection.

Note: If you clear this check box, the information that is contained in the fields is cleared only when the operation is completed.

Access name

Type a name to identify an access item.

Select access type

Select an access type from the **Access Types** tree structure.

Access Types

Expand or collapse a node in the tree to view and select an access type. For example, Application, Role, and other access types.

Access description

Provide more information about the access item.

Icon URL

Provide a uniform resource identifier (URI) string for the icon. A preview of the icon is displayed that is based on the following conditions:

- If an icon URL is not specified, and the category image exists, then the preview displays the category image. An information message is displayed that this image is used.
- If an icon URL is not specified, and the category image does not exist, then the preview displays a message that there is no image.
- If an icon URL is specified, then the referenced image is displayed.

For more information, see the [Customizing an access card in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Search terms

Type the search strings that you want to add to return specific search terms. You can use multiple values for the search terms.

Use these buttons for the search terms:

Add

Click to add a search term.


Delete

Click to delete one or more search terms.

Additional information

Displays information about the access card by default. It is a free form information about the access item that the administrator considers useful.

Badges

Specify one or more badges for an access item that is associated with this service. Click the twistie icon  next to **Badges** to specify one or more badges. You can add a maximum of five badges for an access item.

Use these buttons for the badges:

Add

Click to add a badge. The button becomes inactive after a maximum of five badges are assigned to an access item.

Remove

Click to remove a badge. The button is not active until a badge is added.

Select a check box next to a badge to modify or delete it.

Badge text

Type a short text string for the badge. For example, High risk.

To customize the value of a badge text, add a \$ prefix to it. For example, \$Risk. You can customize only the value of a badge text when it is prefixed with \$. For example, \$Risk=High Risk. You cannot customize a badge text if it is not prefixed with \$.

You might want to configure the `CustomLabels.properties` file to customize the value for the badge text. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Badge class

Select a specific CSS class from the list to apply to the badge text. You can customize a badge class, where you can specify your own styles to be displayed in the **Badge class** list. For example, a CSS class can consist of font type, size, color, or other formatting styles, which you can apply to the specified badge text.

You might want to customize a badge CSS style to suit your requirements. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Preview

A preview displays the badge text that is based on the badge class you selected.

Status and Information

Use this page to view information about the adapter and managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. For example, ADK adapters do not include fields for TDI version and Dispatcher version, and TDI adapters do not include the ADK version field. The adapter must be running to obtain the information.

- Verify the adapter log to ensure that the IBM Security Identity Manager test request was successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify IBM Security Identity Manager service parameters for the adapter profile. For example, verify the workstation name or the IP address of the managed resource and the port.

Last status update: Date

Specifies the most recent date when the **Status and Information** tab was updated.

Last status update: Time

Specifies the most recent time of the date when the **Status and Information** tab was updated.

Managed resource status

Specifies the status of the managed resource that the adapter is connected to.

Managed resource version

Specifies the version of the managed resource.

Profile version

Specifies the version of the profile that is installed in the IBM Security Identity Manager server.

Adapter version

Specifies the version of the adapter that the IBM Security Identity Manager service uses to provision request to the managed resource.

TDI connector version

Specifies the version of the TDI connector.

Managed resource status message

Specifies the status message for the managed resource.

TDI version

Specifies the version of the Security Directory Integrator on which the adapter is deployed.

Dispatcher version

Specifies the version of the dispatcher.

ADK version

Specifies the version of the ADK that the adapter uses.

Installation platform

Specifies summary information about the operating system where the adapter is installed.

Adapter account

Specifies the account that running the adapter binary file.

Adapter up time: Date

Specifies the date when the adapter started.

Adapter up time: Time

Specifies the time of the date when the adapter started.

Adapter memory usage

Specifies the memory usage for running the adapter. If the connection fails, follow the instructions in the error message.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Participants

Use this page to specify participant information. This page is displayed only if you are changing a manual service.

Participant type

Indicates the type of participant that you select. Possible participant types include:

- Administrator
- Service owner
- Manager
- User
- Group

Person name

Indicates the person's name. This field is displayed only when the **User** participant type is selected.

Group name

Indicates the group's name. This field is displayed only when the **Group** participant type is selected.

Escalation time in days

The amount of time in days the participant has to perform an activity before the activity is escalated.

Escalation participant type

Indicates the type of escalation participant that you select. Possible escalation participant types include:

- Administrator
- Service owner
- Manager
- User
- Group

Person name

Indicates the person's name. This field is displayed only when the **User** escalation participant type is selected.

Group name

Indicates the group's name. This field is displayed only when the **Group** escalation participant type is selected.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Messages

Optionally, use this page to change the contents of an email message to send when corresponding operations are performed. This page is displayed only for manual services.

This **Messages** page is available only when you select **Manual** from **Connection mode**. For information about Connection mode, see "[POSIX Solaris Profile: General Information](#)" on page 80

Messages table

Lists the email messages to send when corresponding operations are performed. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates the message that is selected.

Operation

Identifies the operation that must be performed to send the email message.

Subject

Identifies the subject of the email message.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Change** to change the contents of the selected message.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Participants

Use this page to specify participant information. This page is displayed only if you are changing a manual service.

Participant type

Indicates the type of participant that you select. Possible participant types include:

- Administrator
- Service owner
- Manager
- User
- Group

Person name

Indicates the person's name. This field is displayed only when the **User** participant type is selected.

Group name

Indicates the group's name. This field is displayed only when the **Group** participant type is selected.

Escalation time in days

The amount of time in days the participant has to perform an activity before the activity is escalated.

Escalation participant type

Indicates the type of escalation participant that you select. Possible escalation participant types include:

- Administrator
- Service owner
- Manager
- User
- Group

Person name

Indicates the person's name. This field is displayed only when the **User** escalation participant type is selected.

Group name

Indicates the group's name. This field is displayed only when the **Group** escalation participant type is selected.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Reconciliation

Optionally, use this page to specify a reconciliation file. This page is displayed only if you are changing a manual service.

Reconcile supporting data only

Select this check box to reconcile only supporting data from the inputted CSV file. No account data is reconciled. Group information is added or updated in IBM Security Identity Manager, but accounts are not added or updated.

Reconciliation file

Identifies the name of the reconciliation file that you select. The file cannot contain binary attributes. If you include multivalued attributes, they must be represented by using multiple columns with the same attribute name.

You can use these buttons:

Browse

Click to navigate to the reconciliation file.

Upload file

Click to upload the reconciliation file to the system.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Change a Manual Service

Use this page to change the general information, participants, e-mail messages, and reconciliation file for a manual service instance.

Related information

For more information, see the [IBM Knowledge Center](#).

General Information

Use this page to specify general information about the manual service.

The fields that are displayed on this page vary, depending on the way you configured the service type that was used to create this manual service.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Information

Use the **Access Information** page to specify access information for a service of users, including the name, type, description, and other business metadata for accesses.

Define an Access

Select this check box to activate the fields that are required to define an access item. Clearing this check box clears the access item selection.

Note: If you clear this check box, the information that is contained in the fields is cleared only when the operation is completed.

Access name

Type a name to identify an access item.

Select access type

Select an access type from the **Access Types** tree structure.

Access Types

Expand or collapse a node in the tree to view and select an access type. For example, Application, Role, and other access types.

Access description

Provide more information about the access item.

Icon URL

Provide a uniform resource identifier (URI) string for the icon. A preview of the icon is displayed that is based on the following conditions:

- If an icon URL is not specified, and the category image exists, then the preview displays the category image. An information message is displayed that this image is used.
- If an icon URL is not specified, and the category image does not exist, then the preview displays a message that there is no image.
- If an icon URL is specified, then the referenced image is displayed.

For more information, see the [Customizing an access card in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Search terms

Type the search strings that you want to add to return specific search terms. You can use multiple values for the search terms.

Use these buttons for the search terms:

Add

Click to add a search term.


Delete

Click to delete one or more search terms.

Additional information

Displays information about the access card by default. It is a free form information about the access item that the administrator considers useful.

Badges

Specify one or more badges for an access item that is associated with this service. Click the twistie icon  next to **Badges** to specify one or more badges. You can add a maximum of five badges for an access item.

Use these buttons for the badges:

Add

Click to add a badge. The button becomes inactive after a maximum of five badges are assigned to an access item.

Remove

Click to remove a badge. The button is not active until a badge is added.

Select a check box next to a badge to modify or delete it.

Badge text

Type a short text string for the badge. For example, High risk.

To customize the value of a badge text, add a \$ prefix to it. For example, \$Risk. You can customize only the value of a badge text when it is prefixed with \$. For example, \$Risk=High Risk. You cannot customize a badge text if it is not prefixed with \$.

You might want to configure the `CustomLabels.properties` file to customize the value for the badge text. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Badge class

Select a specific CSS class from the list to apply to the badge text. You can customize a badge class, where you can specify your own styles to be displayed in the **Badge class** list. For example, a CSS class can consist of font type, size, color, or other formatting styles, which you can apply to the specified badge text.

You might want to customize a badge CSS style to suit your requirements. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Preview

A preview displays the badge text that is based on the badge class you selected.

Participants

Use this page to specify participant information. This page is displayed only if you are changing a manual service.

Participant type

Indicates the type of participant that you select. Possible participant types include:

- Administrator
- Service owner
- Manager

- User
- Group

Person name

Indicates the person's name. This field is displayed only when the **User** participant type is selected.

Group name

Indicates the group's name. This field is displayed only when the **Group** participant type is selected.

Escalation time in days

The amount of time in days the participant has to perform an activity before the activity is escalated.

Escalation participant type

Indicates the type of escalation participant that you select. Possible escalation participant types include:

- Administrator
- Service owner
- Manager
- User
- Group

Person name

Indicates the person's name. This field is displayed only when the **User** escalation participant type is selected.

Group name

Indicates the group's name. This field is displayed only when the **Group** escalation participant type is selected.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Messages

Optionally, use this page to change the contents of an email message to send when corresponding operations are performed. This page is displayed only for manual services.

This **Messages** page is available only when you select **Manual** from **Connection mode**. For information about Connection mode, see "[POSIX Solaris Profile: General Information](#)" on page 80

Messages table

Lists the email messages to send when corresponding operations are performed. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates the message that is selected.

Operation

Identifies the operation that must be performed to send the email message.

Subject

Identifies the subject of the email message.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Change** to change the contents of the selected message.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Reconciliation

Optionally, use this page to specify a reconciliation file. This page is displayed only if you are changing a manual service.

Reconcile supporting data only

Select this check box to reconcile only supporting data from the inputted CSV file. No account data is reconciled. Group information is added or updated in IBM Security Identity Manager, but accounts are not added or updated.

Reconciliation file

Identifies the name of the reconciliation file that you select. The file cannot contain binary attributes. If you include multivalued attributes, they must be represented by using multiple columns with the same attribute name.

You can use these buttons:

Browse

Click to navigate to the reconciliation file.

Upload file

Click to upload the reconciliation file to the system.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Change Message: *Operation*

Use this page to modify the contents of an e-mail message to send to the selected operation.

Subject

Specify the subject of the e-mail message.

Plaintext body

Specify the main content of the notification message in plaintext format. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Specify the XHTML body of the notification message. The content in this section can include images and hyperlinks.

Related information

For more information, see the [IBM Knowledge Center](#).

Set Up Account Reconciliation

Use this page to create, change, or delete a scheduled reconciliation.

Lists the reconciliation schedules for a service. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a schedule. To select one or more schedules, select the check box adjacent to the schedule. To select all schedules, select the check box at the top of the column.

Name

Identifies the name of a schedule. Click the name of the schedule to view or change its details.

Schedule

Provides interval and date information about a scheduled reconciliation.

Description

Provides additional information about the schedule.

Check policy during reconciliation

Indicates whether the policy is enforced on an account during reconciliation.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new schedule.

Change

Click to change the information for the selected schedule.

Delete

Click to delete the selected schedule.

Related information

[For more information, see the IBM Knowledge Center.](#)

Set Up Account Reconciliation

Use this notebook to define account reconciliation information, schedule, and query a service. The tabs that are available for this notebook vary, depending on the service type.

Related information

[For more information, see the IBM Knowledge Center.](#)

General

Use this page to specify reconciliation information for a service.

Display name

Identifies the name of the reconciliation schedule for display purposes.

Description

Provides a description of the reconciliation schedule.

Lock service during reconciliation

Indicates whether other provisioning requests are queued until an active reconciliation completes.

Maximum duration (minutes)

Indicates the maximum amount of time in minutes that a reconciliation can run.

Click other tabs to specify additional information.

Related information

[For more information, see the IBM Knowledge Center.](#)

Schedule

Use this page to schedule a reconciliation for the accounts on the managed resource.

The fields displayed vary, depending on the scheduling option that is selected. Select one of these schedule intervals to reconcile accounts for this service:

Daily

Reconciles accounts every day. After you select this option, click the clock icon to specify a time in the **At this time** field.

Weekly

Reconciles accounts once a week. After you select this option, select a day from the **On this day of the week** list, and then click the clock icon to specify a time in the **At this time** field.

Monthly

Reconciles accounts once a month. After you select this option, select a date from the **On this day of the month** list, and then click the clock icon to specify a time in the **At this time** field.

Hourly

Reconciles accounts once an hour. After you select this option, select a time from the **At this minute** list.

Annually - On a specific day of the year

Reconciles accounts on a specific date and time. After you select this option, select a month from the **Month** list. Then select a date from the **On this day of the month** list, and then click the clock icon to specify a time in the **At this time** field.

During a specific month

Reconciles accounts on a specific month, day, and time. After you select this option, select a month from the **Month** list. Then select a day from the **On this day of the week** list, and then click the clock icon to specify a time in the **At this time** field.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Query

Use this page to specify a reconciliation query.

Reconcile supporting data only

Indicates whether to reconcile supporting data from the managed resource instead of the actual accounts on the resource. For example, supporting data might be a list of groups defined on the resource.

Reconcile accounts that match this filter

Indicates valid LDAP search filter statements that select a list of accounts to reconcile.

Available attributes

Identifies attributes that are not processed during reconciliation.

Selected attributes

Identifies attributes that are included in processing during reconciliation.

You can use these buttons:

Add

Click to add an attribute to the query.

Remove

Click to remove an attribute from the query.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Query

Use this page to select a reconciliation query to reconcile all accounts or selected accounts.

Query

None

Includes all accounts in the reconciliation.

Use query from existing schedule

Select a query for the reconciliation from an existing schedule. The **Reconciliation Schedule** table displays the reconciliation schedules for a service. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the schedule that you want to use.

Name

Identifies the name of a schedule.

Schedule

Provides interval and date information about a scheduled reconciliation.

Description

Provides additional information about the schedule.

Define query

Specify an LDAP search filter for account attributes to include in a query.

Reconcile supporting data only

Indicates whether to reconcile supporting data from the managed resource instead of the actual accounts on the resource. For example, supporting data might be a list of groups defined on the resource.

Reconcile accounts that match this filter

Indicates valid LDAP search filter statements that select a list of accounts to reconcile.

Available attributes

Identifies attributes that are not processed during reconciliation.

Selected attributes

Identifies attributes that are included in processing during reconciliation.

You can use these buttons:

Add

Click to add an attribute to the query.

Remove

Click to remove an attribute from the query.

Click **Submit** to submit your request.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Action

Use this page to specify the policy enforcement action that occurs for an account that has a noncompliant attribute.

Mark

Sets a mark on an account that has a noncompliant attribute.

Suspend

Suspends an account that has a noncompliant attribute.

Correct

Replaces a noncompliant attribute on an account with the correct attribute.

Alert

Issues an alert for an account that has a noncompliant attribute.

Use Global Enforcement Action: <action>

Specifies a global enforcement action for an account that has a noncompliant attribute. The current global setting is displayed.

You can use these buttons:

Submit

Click to save the selection and continue to the next page. This button is displayed when **Mark**, **Suspend**, **Correct**, or **Use Global Enforcement Action** is selected as the enforcement action.

Continue

Click to save the selection and continue to the next page. This button is displayed only when **Alert** is selected as the enforcement action.

Related information

For more information, see the [IBM Knowledge Center](#).

Configure Policy Enforcement

Use this notebook to configure policy enforcement for a service.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to specify an alert, including participants, escalation intervals, and process types.

Alert name

Type a name to identify the alert.

Send compliance alert to

Select the participant type you want to receive the unattended compliance alert to-do items. Depending on which type of participant you select, one of these fields might be displayed:

User (with ITIM Account) name

Specify the user name for the participant. Click **Browse** to navigate to a list of user names, or click **Clear** to remove the currently specified user name.

This field is displayed only when you select **User (with ITIM Account) name** in the previous field.

Organizational role name

Specify the organizational role name for the participant. Click **Browse** to navigate to a list of role names, or click **Clear** to remove the currently specified role name.

This field is displayed only when you select **Organizational Role** in the previous field.

Custom participant script

Type an LDAP search filter. The search filter is the search criteria for getting the participants.

This field is displayed only when you select **Custom-Defined Participant** in the previous field.

Number of days to wait before escalating compliance alert

Type the number of days to elapse before the unattended compliance alert to-do items are escalated and sent to the escalation participant.

Escalate compliance alert to

Select the second-level participant type you want to receive the unattended compliance alert to-do items. Depending on which type of participant you select, one of these fields might be displayed:

User (with ITIM Account) name

Specify the user name for the participant. Click **Browse** to navigate to a list of user names, or click **Clear** to remove the currently specified user name.

This field is displayed only when you select **User (with ITIM Account) name** in the previous field.

Organizational role name

Specify the organizational role name for the participant. Click **Browse** to navigate to a list of role names, or click **Clear** to remove the currently specified role name.

This field is displayed only when you select **Organizational Role** in the previous field.

Custom participant script

Type an LDAP search filter. The search filter is the search criteria for getting the participants.

This field is displayed only when you select **Custom-Defined Participant** in the previous field.

Number of days after which the system will take corrective action

Type the maximum number of days that the compliance alert to-do items can remain unanswered. When the number of days specified in this field is reached, the associated accounts are automatically corrected with the suggested values in the compliance alert to-do item.

Process Types table

Lists the processes that generate a compliance alert. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Generate Alert

Specifies a process type. To select one or more process types, select the check box adjacent to the process type. To select all process types, select the check box at the top of the column.

If the process type is checked, an alert is generated. Otherwise, the noncompliance is automatically corrected. Correction can result in either the account being modified to a compliance state, or deletion of the account if no entitlement is defined for the owner of the account.

Process Type

Indicates the type of workflow process that generates a compliance alert to-do item.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click other tabs to specify additional information. Then, click **Submit** to submit your request.

Related information

For more information, see the [IBM Knowledge Center](#).

E-mail

Use this page to specify an alert e-mail.

Use default template

Select this check box to use the default e-mail template instead of the custom fields for the alert. If this option is selected, the custom fields are read-only.

Subject

Type the subject line of the e-mail notification.

Plain text body

Type the plain text body of the e-mail notification.

XHTML body

Specify the XHTML dynamic content of the e-mail notification.

Click other tabs to specify additional information. Then, click **Submit** to submit your request.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Groups on Service

Use this page to search for a group or access definition.

Group information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Group searches for groups in which the group name contains the text that is entered in the **Group information** field.

Access searches for the name of the access definition that is associated with the group that is entered in the **Group information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Groups and Access table

Lists the groups matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group or access definition to which the **Define Access** button applies. To select one or more group or access definitions, select the check box adjacent to the group or access definition. To select all groups or access definitions, select the check box at the top of the column.

Common Access

Specifies whether the access defined for the group is visible to users. If no access is defined, or if the group is not enabled for access, the column is empty. Your selection is saved immediately.

Group Name

Identifies the group's name.

Click the name of the group to view the group details.

Click the icon (▶) adjacent to the group to show the tasks that can be performed on the group.

Use these menu items to perform a task on the selected group:

Define Access

Defines the group as an access.

Group Membership

Enables you to add users to, or remove users from, group membership.

Access Recertification Status

Identifies the recertification status for access definitions for the group.

Group Type

Displays the type of group, based on the group profile. For example, AIX types include AIX groups and AIX AIX.

Description

Displays information about the intended purpose of the group.

Access Name

Identifies the name of the access for the group. Click the access name for details about the access.

Access Type

Identifies the type of access, such as a shared folder.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Define Access

Click to define the group as an access.

Clear Access

Click to remove the group as an access.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Define Access

Use this notebook to define access for a group of users.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Information

Use the **Access Information** page to specify general information about the access, including the name, type, description, owner, and other business metadata for accesses.

Access name

Type a name to identify the access.

Access type

Select the type of access that is defined by the group.

Description

Provide more information about the access.

Access owner

Specify the user who has access ownership. To see a list of owners, click **Search**.

Display in Access List

Select this check box to include the access in the access list.

Display in Common Access list

Select this check box to include the access in a common access list that is visible to users.

Icon URL

Provide a uniform resource identifier (URI) string for the icon. A preview of the icon is displayed that is based on the following conditions:

- If an icon URL is not specified, and the category image exists, then the preview displays the category image. An information message is displayed that this image is used.
- If an icon URL is not specified, and the category image does not exist, then the preview displays a message that there is no image.
- If an icon URL is specified, then the referenced image is displayed.

For more information, see the [Customizing an access card in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Search terms

Type the search strings that you want to add to return specific search terms. You can use multiple values for the search terms.

Use these buttons for the search terms:

Add

Click to add a search term.


Delete

Click to delete one or more search terms.

Additional information

Displays information about the access card by default. It is a free form information about the access item that the administrator considers useful.

Badges

Specify one or more badges for an access item that is associated with this group. Click the twistie icon  next to **Badges** to specify one or more badges. You can add a maximum of five badges for an access item.

Use these buttons for the badges:

Add

Click to add a badge. The button becomes inactive after a maximum of five badges are assigned to an access item.

Remove

Click to remove a badge. The button is not active until a badge is added.

Select a check box next to a badge to modify or delete it.

Badge text

Type a short text string for the badge. For example, High risk.

To customize the value of a badge text, add a \$ prefix to it. For example, \$Risk. You can customize only the value of a badge text when it is prefixed with \$. For example, \$Risk=High Risk. You cannot customize a badge text if it is not prefixed with \$.

You might want to configure the CustomLabels.properties file to customize the value for the badge text. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Badge class

Select a specific CSS class from the list to apply to the badge text. You can customize a badge class, where you can specify your own styles to be displayed in the **Badge class** list. For example, a CSS class can consist of font type, size, color, or other formatting styles, which you can apply to the specified badge text.

You might want to customize a badge CSS style to suit your requirements. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Preview

A preview displays the badge text that is based on the badge class you selected.

Click other tabs to specify more information.

Related information

For more information, see the [IBM Knowledge Center](#).

Provisioning Options

Use this page to specify access approval and notification options.

Approval workflow

Specify whether no approval or specific approval is required to grant access.

Notify users when access is provisioned and available for use

Select this check box to ensure that users are notified when access is provisioned.

Notify users when access is de-provisioned

Select this check box to ensure that users are notified when access is de-provisioned.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Group Members

Use this page to add or remove accounts that are associated with a group.

Account information

Type the user ID or name of the user who owns the account in this field. If you do not know the name of the account that you want to find, you can type a portion of the name to display a list of accounts. If you do not type a value in this field or if you type an asterisk (*), and then click **Search**, the entire list of accounts is displayed as long as the number of accounts does not exceed the search limit.

Search by

Select the search category.

User ID searches for accounts with user IDs that contain the text that is entered in the **Search information** field.

Owner searches for accounts in which the full name of the account owner contains the text that is entered in the **Account information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Accounts table

Lists the accounts that match the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box next to the account. To select all accounts, select the check box at the top of the column.

State

Indicates the state of the group.

User ID

Identifies the user ID that is associated with the group. Click the user ID to review the account information.

Owner

Identifies the full name of the user who owns the account that is associated with the group. Click the name of the owner to view the personal profile of the user.

Ownership Type

Identifies the ownership of the account. The ownership type can be a default type of Device, Individual, System, or Vendor, or a custom ownership type.

Status

Indicates whether the account is active or inactive.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add accounts to the group.

Remove

Click to remove the selected accounts from the group

Add to Vault

Click to add the sponsored account to the credential vault so that the account can be shared. This function is available only if the Shared Access Module is installed.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Add Members

Use this page to add a group that has access to a specified account.

Account information

Type the user ID or name of the user who owns the account in this field. If you do not know the name of the account that you want to find, you can type a portion of the name to display a list of accounts. If you do not type a value in this field or if you type an asterisk (*), and then click **Search**, the entire list of accounts is displayed as long as the number of accounts does not exceed the search limit.

Search by

Select the search category.

User ID searches for accounts with user IDs that contain the text that is entered in the **Search information** field.

Owner searches for accounts in which the account owner's full name contains the text that is entered in the **Account information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Accounts table

Lists the accounts matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box adjacent to the account. To select all accounts, select the check box at the top of the column.

State

Indicates the state of the group.

User ID

Identifies the user ID that is associated with the group. Click the user ID to review the account information.

Owner

Identifies the full name of the user who owns the account that is associated with the group. Click the name of the owner to view the user's personal profile.

Status

Indicates whether the account is active or inactive.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Group Membership

Use this page to add or remove accounts that are associated with a group.

Account information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

User ID searches for accounts with user IDs that contain the text that is entered in the **Search information** field.

Owner searches for accounts in which the account owner's full name contains the text that is entered in the **Account information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Accounts table

Lists the accounts matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box adjacent to the account. To select all accounts, select the check box at the top of the column.

State

Indicates the state of the group.

User ID

Identifies the user ID that is associated with the group. Click the user ID to review the account information.

Owner

Identifies the full name of the user who owns the account that is associated with the group. Click the name of the owner to view the user's personal profile.

Status

Indicates whether the account is active or inactive.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add accounts to the group.

Remove

Click to remove the selected accounts from the group.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Recertification Status

Use this page to locate and recertify access to accounts that are associated with a group.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

User ID searches for access definitions with user IDs that contain the text that is entered in the **Search information** field.

Owner searches for access definitions in which the access owner's full name contains the text that is entered in the **Search information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Access table

Lists the current access definitions for the group. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an access definition. To select one or more access definitions, select the check box adjacent to the access definition. To select all access definitions, select the check box at the top of the column. Access definitions that have a status of Recertified or Admin Recertified cannot be selected.

User ID

Identifies the user ID for the access.

Owner

Identifies the name of the owner of the access. Click the name of the owner to view the user's personal profile.

Status

Indicates whether the access is active or inactive.

Recertification Status

Identifies the recertification status of the access. The possible recertification status values of the access definitions are:

- Recertified
- Admin Recertified
- Rejected and marked
- Never Recertified

Recertification Status Date

Indicates the date on which the recertification status of the access was last updated.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Recertify** to change the status of an access to Administrator Recertified.

Related information

For more information, see the [IBM Knowledge Center](#).

Account Information

Use this page to request an account for another user.

The pages that are displayed vary, depending on the type of service that you selected and by the authority that the system administrator has granted you.

The fields that are displayed on these pages also vary, depending on the type of service that you selected and by the authority that the system administrator has granted you.

The following topics define the default service attributes for the default services. For information about other service attributes, see your system administrator.

Related information

For more information, see the [IBM Knowledge Center](#).

AIX Default Attributes

For the AIX service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Access information page

UNIX Shell

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the read, write, and execute permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the access used by the account as a default change file mode value for the user home directory.

Administration choices(1) page

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as the secondary group of the user.

Groups that can use the su command on this user

Specify the name of the group that can use the UNIX **su** command on the user.

Groups to be administered

Specify the groups to administer.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before the date that a password expires that a warning is issued to the user.

Administrative roles

Specify the administrative roles for the user.

Additional mandatory methods for authenticating the user

Specify other mandatory authentication methods.

Additional optional methods for authenticating the user

Specify other optional authentication methods.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices(2) page

Audit class

Specify the list of audit classes for the user.

Allow user to execute daemon process?

Select this check box to enable the user to run daemon processes on the system.

Allow user to log in to the system?

Select this check box to enable the user to log directly into the system.

Allow user to remotely login to the system?

Select this check box to enable the user to log into the system remotely.

Can another user switch user to this user?

Select this check box to enable another user to use the UNIX **su** command on this user.

Is this user an administrator?

Select this check box to designate the user as an administrator of the system.

Trusted path status

Select the default trusted path status for the account.

always

Specifies that the user that is confined to the trusted path.

/notsh

Specifies that the user session ends if the secure attention key (SAK) signal is detected.

nosak

Specifies that the SAK key is disabled.

on

Specifies that the standard trusted path management is used.

Soft limit for largest core size

Specify the soft limit for the largest core file that the user's process can create.

Soft limit for maximum amount of CPU utilization

Specify the soft limit for the largest amount of system unit time (in seconds) that the user's process can use.

Soft limit for largest data segment

Specify the soft limit for the largest process data segment for the user's process.

Soft limit for largest file size

Specify the soft limit for the largest file that the user's process can create or extend.

Soft limit for largest stack segment

Specify the soft limit for the largest process stack segment for the user's process.

Largest core size

Specify the largest core file that the user's process can create.

Maximum CPU utilization

Specify the largest amount of system unit time (in seconds) that the user's process can use.

Largest data segment

Specify the largest process data segment for the user's process.

Largest file size

Specify the largest file that the user's process can create or extend.

Largest stack segment

Specify the largest amount of physical memory that the user's process can allocate.

Allowed login time

Specify the days and times that the user is allowed to access the system.

Allowed number of login retries before locking the account

Specify the number of failed login attempts before the account is locked.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in weeks) that the account can remain active after the password for the account has expired.

Minimum alphabetic characters in password

Specify the minimum number of alphabetic characters that must be included in the password for the account.

Minimum difference between the current and last password

Specify the minimum number of characters that are required in a new password that were not in the old password.

Maximum number of characters that can be repeated in a password

Specify the maximum number of characters in a password that can be repeated.

Minimum length of the password

Specify the minimum length of the password.

Password restriction methods

Specify password restriction methods to the account.

Password dictionaries used to restrict passwords

Specify the password dictionary files that are used to restrict which passwords can be used by the account.

Number of previous passwords that cannot be reused

Specify the number of passwords to be kept in the password history.

Account last accessed on

Specify a value for the last access date and time.

Valid terminals allowed to access the account

Specify which terminals can log in using this account.

System authentication mechanism for the user

Specify the authentication mechanism the system uses to authenticate the user.

Authentication registry where the user is administered

Specify the registry that is used for authenticating the user.

Related information

For more information, see the [IBM Knowledge Center](#).

HP-UX Default Attributes

For the HP-UX service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX Shell**

Specify a default command shell for the account.

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the names of the groups to use as secondary groups of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices page**Password warning age**

Specify the number of days before the date that a password expires that a warning is sent to the user.

Maximum number of days (weeks for AIX) the account can remain valid after the password expires

Specify the maximum time that the account can remain active after the password for the account has expired.

Number of days the account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allowed number of login retries before locking the account

Specify the number of login attempts that can occur before the account is locked.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Although you can specify a time, this feature is disabled and you can only set an account expiration date. Alternatively, select **Never** to set the account to never expire.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP Default Attributes

For the LDAP service type, IBM Security Identity Manager provides a set of default attributes.

User page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

User Container

Click **Search** to search for the location in the LDAP tree where you want to add the user.

Full name

Type a value for distinguishing users, for example, the full name of the user.

Preferred user ID

Type the user ID. This determines the default user ID that new accounts and access use when they are created.

Last name

Type the last name of the user.

First name

Type the first name of the user.

Initials

Type the initials of the user.

E-mail address

Type the e-mail address of the user.

Display name

Type the name of the user that you want to be displayed in the IBM Security Identity Manager interface.

Description

Type information about the intended purpose of the account.

Home telephone number

Type the home telephone number of the user.

Mobile telephone number

Type the mobile telephone number of the user.

Pager

Type the pager number of the user.

Business page**Title**

Type the business title of the user.

Employee number

Type the employee number of the user.

Employee type

Type the employment specification of the user, such as regular, contractor, or business partner.

Manager

Type the name of the manager of the user.

Administrative assistant

Type the name of the assistant of the user.

Business category

Type the business category type of the user.

Department number

Type the department number of the user.

Telephone number

Type the business telephone number of the user.

Fax number

Type the business fax number of the user.

Postal address

Type the business postal address of the user.

Office number

Type the office location of the user.

Location name

Type the locale of the user.

Address page**Registered address**

Type the registered address of the user.

Street

Type the street name of the registered address.

State

Type the state in which the user resides.

Destination indicator

Type an applicable destination indicator.

Physical delivery office name

Type the name of the physical address.

Home address

Type the home address of the user.

Postal code

Type the postal code of the user.

Post office box

Type the post office box number of the user.

Preferred delivery method

Type the preferred method of delivery of the user.

Other page**Driver license**

Type the driver's license number of the user.

Preferred language

Type the preferred language of the user.

Teletex terminal ID

Type the teletex terminal ID of the user.

Telex number

Type the teletex number of the user.

Related information

For more information, see the [IBM Knowledge Center](#).

Linux Default Attributes

For the Linux service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page

UNIX shell

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

This field is not supported for Linux operating systems.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices pages

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Password warning age

Specify the number of days before expiration that a password expiration warning is issued to the user.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in days) that the account can remain active after the password for the account has expired.

Related information

For more information, see the [IBM Knowledge Center](#).

Solaris Default Attributes

For the Solaris service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX Shell**

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices page**Force a password change?**

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before expiration that a password expiration warning is issued to the user.

Number of days account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allow at jobs?

Select this check box to allow this account to run an *at* job.

Allow cron jobs?

Select this check box to allow this account to run a *cron* job.

Related information

For more information, see the [IBM Knowledge Center](#).

Accounts

Use this page to find the account that you want to manage.

Account information

Type the user ID or name of the user who owns the account in this field. If you do not know the name of the account that you want to find, you can type a portion of the name to display a list of accounts. If

you do not type a value in this field or if you type an asterisk (*), and then click **Search**, the entire list of accounts is displayed as long as the number of accounts does not exceed the search limit.

Search by

Select the search category.

User ID searches for user IDs that contain the text that is entered in the **Account information** field.

Owner searches for owner names that contain the text that is entered in the **Account information** field.

Ownership type

Select an ownership type from the list to display accounts with that ownership type. The list contains default and custom ownership types. If you select an ownership type, the search is based on that ownership type.

All searches for all the accounts.

Device searches for the device accounts.

Individual searches for the individual accounts.

System searches for the system accounts.

Vendor searches for the vendor accounts.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Accounts table

Lists the accounts that match the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box next to the account. To select all accounts, select the check box at the top of the column.

State

Indicates the compliancy state of the account.

Blank (no symbol)

Indicates that the account is compliant.



Indicates that the account was returned from a reconciliation, which means it was not checked against the existing provisioning policies.



Indicates that the account can exist for the user, but that one or more of the account attributes does not comply with the existing provisioning policies.



Indicates either of the following:


The account is not supposed to exist because the user is not allowed to have access to the specified resource.

The provisioning policy is not defined for the resource.

User ID

Identifies the user ID for the account.

Click the user ID to review the account information.

Click the icon () next to the account to show the tasks that can be performed on the account.

Use these menu items to perform a task on the selected account:

Change

Changes the information for the selected account.

Delete

Deletes the selected account.

Change Password

Changes the password for the account. The account must be assigned to a user for this option to be available.

Suspend

Suspends the selected account. The account must be active for this option to be available.

Restore

Restores the selected account. The account must be inactive for this option to be available. Depending on how your system administrator configured the system, you might be prompted to enter a password.

Assign to User

Assigns the selected account to a specified user. A value of None in the **Owner** column indicates that the account is an orphan account.

Orphan

Makes the account an orphan account. The account must be already assigned to a user for this option to be available.

Add to Vault

Click to add the sponsored account to the credential vault so that the account can be shared. This function is available only if the Shared Access Module is installed. This function is disabled if the credentials exist in the vault. You cannot add individual, inactive, or orphan accounts to the credential vault.

Owner

Identifies the name of the owner of the account. Click the name of the owner to view the user personal profile. A value of None indicates that the account is an orphan account.

Ownership Type

Identifies the ownership type of the account. A value of None is displayed if no owner is assigned to the account. To assign or change the ownership type, use the **Assign to User** task. After selecting an owner, you will be prompted to select Ownership Type if the selected user is entitled for more than one ownership type.

Status

Identifies the status of the account. Accounts can be active or inactive. Contact your help desk assistant, the service owner, or your system administrator to restore an inactive account.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Request

Click to request an account.

Change

Click to change the information for the selected account.

Delete

Click to delete the selected account.

Suspend

Click to suspend the selected account.

Restore

Click to restore the selected account. Depending on how your system administrator configured the system, you might be prompted to enter a password.

Assign to User

Click to assign the selected account to a specified user.

Add to Vault

Click to add the sponsored account to the credential vault so that the account can be shared. This function is available only if the Shared Access Module is installed.

Refresh

Click to update the list of items in the table.

Related information

[For more information, see the IBM Knowledge Center.](#)

Noncompliant Account Attributes

Use this page to view an account that has one or more attributes with values that do not comply with an existing policy.

Attribute

Identifies the name of an attribute.

Non-Compliant Value

Provides the value that does not comply with an existing policy. If an attribute value is empty, the suggested value is used. If there is no suggested value, the noncompliant value is removed when you change the account.

Suggested Value

Provides the compliant value for the attribute based on the policy evaluation.

Related information

[For more information, see the IBM Knowledge Center.](#)

Change an Account

Use this notebook to change an account for another user.

The pages that are displayed in the notebook vary, depending on the type of service that you selected and by the authority that the system administrator has granted you. For example, for the AIX service, the Account information, Access information, and Administration choices pages might be displayed.

The fields that are displayed on these pages also vary, depending on the type of service that you selected and by the authority that the system administrator has granted you.

Actions**Submit Now**

Click **Submit Now** to implement your changes.

Schedule Submission

Click **Schedule Submission** to specify a date and time for the changes to take effect.

Cancel

Click **Cancel** to discard any changes you made.

Default service attributes for default services

The following topics define the default service attributes for the default services. For information about other service attributes, see your system administrator.

Related information

[For more information, see the IBM Knowledge Center.](#)

AIX Default Attributes

For the AIX service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Access information page

UNIX Shell

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the read, write, and execute permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the access used by the account as a default change file mode value for the user home directory.

Administration choices(1) page

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as the secondary group of the user.

Groups that can use the su command on this user

Specify the name of the group that can use the UNIX **su** command on the user.

Groups to be administered

Specify the groups to administer.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before the date that a password expires that a warning is issued to the user.

Administrative roles

Specify the administrative roles for the user.

Additional mandatory methods for authenticating the user

Specify other mandatory authentication methods.

Additional optional methods for authenticating the user

Specify other optional authentication methods.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices(2) page**Audit class**

Specify the list of audit classes for the user.

Allow user to execute daemon process?

Select this check box to enable the user to run daemon processes on the system.

Allow user to log in to the system?

Select this check box to enable the user to log directly into the system.

Allow user to remotely login to the system?

Select this check box to enable the user to log into the system remotely.

Can another user switch user to this user?

Select this check box to enable another user to use the UNIX **su** command on this user.

Is this user an administrator?

Select this check box to designate the user as an administrator of the system.

Trusted path status

Select the default trusted path status for the account.

always

Specifies that the user that is confined to the trusted path.

/notsh

Specifies that the user session ends if the secure attention key (SAK) signal is detected.

nosak

Specifies that the SAK key is disabled.

on

Specifies that the standard trusted path management is used.

Soft limit for largest core size

Specify the soft limit for the largest core file that the user's process can create.

Soft limit for maximum amount of CPU utilization

Specify the soft limit for the largest amount of system unit time (in seconds) that the user's process can use.

Soft limit for largest data segment

Specify the soft limit for the largest process data segment for the user's process.

Soft limit for largest file size

Specify the soft limit for the largest file that the user's process can create or extend.

Soft limit for largest stack segment

Specify the soft limit for the largest process stack segment for the user's process.

Largest core size

Specify the largest core file that the user's process can create.

Maximum CPU utilization

Specify the largest amount of system unit time (in seconds) that the user's process can use.

Largest data segment

Specify the largest process data segment for the user's process.

Largest file size

Specify the largest file that the user's process can create or extend.

Largest stack segment

Specify the largest amount of physical memory that the user's process can allocate.

Allowed login time

Specify the days and times that the user is allowed to access the system.

Allowed number of login retries before locking the account

Specify the number of failed login attempts before the account is locked.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in weeks) that the account can remain active after the password for the account has expired.

Minimum alphabetic characters in password

Specify the minimum number of alphabetic characters that must be included in the password for the account.

Minimum difference between the current and last password

Specify the minimum number of characters that are required in a new password that were not in the old password.

Maximum number of characters that can be repeated in a password

Specify the maximum number of characters in a password that can be repeated.

Minimum length of the password

Specify the minimum length of the password.

Password restriction methods

Specify password restriction methods to the account.

Password dictionaries used to restrict passwords

Specify the password dictionary files that are used to restrict which passwords can be used by the account.

Number of previous passwords that cannot be reused

Specify the number of passwords to be kept in the password history.

Account last accessed on

Specify a value for the last access date and time.

Valid terminals allowed to access the account

Specify which terminals can log in using this account.

System authentication mechanism for the user

Specify the authentication mechanism the system uses to authenticate the user.

Authentication registry where the user is administered

Specify the registry that is used for authenticating the user.

Related information

For more information, see the [IBM Knowledge Center](#).

HP-UX Default Attributes

For the HP-UX service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX Shell**

Specify a default command shell for the account.

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the names of the groups to use as secondary groups of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices page**Password warning age**

Specify the number of days before the date that a password expires that a warning is sent to the user.

Maximum number of days (weeks for AIX) the account can remain valid after the password expires

Specify the maximum time that the account can remain active after the password for the account has expired.

Number of days the account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allowed number of login retries before locking the account

Specify the number of login attempts that can occur before the account is locked.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Although you can specify a time, this feature is disabled and you can only set an account expiration date. Alternatively, select **Never** to set the account to never expire.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP Default Attributes

For the LDAP service type, IBM Security Identity Manager provides a set of default attributes.

User page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

User Container

Click **Search** to search for the location in the LDAP tree where you want to add the user.

Full name

Type a value for distinguishing users, for example, the full name of the user.

Preferred user ID

Type the user ID. This determines the default user ID that new accounts and access use when they are created.

Last name

Type the last name of the user.

First name

Type the first name of the user.

Initials

Type the initials of the user.

E-mail address

Type the e-mail address of the user.

Display name

Type the name of the user that you want to be displayed in the IBM Security Identity Manager interface.

Description

Type information about the intended purpose of the account.

Home telephone number

Type the home telephone number of the user.

Mobile telephone number

Type the mobile telephone number of the user.

Pager

Type the pager number of the user.

Business page

Title

Type the business title of the user.

Employee number

Type the employee number of the user.

Employee type

Type the employment specification of the user, such as regular, contractor, or business partner.

Manager

Type the name of the manager of the user.

Administrative assistant

Type the name of the assistant of the user.

Business category

Type the business category type of the user.

Department number

Type the department number of the user.

Telephone number

Type the business telephone number of the user.

Fax number

Type the business fax number of the user.

Postal address

Type the business postal address of the user.

Office number

Type the office location of the user.

Location name

Type the locale of the user.

Address page**Registered address**

Type the registered address of the user.

Street

Type the street name of the registered address.

State

Type the state in which the user resides.

Destination indicator

Type an applicable destination indicator.

Physical delivery office name

Type the name of the physical address.

Home address

Type the home address of the user.

Postal code

Type the postal code of the user.

Post office box

Type the post office box number of the user.

Preferred delivery method

Type the preferred method of delivery of the user.

Other page**Driver license**

Type the driver's license number of the user.

Preferred language

Type the preferred language of the user.

Teletex terminal ID

Type the teletex terminal ID of the user.

Telex number

Type the teletex number of the user.

Related information

For more information, see the [IBM Knowledge Center](#).

Linux Default Attributes

For the Linux service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page

UNIX shell

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

This field is not supported for Linux operating systems.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices pages

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Password warning age

Specify the number of days before expiration that a password expiration warning is issued to the user.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in days) that the account can remain active after the password for the account has expired.

Related information

For more information, see the [IBM Knowledge Center](#).

Solaris Default Attributes

For the Solaris service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX Shell**

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices page**Force a password change?**

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before expiration that a password expiration warning is issued to the user.

Number of days account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allow at jobs?

Select this check box to allow this account to run an *at* job.

Allow cron jobs?

Select this check box to allow this account to run a *cron* job.

Related information

For more information, see the [IBM Knowledge Center](#).

Account Recertification Status

Use this page to view the recertification status of accounts and to override the recertification state, if required. For example, accounts that have been rejected through normal recertification processes can be set to the Admin Recertified state.

Account information

Type the user ID or name of the user who owns the account in this field. If you do not know the name of the account that you want to find, you can type a portion of the name to display a list of accounts. If you do not type a value in this field or if you type an asterisk (*), and then click **Search**, the entire list of accounts is displayed as long as the number of accounts does not exceed the search limit.

Search by

Select the search category.

User ID searches for accounts with user IDs that contain the text that is entered in the **Account information** field.

Owner searches for accounts in which the account owner's full name contains the text that is entered in the **Account information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Accounts table

Lists the accounts matching the specified search criteria. This table also displays related information and recertification status of accounts. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box adjacent to the account. To select all accounts, select the check box at the top of the column. Accounts that have a status of Recertified or Admin Recertified cannot be selected.

User ID

Identifies the user ID for the account. Click the user ID to view the account information for the user ID.

Owner

Identifies the name of the owner of the account. Click the name of the owner to view the personal, business, and contact information for the user.

Status

Indicates whether the account is active or inactive.

Recertification Status

Identifies the recertification status of the account. The possible recertification status values of the accounts are:

- Recertified
- Admin Recertified
- Rejected and suspended
- Rejected and marked
- Never Recertified

Recertification Status Date

Indicates the date on which the recertification status of the account was last updated.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Recertify

Click to change the status of an account to Admin Recertified.

Refresh

Click to update the list of items in the table.

Related information

[For more information, see the IBM Knowledge Center.](#)

Confirm

Use this page to confirm recertification of the selected accounts.

Specify a justification for performing the administrative recertification of the accounts in the **Justification** field. This information is stored in a log that can be reported on at a later date.

Click **Recertify** to perform the recertification action on the accounts.

Related information

[For more information, see the IBM Knowledge Center.](#)

Manage Account Defaults

Select an Account Attribute

Use this page to add, change, or remove the default account attributes for a service instance.

When you define account defaults for a service, any defaults that are defined for that service's type are pre-populated into the table. After the account defaults are saved for the service, they override the account defaults that are defined for the service's type.

Use the global account defaults for the service type

Select this check box to use the global account defaults for the service type instead of adding an attribute default to the service type.

Account Attributes table

Lists the attributes that are associated with the account for the given service instance. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account attribute. To select one or more account attributes, select the check box adjacent to the account attribute. To select all account attributes, select the check box at the top of the column.

Account Attribute

Identifies the name of the attributes associated with the service.

Template Value

Indicates the default value of the account attribute.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add an attribute default to the service type.

Change (Basic)

Click to change the selected attribute.

Change (Advanced)

Click to change the selected attribute using JavaScript to define the account default.

Remove

Click to remove the selected attribute.

Related information

For more information, see the [IBM Knowledge Center](#).

Select an Attribute to Default

Use this page to specify default values for attributes that are associated with an account.

Attributes table

Lists the attributes that are associated with the account for the given service instance. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates the account attribute to which the **Add** and **Add (Advanced)** buttons apply.

Attribute name

Identifies the name of the attribute.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a default value for the selected attribute.

Add (Advanced)

Click to add a script that specifies a default value for the selected attribute.

Related information

For more information, see the [IBM Knowledge Center](#).

Set Default for Attribute Name

Use this page to specify or change the default value of an attribute. The default value applies to accounts associated with the specified service instance.

The fields that are displayed on this page vary, depending on the type of the attribute as specified in the Form Designer.

This page might not display the existing default value for the attribute if the default is an advanced value. Click **OK** to replace the existing value with the value on this page.

Attributes are validated against constraints in the Form Designer. However, an attribute that is a text area or text field, such as a description or comment attribute, is not validated. For example, in AIX, the Gecos (comments) attribute is not validated.

Related information

For more information, see the [IBM Knowledge Center](#).

AIX Default Attributes

For the AIX service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Access information page

UNIX Shell

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the read, write, and execute permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the access used by the account as a default change file mode value for the user home directory.

Administration choices(1) page

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as the secondary group of the user.

Groups that can use the su command on this user

Specify the name of the group that can use the UNIX **su** command on the user.

Groups to be administered

Specify the groups to administer.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before the date that a password expires that a warning is issued to the user.

Administrative roles

Specify the administrative roles for the user.

Additional mandatory methods for authenticating the user

Specify other mandatory authentication methods.

Additional optional methods for authenticating the user

Specify other optional authentication methods.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices(2) page**Audit class**

Specify the list of audit classes for the user.

Allow user to execute daemon process?

Select this check box to enable the user to run daemon processes on the system.

Allow user to log in to the system?

Select this check box to enable the user to log directly into the system.

Allow user to remotely login to the system?

Select this check box to enable the user to log into the system remotely.

Can another user switch user to this user?

Select this check box to enable another user to use the UNIX **su** command on this user.

Is this user an administrator?

Select this check box to designate the user as an administrator of the system.

Trusted path status

Select the default trusted path status for the account.

always

Specifies that the user that is confined to the trusted path.

/notsh

Specifies that the user session ends if the secure attention key (SAK) signal is detected.

nosak

Specifies that the SAK key is disabled.

on

Specifies that the standard trusted path management is used.

Soft limit for largest core size

Specify the soft limit for the largest core file that the user's process can create.

Soft limit for maximum amount of CPU utilization

Specify the soft limit for the largest amount of system unit time (in seconds) that the user's process can use.

Soft limit for largest data segment

Specify the soft limit for the largest process data segment for the user's process.

Soft limit for largest file size

Specify the soft limit for the largest file that the user's process can create or extend.

Soft limit for largest stack segment

Specify the soft limit for the largest process stack segment for the user's process.

Largest core size

Specify the largest core file that the user's process can create.

Maximum CPU utilization

Specify the largest amount of system unit time (in seconds) that the user's process can use.

Largest data segment

Specify the largest process data segment for the user's process.

Largest file size

Specify the largest file that the user's process can create or extend.

Largest stack segment

Specify the largest amount of physical memory that the user's process can allocate.

Allowed login time

Specify the days and times that the user is allowed to access the system.

Allowed number of login retries before locking the account

Specify the number of failed login attempts before the account is locked.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in weeks) that the account can remain active after the password for the account has expired.

Minimum alphabetic characters in password

Specify the minimum number of alphabetic characters that must be included in the password for the account.

Minimum difference between the current and last password

Specify the minimum number of characters that are required in a new password that were not in the old password.

Maximum number of characters that can be repeated in a password

Specify the maximum number of characters in a password that can be repeated.

Minimum length of the password

Specify the minimum length of the password.

Password restriction methods

Specify password restriction methods to the account.

Password dictionaries used to restrict passwords

Specify the password dictionary files that are used to restrict which passwords can be used by the account.

Number of previous passwords that cannot be reused

Specify the number of passwords to be kept in the password history.

Account last accessed on

Specify a value for the last access date and time.

Valid terminals allowed to access the account

Specify which terminals can log in using this account.

System authentication mechanism for the user

Specify the authentication mechanism the system uses to authenticate the user.

Authentication registry where the user is administered

Specify the registry that is used for authenticating the user.

Related information

For more information, see the [IBM Knowledge Center](#).

HP-UX Default Attributes

For the HP-UX service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page

UNIX Shell

Specify a default command shell for the account.

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the names of the groups to use as secondary groups of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices page

Password warning age

Specify the number of days before the date that a password expires that a warning is sent to the user.

Maximum number of days (weeks for AIX) the account can remain valid after the password expires

Specify the maximum time that the account can remain active after the password for the account has expired.

Number of days the account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allowed number of login retries before locking the account

Specify the number of login attempts that can occur before the account is locked.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Although you can specify a time, this feature is disabled and you can only set an account expiration date. Alternatively, select **Never** to set the account to never expire.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP Default Attributes

For the LDAP service type, IBM Security Identity Manager provides a set of default attributes.

User page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

User Container

Click **Search** to search for the location in the LDAP tree where you want to add the user.

Full name

Type a value for distinguishing users, for example, the full name of the user.

Preferred user ID

Type the user ID. This determines the default user ID that new accounts and access use when they are created.

Last name

Type the last name of the user.

First name

Type the first name of the user.

Initials

Type the initials of the user.

E-mail address

Type the e-mail address of the user.

Display name

Type the name of the user that you want to be displayed in the IBM Security Identity Manager interface.

Description

Type information about the intended purpose of the account.

Home telephone number

Type the home telephone number of the user.

Mobile telephone number

Type the mobile telephone number of the user.

Pager

Type the pager number of the user.

Business page**Title**

Type the business title of the user.

Employee number

Type the employee number of the user.

Employee type

Type the employment specification of the user, such as regular, contractor, or business partner.

Manager

Type the name of the manager of the user.

Administrative assistant

Type the name of the assistant of the user.

Business category

Type the business category type of the user.

Department number

Type the department number of the user.

Telephone number

Type the business telephone number of the user.

Fax number

Type the business fax number of the user.

Postal address

Type the business postal address of the user.

Office number

Type the office location of the user.

Location name

Type the locale of the user.

Address page**Registered address**

Type the registered address of the user.

Street

Type the street name of the registered address.

State

Type the state in which the user resides.

Destination indicator

Type an applicable destination indicator.

Physical delivery office name

Type the name of the physical address.

Home address

Type the home address of the user.

Postal code

Type the postal code of the user.

Post office box

Type the post office box number of the user.

Preferred delivery method

Type the preferred method of delivery of the user.

Other page**Driver license**

Type the driver's license number of the user.

Preferred language

Type the preferred language of the user.

Teletex terminal ID

Type the teletex terminal ID of the user.

Telex number

Type the teletex number of the user.

Related information

For more information, see the [IBM Knowledge Center](#).

Linux Default Attributes

For the Linux service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page

UNIX shell

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

This field is not supported for Linux operating systems.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices pages

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Password warning age

Specify the number of days before expiration that a password expiration warning is issued to the user.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in days) that the account can remain active after the password for the account has expired.

Related information

For more information, see the [IBM Knowledge Center](#).

Solaris Default Attributes

For the Solaris service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX Shell**

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices page**Force a password change?**

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before expiration that a password expiration warning is issued to the user.

Number of days account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allow at jobs?

Select this check box to allow this account to run an *at* job.

Allow cron jobs?

Select this check box to allow this account to run a *cron* job.

Related information

For more information, see the [IBM Knowledge Center](#).

Set Default for Attribute Name

Use this page to specify a script that defines the account default.

Script

Type the JavaScript code used to define the account default.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a User Attribute

Use this page to select attributes for the account.

User Type

Select a user type from the list. Available user types are Person and Business Partner Person.

Attributes table

Lists the attributes that are associated with the account. The list of attributes varies, depending on the type of user that you select.

Select

Indicates the user attribute that is selected.

Attribute

Identifies the name of the attribute.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select an Ownership Type

Use this page to select an ownership type or account category for the account you want to request.

Ownership Type table

Lists the ownership types. The table contains these columns:

Select

Select to specify an ownership type.

Ownership Type

Identifies the ownership type for an account, such as:

Device
Individual
Individual/Category1
System
Vendor

Note: The provisioning policy entitlements control the ownership types that are available for the account.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Orphan Accounts

Manage Orphan Accounts

Use this page to find the orphan accounts that you want to manage. Orphan accounts are included in the list of accounts that are associated with a service. You can suspend or delete orphan accounts or assign them to users.

Account information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

User ID searches for user IDs across all service types or descriptions that contain the text that is entered in the **Search information** field.

Service Name searches for services in which the service name contains the text that is entered in the **Search information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to use additional filter criteria when searching for user IDs or service names.

Accounts table

Lists the accounts that match the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box next to the account. To select all accounts, select the check box at the top of the column.

User ID

Identifies the user ID.

Service Name

Identifies the name of the service.

Service Type

Identifies the type of service.

Status

Indicates the status of the account.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Delete

Click to delete the selected account from the system. When you delete an orphan account, it is deleted on the managed resource.

Suspend

Click to suspend the selected account. When you suspend an orphan account, it is suspended on the Security Identity Manager Server and on the managed resource.

Assign to User

Click to assign the selected account to a user. When you assign an orphan account to a user, the user becomes the owner of the account. Also, the policies that are applicable to the users are evaluated and enforced for the account. The owner can manage the account with the Self Service or the Identity Service Center application.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Groups

Select a Service

Use this page to find the service with the groups that you want to manage.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Service searches for service names or descriptions that contain the text that is entered in the **Search information** field.

Business unit searches for business units in which the business unit name contains the text that is entered in the **Search information** field.

Service type

Select a service type from the list. The list contains the service types that have groups enabled that are installed by the administrator. Select **All** from the list to display all of the services that have groups enabled that are managed by IBM Security Identity Manager.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Services table

Lists the services matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select a service, click the radio button adjacent to the service.

Service Name

Identifies the name of the service.

Description

Provides information about the intended purpose of the service.

Service Type

Identifies the type of service.

Note: Accesses that are defined on the original service are not available for the hosted service, and those accesses cannot be requested by users in different organizations.

Business Unit

Identifies the business unit in which the service is created.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related concepts**Advanced Search**

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Group

Use the **Select Group** page to search for a group.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Group name or description

Searches for groups with a name or description that contains text that is entered in the **Search information** field.

Business unit

Searches for business units in which the business unit name contains the text that is entered in the **Search information** field.

Groups table

Lists the groups matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box next to the group. To select all groups, select the check box at the top of the column.

Group Name

Identifies the name of the group.

You can use these menu items:

Manage Members

Click to see which users are members in the selected group. You can also add or remove members from the selected group.

Add Members

Click to add members to the selected group.

Description

Displays information about the intended purpose of the group.

View

Identifies the view of tasks that users have in this group.

Business Unit

Identifies the business unit in which the group is specified.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new group.

Change

Click to change the description or membership for the selected group.

Delete

Click to remove the selected group from the system.

Export Access Data

Click to open the **Export Access Data** page, and export the group access data. The **Export Access Data** button is not active until you select some accesses to activate it. Only the group access that you selected are exported.

Import Access Data

Click to open the **Import Access Data** page to import the access data for a group access. You can also import access data for a set of groups.

Refresh

Click to refresh the list of items in the table.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Export access data

Use the **Export Access Data** page to export the group access data. The access data is specified in a comma-separated value (CSV) file. IBM Security Identity Manager uses the settings that are indicated in the CSV file.

The **Export Access Data** page is displayed after you click **Export Access Data** in the **Select Group** page.

After you submit the export request, a process status indicates the progress of the export operation.

Download Exported Data

Click to download the exported data for the group access. Download the file on your local system by using your web browser settings.

The exported data contains information such as Group DN, Group name, Define as Access, Access name, Access type, Access description, Icon URL, Search terms, Additional information, and Badges.

Download Export Log File

Click to view any error or log information about the export operation. This button is displayed only if the submitted export operation contains any log information or encountered any errors.

Cancel

Click to cancel the export operation. The operation is discontinued if you cancel it during an active export session.

Close

Click to close the **Export Access Data** page. The operation fails if you close the **Export Access Data** page during an active export session.

Import access data

Use the **Import Access Data** page to import the group access data. The access data is specified in the comma-separated value (CSV) file. IBM Security Identity Manager uses the settings that are indicated in the CSV file.

File to Upload (.CSV)

Displays the name of the CSV file that contains all the group access data. This field is required.

Browse

Click to locate and upload the CSV file for import. You can also type the complete and correct path to the file on your workstation along with the file name.

Import

Click to immediately import the CSV file.

After you submit the import request, a process status indicates the progress of the import operation.

Note: If you click **Import** with an invalid file format, a message is displayed to inform you that the file format is not valid.

Cancel

Click to cancel the import operation. The operation is discontinued if you cancel it during an active import session.

Download Import Log File

Click to view any error or log information about the import operation. This button is displayed only if the submitted import operation contains any log information or encountered any errors.

Close

Click to close the **Import Access Data** page. The operation fails if you close the **Import Access Data** page during an active import session.

Change Group

Use this page to change a group description or to change the view of tasks for the group. You cannot change the name of the group.

Group name

Displays the name of the group.

View

Identifies the view of tasks that users have in this group.

Description

Displays information about the intended purpose of the group.

Business unit

Identifies the business unit in which the group is specified.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

[For more information, see the IBM Knowledge Center.](#)

Business Unit Details

Use this page to view business unit details for an organization. The business unit fields available on this page vary according to the business unit type. All text fields are read-only.

Context within the organization

Provides a root structure below a Root Organization showing the organization structure, including organizations, organizational units, business partner organizational units, locations, and admin domains.

Related information

For more information, see the [IBM Knowledge Center](#).

Enable Access

You can control access by granting access to selected groups.

Use group description for the access description

Lets you use the same group description for the access description.

Note: If selected, the group description overrides the existing access description.

Enable as Common Access

Enables the group as common access.

Select an access type that you want to grant to all the specified groups

Specifies the access type that you want to grant for the selected groups.

Access Type

Select an access type for a group. The default access type for a group is **Application**. If **Application** is removed as an access type, the first access type is the default option.

Groups table

Lists the available groups that you can select and the associated access details. The table contains the following columns:

Group Name

Specifies the name of the group.

Description

Specifies the associated description for the group.

Access Type

Specifies the assigned access type for the group. For example: Application

You can use the following buttons:

Enable

Click to enable access for the displayed groups.

Cancel

Click to cancel any changes.

Create Group

Create a Group

Use the **Create a Group** wizard to create additional groups and add members to the groups.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

General Information

Use this page to specify information about a group.

Group Name

Type a unique, user-friendly name for the new group. It is important to specify meaningful group names because, in some cases, users might have only this information to guide a group membership decision for an account.

View

Select the view of tasks.

Description

Type information about the group's intended purpose. It is important to specify meaningful descriptions because, in some cases, users might only have this information to guide a group membership decision for an account.

Business Unit

Specify the business unit. To locate available business units, click **Search**.

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Group Membership

Use this page to specify which users are members of a group.

Group Membership table

Lists the users that you can select as members of the group. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

User Name

Identifies the full name of the user. Click the name to see the user's information profile.

User ID

Identifies the user ID for the user. This field is available after you add a user to the group.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a member to the group.

Remove

Click to remove a selected member.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule Add Member Operation

Use this page to submit a request. This page is available after you add one or more members to a group.

Immediate

Runs the request immediately after you click the button to complete the task.

Effective date

Runs the request at a day and hour that you specify. After you select this option, click the calendar icon to specify the scheduled day, and click the clock icon to specify the scheduled hour.

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Policies

Adoption Policies

Work with Adoption Policies

Use this page to create, change, or delete adoption policies.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Adoption policy searches for adoption policy names that contain the text that is entered in the **Search information** field.

Service searches for adoption policies that specify service targets that have a service name that contains the text that is entered in the **Search information** field.

Adoption Policies table

Lists the set of adoption policies matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an adoption policy. To select one or more adoption policies, select the check box adjacent to the adoption policy. To select all adoption policies, select the check box at the top of the column.

Adoption Policy Name

Identifies the name of the adoption policy. Click the name to view or change the adoption policy.

Adoption Policy Description

Identifies a brief description of the adoption policy.

Service

Identifies the name of the service.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new adoption policy.

Change

Click to change a selected adoption policy.

Delete

Click to delete one or more selected adoption policies.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Adoption Policies

Use this notebook to specify information about an adoption policy.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to specify general information about an adoption policy.

Name

Specify the name of the adoption policy.

Description

Provide a description of the intended purpose of the adoption policy.

After you have specified the required information for the policy, click **Apply** to save your changes and continue.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Services

Use this page to add or remove services to which the adoption policy applies.

You must specify at least one service for the adoption policy. You cannot associate more than one adoption policy with a service.

Services table

Lists the services matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box adjacent to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view the service details.

Description

Identifies a brief description of the service.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a service.

Remove

Click to remove one or more selected services.

Apply

Click to save your changes and continue after you have specified the required information for the policy.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Rule

Use this page to specify the attributes that the adoption policy uses to match accounts to users.

Specify rule by

Specify how you want to specify the adoption policy:

Defining matches

Select one or more account attributes to match to a user attribute.

Account attribute matches

Select an account attribute from the list. During reconciliation, the value of the account attribute is compared to the value of the user attribute.

User attribute

Select a user attribute from the list. During reconciliation, the value of this user attribute is compared to the value of an attribute of an account on a managed resource.

Click **Remove** to remove a matching pair of attributes.

Click **Add a match field** to specify matching criteria for a rule.

Providing a script

Type a script to define a custom adoption policy that compares the account attribute values to the user attribute values. If the values match, the account is assigned to the matching user during reconciliation.

If you select this option and then switch back to **Defining Matches**, a warning is displayed, notifying you that switching the input mode loses any modifications made to the script. Verify that you want to continue.

Click **Apply** to save your changes and continue.

Related information

For more information, see the [IBM Knowledge Center](#).

Services

Use this page to find the service that you want to associate with the adoption policy.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Service searches for service names that contains the text that is entered in the **Search information** field.

Business unit searches for services defined in business units that have a business unit name that contains the text that is entered in the **Search information** field.

Service type

Select a service type from the list.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Services table

Lists the services matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box adjacent to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view the service details.

Description

Identifies a brief description of the service.

Service Type

Identifies the type of service.

Business Unit

Identifies the business unit to which the service applies.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Service Details

Use this page to view the details that are related to the selected service. Each service has its own unique set of information. Refer to the documentation provided with the adapter for details about the displayed fields.

The following fields are common for most services. All fields are read-only, so you cannot change any information related to the service. These fields might or might not be displayed on the service form by default. Except for the **Service name** field, these fields can be added or removed.

Service name

Displays the name of the service.

Description

Displays the description of the service that was provided by the service owner.

URL

For remote services, displays the URL used to connect to the resource hosting the service. The *address* value is displayed in brackets for IPv6 addresses.

User ID

Displays the user ID used to log into the remote resource.

Owner

Displays the name of the service provider.

Service prerequisite

Displays the prerequisite that must be met before the service can be used, for example, at least one service account must exist.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX AIX Profile: General Information

Use this page to specify information about the AIX service instance.

The AIX service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the AIX service instance runs.

Description

Specify additional information about the AIX service instance.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `imi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and

port is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the AIX resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

User registry

Specify how to manage and authenticate users.

- Leave Blank if the users on the service are to be managed only through the `/etc/password` file.
- Type `files` if this is a mixed setup and the users are to be managed through the `/etc/password` file.
- Type LDAP if this is a mixed setup and the users are to be managed through LDAP.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the AIX server when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the AIX service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user be used in administering the service instance

Service prerequisite

Specify an existing service instance or function that the AIX service instance requires.

If a service has another service defined as a service prerequisite, a user can only receive a new account if they have an existing account on the service prerequisite.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX HP-UX Profile: General Information

Use this page to specify information about the HP-UX service instance.

The HP-UX service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the HP-UX service instance runs.

Description

Specify additional information about the HP-UX service instance.

Connection mode

This option is available only if the `erconnectionmode` attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the HP-UX resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

Use a shadow file?

Select this check box to use an access-restricted ASCII system file that stores users' encrypted passwords and related information. This field is unique to the UNIX service types.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the HP-UX server when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the HP-UX service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify to use any user in administering the service instance.

Service prerequisite

Click **Search** to specify an existing service instance or function that the HP-UX service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP Profile: Service Information

Use this page to specify information about the Lightweight Directory Access Protocol (LDAP) service instance.

The LDAP service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

LDAP service**Service name**

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the LDAP service instance runs.

Description

Specify additional information about the LDAP service instance.

Connection mode

This option is available only if the `erconnectionmode` attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`. Where *ip-address* is the Security Directory Integrator host and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Directory server location

Specify the location and port number of the LDAP Adapter. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `ldap://[address]:port number`.

Use SSL communication with LDAP?

Select this check box to use secure communication with the LDAP service instance.

Administrator name

Specify the administrative user ID, such as `cn=root`, for the LDAP service instance. The name must be a distinguished name (DN).

Password

Specify the administrative password for the LDAP service instance. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Directory server name

Choose a directory server from the list.

Owner

Click **Search** to specify the existing user ID of the service owner that administers the LDAP service instance.

Click **Clear** to remove the currently specified user.

Service prerequisite

Click **Search** to specify an existing service instance or function that the LDAP service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user can only receive a new account if they have an existing account on the service prerequisite.

Users and groups**User base DN**

Specify the distinguished name (DN) of the container or base point where the users are stored.

RDN attribute

Specify the required relative distinguished name (RDN) attribute for the LDAP service instance.

Group base DN

Specify the DN of the container or base point where the groups are stored.

Initial group member

Specifies a DN used to create the LDAP group. It is prefilled with `cn=TIM Adapter`. Optionally, you can customize this initial group member.

Group object class name

Select the group object class for example `GroupOfNames`.

Group membership attribute

Select the group membership attribute for example `member`.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Linux Profile: General Information

Use this page to specify information about the Linux service instance.

The Linux service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service is:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the Linux service instance runs.

Description

Specify additional information about the Linux service instance.

Connection mode

This option is available only if the *erconnectionmode* attribute is added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:1099/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the Linux resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

RXA Internet Command TimeOut

The RXA library is used for the internal communication between the adapter and the managed resource. By default, when RXA issues a command, it expects a response within 5000 milliseconds. This property is only used when the managed resource takes more than default time to respond and the RXA call fails with timeout error.

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the Linux server when the account is deleted.

Ensure that you also set the home directory permissions, which by default are none. If no permissions are set, the home directory is not deleted when the account is deleted.

Use a shadow file?

Select this check box if you want to use an access-restricted ASCII system file that stores users' encrypted passwords and related information. This field is unique to the UNIX service types.

Return sudo privileges?

If checked, the adapter returns the sudo privileges granted to users and groups during reconciliation.

Path to the sudoers file

If it is not the default location `/etc/sudoers` on the resource, enter the directory path to the sudoers file.

Owner

Specify the existing user ID of the service owner that administers the Linux service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify to use any user in administering the service instance

Service prerequisite

Specify an existing service instance or function that the Linux service instance requires.

Click **Search** to specify an existing service instance or function that the Linux service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

POSIX Solaris Profile: General Information

Use this page to specify information about the Solaris service instance.

The Solaris service instance uses an agentless adapter based on IBM Security Directory Integrator assembly lines. Complete the following fields to connect to the server where the service resides:

Service name

Specify a name that helps you identify the service instance. For example, you might include the host name of the computer on which the Solaris service instance runs.

Description

Specify additional information about the Solaris service instance.

Connection mode

This option is available only if the `erconnectionmode` attribute has been added to the service form. Specify whether to have the managed resource process account requests or to have the service act as a manual service.

Automated

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user. Selecting Manual enables the Participants page, the Messages page, and a different Reconciliation page in the navigation area.

Tivoli Directory Integrator location

Optional: Specify the URL for the Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Security Directory Integrator host, and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as `rmi://localhost:16231/ITDIDispatcher`. Specify the value of *localhost* in the `etc/hosts` file.

Managed resource location

Specify the host name or IP address for the Solaris resource. For IPv6 addresses, enter the *address* value in brackets. An example of a URL using IPv6 would be `http://[address]:port number`

Delete home directory when the account is deleted?

Select this check box to delete the home directory of the user on the Solaris server when the account is deleted.

Ensure that you also set the home directory permissions, which by default are none. If no permissions are set, the home directory is not deleted when the account is deleted.

Owner

Specify the existing user ID of the service owner that administers the Solaris service instance.

Click **Search** to specify the name of the user who owns the service.

If a name exists in this field, click **Clear** to specify that any user be used in administering the service instance

Service prerequisite

Specify an existing service instance or function that the Solaris service instance requires.

Click **Search** to specify an existing service instance or function that the Linux service instance requires.

Click **Clear** to remove the currently specified service.

If a service has another service defined as a service prerequisite, a user must have an existing account on the service prerequisite. Otherwise the user cannot receive a new account.

Click **Test Connection** to test the connection to the service.

Related information

For more information, see the [IBM Knowledge Center](#).

CSV Identity Feed: Service Information

Use this page to specify information about the comma-separated value (CSV) identity feed.

The comma-separated value (CSV) file cannot contain binary attributes. If you include multivalued attributes, they must be represented by using multiple columns with the same attribute name. You must list all required attributes in the CSV file before you list optional attributes.

If you select a service profile for activities that use a CSV format to import identity data, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

File name

Specify the file name, including the path name, of the CSV file.

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Name attribute

Select an attribute, such as uid, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

DSML Identity Feed: Service Information

Use this page to specify information about the Directory Services Markup Language (DSML) identity feed.

If you select a service profile to import identity data using DSML, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

User ID

Specify the administrative user ID for the service instance.

Password

Specify the administrative password for the service instance. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

File name

Specify the file name, including the path name, that contains the user information.

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

IDI Data Feed: Service Information

Use this page to specify information about the Initial Domain Identifier (IDI) identity feed.

If you select a service profile for activities that use IBM Security Directory Integrator to import identity data, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the name of the principal to authenticate clients using the Java Naming and Directory Interface (JNDI) application programming interface.

Password

Specify the password to authenticate clients using the JNDI application programming interface. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Name attribute

Select an attribute, such as uid, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

INetOrgPerson Identity Feed: Service Information

Use this page to specify information about the INetOrgPerson identity feed.

If you select a service profile to import identity data using LDAP, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the distinguished name (DN) of the administrator who is authorized to access the LDAP server that provides the identity information. For example, the user ID on LDAP is `cn=Administrator,cn=users,dc=itimcv,dc=com`, where *itimcv* is the domain name.

Password

Specify the password for the administrator who is authorized to access the LDAP server that provides the identity feed. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Attribute mapping file name

Specify the absolute path and file name of the file that contains attribute mapping between the identity feed source schema and specified user type schema. The mapping file contains key value pairs that identify the source and target attribute mapping.

Name attribute

Select an attribute, such as uid, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

AD OrganizationalPerson Identity Feed: Service Information

Use this page to specify information about the Active Directory OrganizationalPerson identity feed.

If you select a service profile to import identity data using Active Directory, complete these fields to connect to the server where the service resides:

Service name

Specify a name for the service instance.

Description

Specify additional information about the service instance.

URL

Specify the address as `ldap://address:portnumber` of the LDAP server that provides the identity information. The value of *address* is either the IP address or the host name of the LDAP server. The default value of *portnumber* is 389.

User ID

Specify the distinguished name (DN) of the administrator who is authorized to access the LDAP server that provides the identity information. For example, the user ID on LDAP is `cn=Administrator,cn=users,dc=itimcv,dc=com`, where *itimcv* is the domain name.

Password

Specify the password for the administrator who is authorized to access the LDAP server that provides the identity feed. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

Naming context

Specify the distinguished name (DN) of the container that holds the identity records. The identity feed uses this value to communicate the information, using the Java Naming and Directory Interface (JNDI).

Use workflow

Select this check box to use workflow for the user operation.

Evaluate separation of duty policy when workflow is used

Select this check box to evaluate the separation of duty policy. This option is applicable only when the **Use workflow** check box is selected.

Person profile name

Select a person profile name from the list.

Attribute mapping file name

Specify the absolute path and file name of the file that contains attribute mapping between the identity feed source schema and specified user type schema. The mapping file contains key value pairs that identify the source and target attribute mapping.

Name attribute

Select an attribute, such as uid, that uniquely identifies the object. This value is used to either match the identity record to an existing user ID or to create a user ID based on the value of the attribute.

Placement rule

Type JavaScript for the placement rule. The placement rule returns the distinguished name (DN) of the organization container in which the user is placed.

Use these buttons:

Test Connection

Click to test the connection to the service.

Finish

Click when you are finished with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Separation of Duty Policies

Manage Separation of Duty Policies

Use this page to create, change, delete, or evaluate separation of duty policies. The evaluation process searches for violations to the policies that you specify. You should perform an evaluation after changing a policy or role hierarchy, or after running an identity feed with evaluations disabled.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Name or description searches for separation of duty policy names or descriptions that contain the text that is entered in the **Search information** field.

Business unit searches for separation of duty policies defined in business units that have a business unit name or description that contains the text that is entered in the **Search information** field.

Role searches for separation of duty policies which contain a role whose name or description matches the text that is entered in the **Search information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Separation of Duty Policies table

Lists the policies matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a separation of duty policy. To select one or more separation of duty policies, select the check box adjacent to the separation of duty policy. To select all separation of duty policies, select the check box at the top of the column.

Policy Name

Identifies the name of the separation of duty policy. Click the name to view or change the separation of duty policy.

Description

Identifies a brief description of the separation of duty policy.

Business Unit

Identifies the business unit that is associated with the separation of duty policy. Click the name to view the business unit details.

State

Identifies the state of the policy as enabled or disabled.

Violations

Identifies the number of violations for the separation of duty policy. If there are any violations, click the number to view or make changes to policy violations and exemptions.

Exemptions

Identifies the number of exemptions for any separation of duty policy violations. If there are any exemptions, click the number to view or make changes to policy violations and exemptions.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new separation of duty policy.

Change

Click to change the selected separation of duty policy.

Delete

Click to delete one or more selected separation of duty policies.

Evaluate

Click to evaluate one or more selected separation of duty policies.

Refresh

Click to perform the search again and refresh the list of separation of duty policies.

Related information

For more information, see [the IBM Knowledge Center](#).

Create Separation of Duty Policy

Use this page to create a separation of duty policy.

Policy name

Provide the name of the separation of duty policy.

Description

Provide additional information about the policy. For example, the description can state the policy name, who created the policy, the date the policy was created, and a reason why the policy exists.

Business unit

Select the business unit. To locate an available business unit, click **Search**. Setting the business unit allows you to customize which user can administer the policy.

Policy Rules table

Lists the policy rules. The table contains these columns:

Select

Specifies a policy rule. To select one or more policy rules, select the check box next to the policy rule. To select all policy rules, select the check box at the top of the column.

Description of Separation

Type a description for the policy rule. For example, you might describe a rule that you add to a policy as `People in the IT department cannot be given accounting responsibilities`.

Allowed Number of Roles

Identifies how many roles to which a user can belong.

Roles

Identifies the roles that are associated with the policy rule.

You can use these buttons with the **Policy Rules** table:

Create


Click to create a policy rule.

Change

Click to change the selected policy rule.

Delete

Click to delete one or more selected policy rules.

To provide a list of roles and users that have ownership of the policy, click the  icon adjacent to **Policy Owners**.

Role Policy Owners table

Add one or more organizational roles as owners for the separation of duty policy. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Role Name

Identifies the name of the role.

Role Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

User Policy Owners table

Add one or more users as owners for the separation of duty policy. The table displayed is dependent on the policy owner type specified. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

Full Name

Identifies a value for distinguishing a user, such as the user's full name. Click the name of the user to view the user's personal profile..

E-mail Address

Identifies the user's e-mail address.

Last Name

Identifies the user's last name.

Business Unit

Identifies the business unit associated with the user.

You can use these buttons with the **Role Policy Owners** table or the **User Policy Owners** table:

Add

Click to add a role or user to the list. A search panel will open from which you can select the appropriate roles or users.

Remove

Click to remove one or more roles or users from the list.

Policy state

Select the status of the policy. Click **Enabled** to use the policy and make it active. Click **Disabled** to make the policy inactive. The policy state is enabled by default.

Click **Submit** to save the policy and continue after you have specified the required information for the policy.

Related information

For more information, see the [IBM Knowledge Center](#).

Change Separation of Duty Policy

Use this page to change a separation of duty policy.

Policy name

Provide the name of the separation of duty policy.

Description

Provide additional information about the policy. For example, the description can state the policy name, who created the policy, the date the policy was created, and a reason why the policy exists.

Business unit

Select the business unit. To locate an available business unit, click **Search**. Setting the business unit allows you to customize which user can administer the policy.

Policy Rules table

Lists the policy rules. The table contains these columns:

Select

Specifies a policy rule. To select one or more policy rules, select the check box next to the policy rule. To select all policy rules, select the check box at the top of the column.

Description of Separation

Type a description for the policy rule. For example, you might describe a rule that you add to a policy as *People in the IT department cannot be given accounting responsibilities*.

Allowed Number of Roles

Identifies how many roles to which a user can belong.

Roles

Identifies the roles that are associated with the policy rule.

You can use these buttons with the **Policy Rules** table:

Create


Click to create a policy rule.

Change

Click to change the selected policy rule.

Delete

Click to delete one or more selected policy rules.

To modify the list of roles and users that have ownership of the policy, click the  icon adjacent to **Policy Owners**.

Role Policy Owners table

Add or remove one or more organizational roles as owners for the separation of duty policy. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Role Name

Identifies the name of the role.

Role Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

User Policy Owners table

Add one or more users as owners for the separation of duty policy. The table displayed is dependent on the policy owner type specified. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

Full Name

Identifies a value for distinguishing a user, such as the user's full name. Click the name of the user to view the user's personal profile..

E-mail Address

Identifies the user's e-mail address.

Last Name

Identifies the user's last name.

Business Unit

Identifies the business unit associated with the user.

You can use these buttons with the **Role Policy Owners** table or the **User Policy Owners** table:

Add

Click to add a role or user to the list. A search panel will open from which you can select the appropriate roles or users.

Remove

Click to remove one or more roles or users from the list.

Policy state

Select the status of the policy. Click **Enabled** to use the policy and make it active. Click **Disabled** to make the policy inactive.

Click **Submit** to save the policy and continue after you have specified the required information for the policy.

Related information

For more information, see the [IBM Knowledge Center](#).

Separation of Duty Policy Details

Use this page to view information about a separation of duty policy.

Policy name

Indicates the name of the separation of duty policy.

Description

Indicates additional information about the policy. For example, the description can state the policy name, who created the policy, the date the policy was created, and a reason why the policy exists.

Business unit

Indicates the business unit to which the policy applies.

Policy Rules table

Lists the policy rules. The table contains these columns:

Description of Separation


Type a description for the policy rule. For example, you might describe a rule that you add to a policy as `People in the IT department may not be given accounting responsibilities`.

Allowed Number of Roles

Identifies how many roles to which a user can belong.

Roles

Identifies the roles that are associated with the policy rule.

To view a list of roles and users that have ownership of the policy, click the  icon adjacent to **Policy Owners**.

Role Policy Owners table

Lists the role owners of the policy. The table contains these columns:

Role Name

Identifies the name of the role.

Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

User Policy Owners table

Lists the users who are owners of the policy. The table contains these columns:

Full Name

Identifies a value for distinguishing a user, such as the user's full name. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the user's e-mail address.

Last Name

Identifies the user's last name.

Business Unit

Identifies the business unit associated with the user.

Policy state

Indicates the status of the policy. **Enabled** indicates that the policy is active. **Disabled** indicates that the policy is inactive. The policy state is enabled by default.

Click **Close** when you have finished reviewing the policy.

Related information

For more information, see the [IBM Knowledge Center](#).

Create Policy Rule

Use this page to create a rule for the separation of duty policy.

Description of separation

Type a description for the policy rule. For example, you might describe a rule that you add to a policy as **People in the IT department cannot be given accounting responsibilities**.

Build Role Separation List

Lists the roles to which this policy rule applies. You can add one or more roles to the role separation list.

Role name

Displays the name of the static role that you want to add to the role separation list.

Select

Specifies a static role. To select one or more static roles, select the check box next to the static role. To select all static roles, select the check box at the top of the column.

Name

Displays the name of the static role.

Description

Displays information about the intended purpose of the static role.

Business Unit

Identifies the business unit in which the static role is specified.

Allowed Number of Roles

Identifies how many roles to which a user can belong.

You can use these buttons:

Add

Click to add a static role to the role separation list. If you type the exact name of an existing role in the **Role name** field and click **Add**, the role is immediately added to the list. If you type a value in the **Role name** field that does not exactly match a role or matches more than one role, a search panel opens from which you can select the appropriate roles.

Note: You can search only for the roles for which you have permission.

Search

Click to search for one or more static roles to add to the role separation list.

Remove

Click to remove one or more static roles from the role separation list.

Related information

For more information, see the [IBM Knowledge Center](#).

Change Policy Rule

Use this page to change a rule for the separation of duty policy.

Description of separation

Type a description for the policy rule. For example, you might describe a rule that you add to a policy as **People in the IT department cannot be given accounting responsibilities**.

Build Role Separation List

Lists the roles to which this policy rule applies. You can add one or more roles to the role separation list.

Role name

Displays the name of the static role that you want to add to the role separation list.

Select

Specifies a static role. To select one or more static roles, select the check box next to the static role. To select all static roles, select the check box at the top of the column.

Name

Displays the name of the static role.

Description

Displays information about the intended purpose of the static role.

Business Unit

Identifies the business unit in which the static role is specified.

Allowed Number of Roles

Identifies how many roles to which a user can belong.

You can use these buttons:

Add

Click to add a static role to the role separation list. If you type the exact name of an existing role in the **Role name** field and click **Add**, the role is immediately added to the list. If you type a value in the **Role name** field that does not exactly match a role or matches more than one role, a search panel opens from which you can select the appropriate roles.

Note: You can search only for the roles for which you have permission.

Search

Click to search for one or more static roles to add to the role separation list.

Remove

Click to remove one or more static roles from the role separation list.

Related information

For more information, see the [IBM Knowledge Center](#).

Policy Rule Details

Use this page to view the details of a rule for the separation of duty policy.

Description of separation

Provides a description for the policy rule.

Build Role Separation List

Lists the roles to which this policy rule applies.

Name

Displays the static role's name.

Description

Displays information about the intended purpose of the static role.

Business Unit

Identifies the business unit in which the static role is specified.

Allowed Number of Roles

Identifies how many roles to which a user can belong.

Related information

For more information, see the [IBM Knowledge Center](#).

Organizational Role

Use this page to select a role you want to add.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Role name or description searches for a role with a name or description that contains text that is entered in the **Search information** field.

Business unit searches for a role associated with a business unit that contains text that is entered in the **Search information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Roles table

Lists the roles matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Name

Identifies the name of the role.

Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

Role Type

Indicates whether the role is static or dynamic.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Violations and Exemptions Summary

Use this page to view violation and exemption information and make any necessary changes for each rule in your separation of duty policy.

Total number of violations

Identifies the total number of violations that were found when the policy was last evaluated.


Total number of exemptions

Identifies the total number of violations that are currently exempted.

Order rules

Select the order in which you want the rules to appear. You can sort alphabetically on the name of the rule or by the number of violations or exemptions. Click **Sort** to sort the rules.

Rule list

Lists the rules for the policy that you have selected. Click on the  icon to toggle the rule open or closed. For each rule, there is a **Violations** table and an **Exemptions** table.

Violations table

Lists the separation of duty policy violations. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a violation. To select one or more violations, select the check box adjacent to the violation. To select all violations, select the check box at the top of the column.

Date of Violation

Indicates the date that the violation was identified.

User Name

Identifies the name of the user who violates the separation of duty policy.

Roles in Conflict

Provides the names of the roles in which the user has membership that violate the exclusion rule.

Exemptions table

Lists the separation of duty policy violations that are currently exempt from action. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an exemption. To select one or more exemptions, select the check box adjacent to the exemption. To select all exemptions, select the check box at the top of the column.

User Name

Identifies the name of the user who violates the separation of duty policy.

Approved By

Identifies the user who approved the exemption.

Date Approved

Identifies the date and time of the exemption approval.

Roles in Conflict

Provides the names of the roles in which the user has membership that violate the exclusion rule.

Approval Notes

Provides information about the exemption approval.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Approve

On the **Violations** table, click to approve the exemption for a selected separation of duty policy violation.

Revoke

On the **Exemptions** table, click to revoke the exemption for a selected separation of duty policy violation.

Related information

For more information, see the [IBM Knowledge Center](#).

Approve Violations

Use this page to approve separation of duty policy rule violations.

Violation Summary table

Lists the separation of duty policy violations. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Date of Violation

Indicates the date that the violation was identified.

User Name

Identifies the name of the user who violates the separation of duty policy exclusion rule.

Roles in Conflict

Identifies the roles the user has membership in which violate the exclusion rule.

Notes

Provide a reason for approving the violation.

You can use these buttons:

Approve

Click to approve the separation of duty policy rule violation.

Cancel

Click to cancel the operation and to return to the previous page.

Related information

For more information, see the [IBM Knowledge Center](#).

Revoke Exemptions

Use this page to revoke exemptions for separation of duty policy rule violations.

Exemption Summary table

Lists the separation of duty policy exemptions. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

User Name

Identifies the name of the user who violates the separation of duty policy exclusion rule.

Approved By

Identifies the user who approved the exemption.

Date Approved

Identifies the date and time of the exemption approval.

Roles in Conflict

Identifies the roles the user has membership in which violate the exclusion rule.

Approval Notes

Provides information about the exemption approval.

Notes

Provide a reason for revoking the exemption.

You can use these buttons:

Revoke

Click to revoke the exemption for the separation of duty policy rule violation.

Cancel

Click to cancel the operation and to return to the previous page.

Related information

For more information, see the [IBM Knowledge Center](#).

Separation of Duty Policy Violation

Use this page to view the separation of duty policy violation details. For example, this page might display a user with roles that violate some separation of duty policies.

Separation of Duty Policy Violation Details table

Lists the rules and roles in violation of the separation of duty policy. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Person Name

This column is displayed when adding users to a role. It identifies the name of the person that is violating the separation of duty policy.

Rule Name

Identifies the rule name that is associated with the separation of duty policy.

Roles in Conflict

Identifies the conflicting roles in a separation of duty policy to which a user can belong.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Submit

Click to submit your request after you have verified the information for the policy. This request creates the appropriate approval to be generated.

Cancel

Click to return to the previous page.

Related information

For more information, see the [IBM Knowledge Center](#).

Password Policies

Select Password Policies

Use this page to create, change, or delete password policies.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Password policy name searches for password policy names, descriptions, captions, or keywords that contain the text that is entered in the **Search information** field.

Service searches for password policies that specify service targets that have a service name or description that contains the text that is entered in the **Search information** field.

Business unit searches for password policies defined in business units that have a business unit name or description that contains the text that is entered in the **Search information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Note: If password synchronization is enabled, the administrator needs to ensure that password policies do not have any conflicts. When password synchronization is enabled, the system combines policies for all accounts owned by the user to determine the password to be used. If there are conflicts between password policies, the password might not be set.

Password Policies table

Lists the policies matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a password policy. To select one or more password policies, select the check box adjacent to the password policy. To select all password policies, select the check box at the top of the column.

Password Policy Name

Identifies the name of the password policy. Click the name to view or change the password policy.

Description

Identifies a brief description of the password policy.

Status

Identifies the status of the policy as enabled or disabled.

Targets

Identifies the services or service types to which the password policy applies.

Business Unit

Identifies the business unit that is associated with the password policy. Click the name to view the business unit details.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new password policy.

Change

Click to change a selected password policy.

Delete

Click to delete one or more selected password policies.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Password Policies

Use this notebook to specify details related to a password policy.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to specify information about a password policy. If you are viewing an existing policy and you do not have access control item permission to change the policy, some of the information on this page is displayed in read-only mode.

Name

Provide the name of the password policy.

Caption

Provide additional information about the policy. For example, the caption can state the policy name, who created the policy, and the date the policy was created.

Description

Provide a description of the intended purpose of the password policy.

Keywords

Provide a word or words that reference the password policy.

Business unit

Select the business unit. To locate an available business unit, click **Search**.

Make policy available to services in

Select the extent to which the password policy applies.

This business unit and its subunits

Applies to services in the specified business unit and all subordinate business units.

This business unit only

Applies to services in the specified business unit only.

Status

Click **Enabled** to use the policy and make it active, or click **Disabled** to make the policy inactive.

After you have specified the required information for the policy, click **Apply** to save your changes and continue.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Targets

Use this page to add or remove services or service types to which the password policy applies. If you are viewing an existing policy and you do not have access control item permission to change the policy, some of the information on this page is displayed in read-only mode.

You can have only one active password policy scoped to the same user type and business unit that specifies the same target.

All service types

Click to apply the password policy to all service types.

Services table

Lists the services and service types matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box adjacent to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view the service details.

If the target is a service type, an asterisk (*) is displayed, and detailed information about the service is not available.

Description

Identifies a brief description of the service.

Service Type

Identifies the name of the service type.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a service or service type.

Remove

Click to remove one or more selected services or service types.

Apply

Click to save your changes and continue after you have specified the required information for the policy.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Rules

Use this page to set password attributes that a password policy uses to determine whether a password is valid. For example, you might define settings that disallow the use of a user name or a user ID as a password. If you are viewing an existing policy and you do not have access control item permission to change the policy, some of the information on this page is displayed in read-only mode.

Password Rule table

Lists the available set of password strength rules that you can set in your password policy. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Password Rule

Lists the [“Password Strength Rules”](#) on page 328.

Setting

Type the value for the password strength rule. For example, for the **Minimum length** rule, you might type an 8 in the field to specify that passwords must contain at least 8 characters.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Apply** to save your changes and continue.

Related information

For more information, see the [IBM Knowledge Center](#).

Password Strength Rules

You can set password strength rules that a password policy uses to determine whether a password is valid.

The following table describes each password strength rule.

Attribute	Description
Maximum length	Enter the maximum number of characters that a password can contain. For example: if value of this rule set to 6, then password should have at least 6 characters.

Table 8. Descriptions of the password attributes (continued)

Attribute	Description
Minimum length	Enter the minimum number of characters that a password can contain. For example: if value of this rule set to 12, then user is allowed to set password up to 12 characters.
Maximum repeated characters	Enter the maximum number of duplicate characters that a password can contain. For example, if value of this rule is 2, then user can not add PPP as part of the password.
Minimum unique characters	Enter the minimum number of unique characters that a password must contain. For example: if value of this rule is 3, then password should have at least 3 unique characters such as abcdcba.
Minimum alphabetic characters	Enter the minimum number of alphabetic characters that a password must contain. For example: if value of this rule is 3, then password should have at least 3 alphabets, such as a1b2c3d.
Minimum numeric characters	Enter the minimum number of numeric characters that a password must contain. For example: if value of this rule is 3, then password should have at least 3 numbers, such as a1b2c3d.
Characters not allowed	Enter characters that are not allowed in the password. Do not separate any characters with a space or another delimiter, unless a space or the delimiter is a disallowed character. For example: if you want to specify _- {}& * as disallowed characters, then a correct value for this field is: <div style="background-color: #f0f0f0; padding: 2px; margin: 5px 0;">_ - { } & *</div> An incorrect value for this field is: <div style="background-color: #f0f0f0; padding: 2px; margin: 5px 0;">_ - { } & *</div> or: <div style="background-color: #f0f0f0; padding: 2px; margin: 5px 0;">_ , - , , { , } , & , *</div>

Table 8. Descriptions of the password attributes (continued)

Attribute	Description
Required characters	<p>Enter character that must be in the password. Do not use a comma or a space or another delimiter.</p> <p>For example: if password value must contain a, b and c characters then a correct value for this field is:</p> <p>abc</p> <p>An incorrect value for this field is:</p> <p>a b c</p> <p>or:</p> <p>a, b, c</p>
Restricted to characters	<p>Enter the set of characters to which the password is restricted. That is, the password must contain only these characters. Do not separate any characters with a space or another delimiter, unless a space or the delimiter is a character that must be specified.</p> <p>For example: If you want to specify all lowercase letters then a correct value for this field is:</p> <p>abcdefghijklmnopqrstuvwxyz</p> <p>An incorrect value for this field is:</p> <p>a b c d e f g h i j k l m n o p q r s t u v w x y z</p> <p>or:</p> <p>a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z</p>
Starts with characters	<p>Enter the sequence of characters that the password must start with. Do not separate any characters with a space or another delimiter, unless a space or the delimiter is a character that must be specified.</p> <p>For example, if you want to specify that a password should start with 1234 then a correct value for this field is:</p> <p>1234</p> <p>An incorrect value for this field is:</p> <p>1 2 3 4</p> <p>or:</p> <p>1, 2, 3, 4</p>

Table 8. Descriptions of the password attributes (continued)

Attribute	Description
Repeated history length	<p>Enter the number of passwords that are retained. This value specifies how many unique passwords must be used before a previous password can be re-used. Passwords that match any password in the history list cannot be reused. The history is updated every time the password is changed.</p> <p>For example, if this value is 7, then the password must be changed 7 times to different passwords before the old password can be reused.</p>
Reversed history length	<p>Enter the numeric value that specifies how many passwords, spelled backwards are kept in history. Passwords that match any password in the history list cannot be reused. The history is updated every time the password is changed.</p> <p>For example, if the value for this rule is 7, then the password must be changed 7 times to different passwords before the old password (spelled backwards) can be reused.</p>
Disallow user name	<p>Select the check box to disallow the use of the user name as a password. The comparison is case sensitive.</p> <p>For example, if username is John, then user is not allowed to set a password containing the word John.</p>
Disallow user name (case-insensitive)	<p>Select the check box to disallow the use of the user name as a password. The comparison is case insensitive.</p> <p>For example, if username is John, then user is not allowed to set a password containing the word John, john, johN, or any variation of John as part of the password.</p>
Disallow user ID	<p>Select the check box to disallow the use of the user ID as a password. The comparison is case sensitive.</p> <p>For example, if user ID is JSmith, then user is not allowed to set password containing word JSmith. Since the comparison is case-sensitive, the user can have Jsmith, jsmith, or other variations as part of the password.</p>
Disallow user ID (case-insensitive)	<p>Select the check box to disallow the use of the user ID as a password. The comparison is case insensitive.</p> <p>For example, if user ID is JSmith, then user is not allowed to set password containing the word JSmith, Jsmith, jsmith, or other variations as part of the password.</p>
Do not allow in dictionary	<p>Select the check box to reject the password if its value matches a term in a dictionary that you configure, containing a list of unwanted terms.</p> <p>Note: This option is only available when a dictionary is configured.</p>

Table 8. Descriptions of the password attributes (continued)

Attribute	Description
Passwords must contain characters from three of the four categories	Select the check box to enable a "three of four categories" rule. This rule is compatible with the same rule in Microsoft Active Directory. The categories are as follows: <ol style="list-style-type: none"> 1. Uppercase letter A through Z 2. Lowercase letter a through z 3. Number 0 through 9 4. Special character (nonalphanumeric): <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> ~!@#%\$%^&* _ - += ` \ () { } [] ; : " ' < > , . ? / </div> There is no category available for Unicode characters. They are not currently supported.

Related information

For more information, see the [IBM Knowledge Center](#).

Add Targets

Use this page to specify the service or service type that you want to associate with the policy.

Target type

Select whether you are adding a service or service type to the policy.

Service

Use the fields to search for a service. Then, select the service from the **Services** table.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Service searches for service names or descriptions that contain the text that is entered in the **Search information** field.

Business unit searches for services defined in business units that have a business unit name or description that contains the text that is entered in the **Search information** field.

Service type

Select a service type from the list.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Services table

Lists the services matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box adjacent to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view the service details.

Description

Identifies a brief description of the service.

Service Type

Identifies the type of service.

Business Unit

Identifies the business unit to which the service applies.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Service type

Select the service type from the **Service Type** table.

Service Type table

Lists the service types that you can choose. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service type. To select one or more service types, select the check box adjacent to the service type. To select all service types, select the check box at the top of the column.

Service Type Name

Identifies the name of the service type.

Description

Identifies a brief description of the service.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

[For more information, see the IBM Knowledge Center.](#)

ID Policies

Work with Identity Policies

Use this page to create, change, or delete identity policies.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Identity policy searches for identity policy names, descriptions, captions, or keywords that contain the text that is entered in the **Search information** field.

Service searches for identity policies that specify service targets that have a service name or description that contains the text that is entered in the **Search information** field.

Business unit searches for identity policies defined in business units that have a business unit name or description that contains the text that is entered in the **Search information** field.

Identity Policies table

Lists the identity policies matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an identity policy. To select one or more identity policies, select the check box adjacent to the identity policy. To select all identity policies, select the check box at the top of the column.

Identity Policy Name

Identifies the name of the identity policy. Click the name to view or change the identity policy.

Description

Identifies a brief description of the identity policy.

User Type

Identifies the scope of the identity policy to apply only to people of a certain type.

Status

Identifies the status of the policy as enabled or disabled.

Targets

Identifies the services or service types to which the identity policy applies.

Business Unit

Identifies the business unit that is associated with the identity policy. Click the name to view the business unit details.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new identity policy.

Change

Click to change a selected identity policy.

Delete

Click to delete one or more selected identity policies.

Manage Identity Policies

Use this notebook to specify information about an identity policy.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to specify information about an identity policy. If you are viewing an existing policy and you do not have access control item permission to change the policy, some of the information on this page is displayed in read-only mode.

Name

Provide the name of the identity policy.

Caption

Provide additional information about the policy. For example, the caption can state the policy name, who created the policy, and the date that the policy was created.

Description

Provide a description of the intended purpose of the identity policy.

Keywords

Provide a word or words that reference the identity policy.

Status

Click **Enabled** to use the policy and make it active, or click **Disabled** to make the policy inactive.

User type

Provide the type of user to which the identity policy applies.

Make policy available to services in

Select the extent to which the identity policy applies.

This business unit and its subunits

Applies to services in the specified business unit and all subordinate business units.

This business unit only

Applies to services in the specified business unit only.

Business unit

Select the business unit. To locate an available business unit, click **Search**.

After you have specified the required information for the policy, click **Apply** to save your changes and continue.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Targets

Use this page to add or remove services or service types to which the identity policy applies. If you are viewing an existing policy and you do not have access control item permission to change the policy, some of the information on this page is displayed in read-only mode.

You can have only one active identity policy scoped to the same user type and business unit that specifies the same target.

All service types

Click to apply the identity policy to all service types.

Targets table

Lists the services or service types that you can apply to the identity policy. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box adjacent to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view the service details.

If the target is a service type, an asterisk (*) is displayed, and detailed information about the service is not available.

Description

Identifies a brief description of the service.

Service Type

Identifies the name of the service type.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a service or service type.

Remove

Click to remove one or more selected services or service types.

Apply

After you have specified the required information for the policy, click to save your changes and continue.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Rule

Use this page to specify the schema attributes that the identity policy uses to create a user ID. If you are viewing an existing policy and you do not have access control item permission to change the policy, some of the information on this page is displayed in read-only mode.

Input mode

Simple - define rule

Applies a rule using schema attributes.

First attribute

Select an attribute from the list.

Character limit

Type a numeric value that identifies the number of characters to use from this attribute. If a character limit is not specified, all characters of the attribute are used.

Apply case

Select the type of case to apply to this attribute from the list.

Second attribute

Select a different attribute from the list.

Character limit

Type a numeric value that identifies the number of characters to use from this attribute. If a character limit is not specified, all characters of the attribute are used.

Apply case

Select the type of case to apply to this attribute from the list.

Advanced - define script

Type a script to define a custom identity policy.

Click **Apply** to save your changes and continue.

Related information

For more information, see the [IBM Knowledge Center](#).

Add Targets

Use this page to specify the service or service type that you want to associate with the policy.

Target type

Select whether you are adding a service or service type to the policy.

Service

Use the fields to search for a service. Then, select the service from the **Services** table.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Service searches for service names or descriptions that contain the text that is entered in the **Search information** field.

Business unit searches for services defined in business units that have a business unit name or description that contains the text that is entered in the **Search information** field.

Service type

Select a service type from the list.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Services table

Lists the services matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box adjacent to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view the service details.

Description

Identifies a brief description of the service.

Service Type

Identifies the type of service.

Business Unit

Identifies the business unit to which the service applies.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Service type

Select the service type from the **Service Type** table.

Service Type table

Lists the service types that you can choose. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service type. To select one or more service types, select the check box adjacent to the service type. To select all service types, select the check box at the top of the column.

Service Type Name

Identifies the name of the service type.

Description

Identifies a brief description of the service.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Provisioning Policies

Manage Provisioning Policies

Use this page to create, change, or delete provisioning policies.

Policy information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Specify one of these filters:

Provisioning policy

List provisioning policies that you have the appropriate authority to view or change. Type a value in the **Policy information** field and click **Search**.

Business unit

List provisioning policies that are associated with a business unit that you specify. Type a value in the **Policy information** field and click **Search**.

Role

List provisioning policies that are associated with a role that you specify. If you do not have the appropriate authority to view or change the provisioning policy, a warning message appears.

- To see all policies for all roles in the **Provisioning Policies** table, click **Search**.
- To work with provisioning policies for a specific role, click **Search...**

On the **Select Roles** page:

- Select **Role name or description** or select **Business unit**.
- Click **Search**.
- Select a role from the **Roles** table and click **OK**.
- To see all policies associated with the selected role, click **Search**.

Provisioning Policies table

Lists the policies matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a provisioning policy. To select one or more provisioning policies, select the check box adjacent to the provisioning policy. To select all provisioning policies, select the check box at the top of the column.

Provisioning Policy

Identifies the name of the provisioning policy. Click the name to make changes to the policy.

Description

Identifies a brief description of the provisioning policy.

Status

Identifies the status of the policy as enabled, disabled, or draft. When you commit a draft policy to the system, the committed policy replaces the original policy, which is removed from the system, along with the draft version.

Priority

Displays an integer value, which prioritizes policies when policy validation uses several provisioning policies. If two policies define the same attribute entitlement, and the first policy has the lowest priority number (for example 1), only the attribute entitlement definition of the first policy is used. The attribute entitlement definition of the second policy (for example, 10) is ignored.

Business Unit

Identifies the business unit that is associated with the provisioning policy. Click the name to view the business unit details.

Role Association

Identifies the association between the policy and the role. This column is displayed only when "Role" is selected for the search. If a role is a member of another organizational role in a provisioning policy, then that role member also inherits the permissions of the provisioning policies of the ancestor roles. The role association can be either Direct or Inherited. Direct association indicates that the policy is directly associated with the role. Inherited association indicates that the policy is associated with the role by inheritance from an ancestor role in the role hierarchy.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new provisioning policy.

Change

Click to change a selected provisioning policy.

Delete

Click to delete one or more selected provisioning policies.

Refresh

Click to update items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Provisioning Policies

Use this notebook to specify information about a provisioning policy.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to specify information about a provisioning policy, including the name, scope, status, and priority. If you are viewing an existing policy and you do not have access control item permission to change the policy, some of the information on this page is displayed in read-only mode.

Policy name

Provide the name of the provisioning policy.

Caption

Provide additional information about the policy. For example, the caption can state the policy name, who created the policy, and the date the policy was created.

Make policy available to services in

Select the extent to which the provisioning policy applies.

This business unit and its subunits

Applies to services in the specified business unit and all subordinate business units.

This business unit only

Applies to services in the specified business unit only.

Description

Provide additional information about the intended purpose of the provisioning policy.

Policy status

Indicates whether the policy is enabled or disabled.

Priority

Indicates an integer value, which prioritizes policies when policy validation uses several provisioning policies. If two policies define the same attribute entitlement, and the first policy has the lowest priority number (for example, 1), only the attribute entitlement definition of the first policy is used. The attribute entitlement definition of the second policy (for example 10) is ignored.

Keywords

Provide a word or words that reference the provisioning policy.

Business unit

Indicates the business unit to which the provisioning policy applies. To see a list of units, click **Browse**.

You can use these buttons:

Submit

Click to submit your request.

Preview

Click to review the effects of the changes before you make them.

Save as Draft

After you have specified the policy name and at least one entitlement, click to save your changes as a draft and continue.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Members

Use this page to add or remove members from a provisioning policy. If you are viewing an existing policy and you do not have access control item permission to change the policy, some of the information on this page is displayed in read-only mode.

Member type

Select the type of users that are granted access to the policy.

All users in the organization

Applies the provisioning policy to all users and all roles in the same organization.

All other users who are not granted to the entitlements defined by this provisioning policy via other policies

Applies the provisioning policy to users who are not included in other provisioning policies.

Roles specified below

Applies the provisioning policy to the available roles. Select to add or remove a role.

Roles table

Lists the organizational roles that are available. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Name

Identifies the name of the role.

Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a role to the table.

Remove

Click to remove a selected role from the table.

Submit

Click to submit your request.

Preview

Click to review the effects of the changes before you make them.

Save as Draft

After you have specified the policy name and at least one entitlement, click to save your changes as a draft and continue.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Entitlements

Use this page to create, change, or delete entitlements, or to change the parameters of an entitlement. If you view an existing policy and do not have access control item permission to change the policy, some of the information is in read-only mode.

Entitlements table

Lists entitlements for accounts on resources. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an entitlement. To select one or more entitlements, select the check box next to the entitlement. To select all entitlements, select the check box at the top of the column.

Name

Identifies the name of the entitlement. Click the name to change the entitlement.

Target Type

Identifies a service type to which the entitlement applies, or a global type.

Provision Option

Indicates whether the entitlement is manually or automatically provisioned to users.

Ownership type

Identifies the ownership type of the account.

Service tag

Identifies the optional service tag values associated with the service type entitlement.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create an entitlement.

Change

Click to change the selected entitlement.

Delete

Click to delete the selected entitlement.

Parameters

Click to manage entitlement parameters. This action is available when you select certain services or service types. It is not available when you select **All Services**.

Submit

Click to submit your request.

Preview

Click to review the effects of the changes before you make them.

Save as Draft

Click to save your changes as a draft and continue.

Cancel

Click to close the current page and go back to the **Work With Provisioning Policies** page.

Related information

For more information, see the [IBM Knowledge Center](#).

Account Entitlement

Use this page to define manual or automatic provisioning of account access and to select an approval workflow to associate with the access.

Provisioning options

Select how the account is provisioned.

Manual

Requires users to manually request account entitlement. If you select this option, the account is provisioned with predefined parameters based on user requests.

Automatic

Automatically provisions new accounts to users, based on defined parameters. This option applies only to individual ownership types.

Ownership type

Select an ownership type that you want to enable for the accounts. Click the arrow to view the available types. The list contains these default ownership types and any custom ownership types. The number of selections depends on the customization.

All: Entitles the accounts to all the ownership types.

Device: Entitles accounts to the Device ownership type.

Individual: Entitles accounts to the Individual ownership type.

System: Entitles accounts to the System ownership type.

Vendor: Entitles accounts to the Vendor ownership type.

Target type

Select a service type from the list.

All Services

Applies the provisioning policy to all services that are provisioned manually. This option cannot be chosen for automatically provisioned accounts.

Service Type

Select a service type from the **Service type** list. Optionally specify one or more service tags. If the service tag field is left blank, this entitlement is applicable to all services of this type within the scope. Otherwise, this entitlement is applicable to this type of services tagged with the specified values and within the scope. For example, an entitlement with DB and LDAP tags is only applicable to any service tagged with DB or LDAP. The tag value comparison is not case-sensitive.

Service Selection Policy

Select a service selection policy from the **Service Selection Policy** list.

Specific Service

Select a specific service from the list. If you select this target type, click **Search** next to the **Service Name** field to select a specific service. The selected service is displayed in the **Service Name** field.

Workflow

Select a workflow to provision account requests. To locate the available workflows, click **Search**. Click **Clear** to remove the currently specified workflow.

Related information

[For more information, see the IBM Knowledge Center.](#)

Entitlement Parameter

Use this page to add, change, or remove parameters for an account.

Parameters table

Lists the constraints and defaults for user attributes that are related to the access. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account attribute. To select one or more account attributes, select the check box adjacent to the account attribute. To select all account attributes, select the check box at the top of the column.

Name

Identifies the name of the account attribute. Click the name to make changes to the attribute.

Template Value

Identifies the string format of the attribute value.

Enforcement Type

Identifies whether the attribute is mandatory, optional, default, or excluded during provisioning.

Value Type

Identifies whether the attribute is a constant, a JavaScript definition, or a regular expression.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new parameter.

Change

Click to change a selected parameter.

Delete

Click to delete a selected parameter.

Continue

Click to save your changes and continue.

Related information

For more information, see the [IBM Knowledge Center](#).

Add New Parameter

Use this page to add new attributes to the parameters for an account.

Attributes table

Lists the attributes that can be added to an account or access. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an attribute. To select one or more attributes, select the check box adjacent to the attribute. To select all attributes, select the check box at the top of the column.

Attribute Name

Identifies the name of the account attribute.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Continue** to save your changes and continue.

Related information

For more information, see the [IBM Knowledge Center](#).

Define Static Values or JavaScript/Regular Expression

Use this page to create or modify the parameters for account attributes. Some values are dynamic and vary, depending on the attribute that you choose.

The following fields are common for all attributes.

Parameter type

To specify policy parameters, select a parameter type and then complete the fields that the parameter type requires.

Constant value

Specifies a IBM Security Identity Manager constant related to the entitlement.

JavaScript

Specifies a JavaScript expression that defines the entitlement attributes.

Regular Expression

Specifies information about the attributes for a specific service type, which vary for each service. An attribute that you do not specify has a null value.

Null

Specifies a null parameter.

Enforcement type

Specify how the policy enforces the account attribute value during provisioning.

Default

Specifies the default value for the account attribute. Attributes with multiple values have multiple default values.

Mandatory

Specifies a required value for the account attribute. Attributes with multiple values have multiple default values.

Allowed

Specifies one or more values that are permitted for the account attribute. This field applies only to attributes with multiple values.

Excluded

Specifies one or more values that are not permitted for the account attribute, unless the value has been granted by another entitlement. This field applies only to attributes with multiple values.

Related information

For more information, see the [IBM Knowledge Center](#).

Workflows Found

Use this page to find one or more workflows that you want to associate with the provisioning policy.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Workflows Found table

Lists the workflows matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a workflow. To select one or more workflows, select the check box adjacent to the workflow. To select all workflows, select the check box at the top of the column.

Name

Identifies the name of the workflow.

Description

Identifies a brief description of the workflow.

Business Unit

Identifies the business unit to which the workflow applies.

Service Type

Identifies the type of service.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Primary Group

Use this page to assign one or more groups to the primary group entitlement parameter.

Group table

To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box adjacent to the group. To select all groups, select the check box at the top of the column.

Name

Identifies the group's name.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Preview Policy Enforcement

Use this page to preview the impact of the policy on user accounts. You can choose to preview the accounts with policy changes only, or you can preview the accounts with the entire defined policy.

Select how to preview the impact of enforcing the entitlement policy on user accounts.

Enforce changes only

Previews the impact when the current changes to the policy are enforced.

Enforce entire policy

Previews the impact when the entire policy definition is enforced.

Click **Continue** to save your changes and continue.

Related information

For more information, see the [IBM Knowledge Center](#).

Preview Policy Summary

Use this page to preview a summary of how accounts are affected if the provisioning policy changes are submitted. You can choose an account link to view details of the account changes.

Evaluation status

Displays the status of the evaluation as analyzing, partitioning completed, or completed.

Accounts evaluated

Displays the number of accounts that have been evaluated. After the evaluation status is complete, this number shows the total number of accounts that are changed if the provisioning policy is submitted.

Error account

Displays the number of accounts that have generated errors.

Provision new account

Displays the number of accounts that are provisioned when the policy is submitted.

Disallowed account

Click to display the number of accounts that are disallowed if the provisioning policy changes are submitted.

Disallowed Account table

To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Enforcement Action

Identifies the actions that are enforced on the accounts.

Number of Accounts

Identifies the number of accounts that are affected.

Noncompliant account

Click to display the number of accounts that are noncompliant if the policy is submitted.

Noncompliant Account table

To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Enforcement Action

Identifies the actions to be enforced on the accounts.

Number of Accounts

Identifies the number of accounts that are affected.

Compliant account

Click to display the number of accounts that are compliant if the policy is submitted.

Compliant Account table

To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Enforcement Action

Identifies the actions that are enforced on the accounts.

Number of Accounts

Identifies the number of accounts that are affected.

Click **Stop Evaluation** to stop evaluating the accounts.

Related information

For more information, see the [IBM Knowledge Center](#).

Preview Disallowed Accounts

Use this page to view the accounts that are disallowed if the provisioning policy is submitted.

Disallowed accounts table

To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select a user ID that is associated with an account.

User ID

Identifies the user ID that is associated with the account. Click the name of the user ID to see the details for the account.

Service Name

Identifies the name of the service for which the user ID has an account.

Owner

Identifies the name of the owner of the user ID.

Status

Identifies the user's status.

Users are either active or inactive. A user must be active to log in to the system. Users become inactive when they are suspended. The suspended users still exist, but they cannot access the system. System administrators can restore inactive users.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **View** to see the details for the account.

Related information

For more information, see the [IBM Knowledge Center](#).

Preview Noncompliant Accounts

Use this page to view the accounts that are noncompliant if the provisioning policy is submitted.

Noncompliant Accounts table

Lists the noncompliant accounts matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select a user ID that is associated with an account.

User ID

Identifies the user ID that is associated with the account. Click the name of the user ID to see the details for the account.

Service Name

Identifies the name of the service for which the user ID has an account.

Owner

Identifies the name of the owner of the user ID.

Status

Identifies the user's status.

Users are either active or inactive. A user must be active to log in to the system. Users become inactive when they are suspended. The suspended users still exist, but they cannot access the system. System administrators can restore inactive users.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **View** to see the details for the account.

Related information

For more information, see the [IBM Knowledge Center](#).

Preview Compliant Accounts

Use this page to view the accounts that are compliant if the provisioning policy is submitted.

Compliant accounts table

To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select a user ID that is associated with an account.

User ID

Identifies the user ID that is associated with the account. Click the name of the user ID to see the details for the account.

Service Name

Identifies the name of the service for which the user ID has an account.

Owner

Identifies the name of the owner of the user ID.

Status

Identifies the user's status.

Users are either active or inactive. A user must be active to log in to the system. Users become inactive when they are suspended. The suspended users still exist, but they cannot access the system. System administrators can restore inactive users.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **View** to see the details for the account.

Related information

For more information, see the [IBM Knowledge Center](#).

Preview New Accounts

Use this page to view the accounts that are created if the provisioning policy is submitted.

New accounts table

To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select a user ID that is associated with an account.

User ID

Identifies the user ID that is associated with the account. Click the name of the user ID to see the details for the account.

Service Name

Identifies the name of the service for which the user ID has an account.

Owner

Identifies the name of the owner of the user ID.

Status

Identifies the user's status.

Users are either active or inactive. A user must be active to log in to the system. Users become inactive when they are suspended. The suspended users still exist, but they cannot access the system. System administrators can restore inactive users.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **View** to see the details for the account.

Related information

For more information, see the [IBM Knowledge Center](#).

Preview Evaluation Errors

Use this page to view the errors that occurred during the evaluation of the provisioning policy.

Evaluation Errors table**Service Name**

The name of the service that the account is provisioned to.

Attribute Name

The name of the attribute for which an error occurred when generating a value.

User Name

The name of the user that the account is provisioned to.

Errors

The error messages that were generated.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Preview Account Attributes

Use this page to view the account attributes to be changed if the provisioning policy changes are submitted.

Account attributes table

Lists the account attributes matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Attribute Name

Identifies the name of the account attribute.

Old Value

Identifies the existing account attribute value.

New Value

Identifies the new value of the account attribute.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Service Selection Policies

Work with Service Selection Policies

Use this page to create, change, or delete service selection policies.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Service selection policy searches for service selection policy names that contain the text that is entered in the **Search information** field.

Business unit searches for service selection policies defined in business units that have a business unit name or description that contains the text that is entered in the **Search information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Service Selection Policies table

Lists the policies matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service selection policy. To select one or more service selection policies, select the check box adjacent to the service selection policy. To select all service selection policies, select the check box at the top of the column.

Policy Name

Identifies the name of the service selection policy. Click the name to view or change the service selection policy.

Description

Identifies a brief description of the service selection policy.

Service Type

Identifies the name of the service type, such as Windows Active Directory.

Business Unit

Identifies the business unit that is associated with the service selection policy. Click the name to view the business unit details.

Status

Identifies the status of the policy as enabled or disabled.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new service selection policy.

Change

Click to change the selected service selection policy.

Delete

Click to delete one or more selected service selection policies.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Service Selection Policies

Use this notebook to specify information about a service selection policy.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to specify information about a service selection policy. If you are viewing an existing policy and you do not have access control item permission to change the policy, some of the information on this page is displayed in read-only mode.

Name

Provide the name of the service selection policy.

Caption

Provide additional information about the policy. For example, the caption can state the policy name, who created the policy, and the date the policy was created.

Description

Provide a description of the intended purpose of the service selection policy.

Keywords

Provide a word or words that reference the service selection policy.

Business unit

Select the business unit. To locate an available business unit, click **Search**.

Make policy available to services in

Select the extent to which the service selection policy applies.

This business unit and its subunits

Applies to services in the specified business unit and all subordinate business units.

This business unit only

Applies to services in the specified business unit only.

Status

Click **Enabled** to use the policy and make it active, or click **Disabled** to make the policy inactive.

You can use these buttons:

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request.

Test

Click when the service selection script is complete, to test the script for errors.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Service Type

Use this page to select service types to which the policy applies. If you are viewing an existing policy and you do not have access control item permission to change the policy, some of the information on this page is displayed in read-only mode.

Service Type table

To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select a service type.

Service Type

Identifies the name of the service type.

Description

Identifies a brief description of the service type.

You can use these buttons:

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request.

Test

Click when the service selection script is complete, to test the script for errors.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Service Selection Script

Use this page to add and test a service selection script for the policy. If you are viewing an existing policy and you do not have access control item permission to change the policy, some of the information on this page is displayed in read-only mode.

The use of JavaScript in service selection policies allow for greater control over how accounts are provisioned and allows a single provisioning policy to provision many accounts to different services and service instances.

Script

Type the JavaScript code to be used by the provisioning policy to determine a service to which the account should be provisioned.

You can use these buttons:

Submit Now

Click to submit your request immediately.

Schedule Submission

Click to schedule your request.

Test

Click when the service selection script is complete, to test the script for errors.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule

Use this page to submit a request.

Immediate

Runs the request immediately after you click the button to complete the task.

Effective date

Runs the request at a day and hour that you specify. After you select this option, click the calendar icon to specify the scheduled day, and click the clock icon to specify the scheduled hour.

Click **Submit** to perform or schedule the request.

Related information

For more information, see the [IBM Knowledge Center](#).

Recertification Policies

Recertification Policies

Use this page to create, change, or delete recertification policies.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Name or description searches for recertification policy names or descriptions that contain the text that is entered in the **Search information** field.

Service name searches recertification policies that specify service targets that have a service name or description that contains the text that is entered in the **Search information** field.

Access name searches recertification policies that specify access targets that have an access name or description that contains the text that is entered in the **Search information** field.

Recertification Policies table

Lists the recertification policies matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a recertification policy. To select one or more recertification policies, select the check box adjacent to the recertification policy. To select all recertification policies, select the check box at the top of the column.

Name

Identifies the name of the recertification policy. Click the name to view or change the recertification policy.

Description

Provides information about the recertification policy.

Status

Identifies the status of the policy as enabled or disabled.

Targets

Identifies the services or accesses to which the recertification policy applies.

Target Type

Identifies the name of the target type, such as accesses, accounts, or users, to which the recertification policy applies. A value of *All indicates that the workflow applies to all target types.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new recertification policy.

Change

Click to change a selected recertification policy.

Delete

Click to delete one or more selected recertification policies.

Run

Click to immediately run one or more selected recertification policies. Any schedule that is defined in the policy is also used.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Recertification Policies

Use this wizard to create a recertification policy. Specify general information, services, participant notices and confirmation notices associated with the recertification policy.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to specify general information about a recertification policy.

Name

Provides the name of the recertification policy. You must specify a name for the recertification policy.

Description

Provides a information about the intended purpose of the recertification policy.

Policy status

Click **Enabled** to use the recertification policy and make it active, or click **Disabled** to make the policy inactive.

Business unit

Click **Search** to search for and select a business unit. Selecting a specific business unit configures the policy to apply to that unit. The business unit to which the policy applies affects the placement of the policy for access control items and administrative delegation, and also sets the scope of targets such as services and accesses.

Scope of this policy in relation to its business unit

Select the range within the business unit you have selected for this policy.

Apply this policy to the business unit and sub units

Applies the policy to the business unit and any subunits.

Apply this policy only to the business unit

Applies the policy only to the business unit. The policy does not apply to any resources in subunits of the business unit.

Related information

For more information, see the [IBM Knowledge Center](#).

Target Type

Use this page to specify the type of user access to recertify.

Policy recertifies

Select the type of user access for this policy to recertify.

Accesses

Applies to access entitlements.

Accounts

Applies to services that provide access to accounts.

Users

Applies to all the roles, accounts, and groups belonging to a user.

Related information

For more information, see the [IBM Knowledge Center](#).

Account Recertification Pages

Use these pages to specify information about an account recertification.

Related information

For more information, see the [IBM Knowledge Center](#).

Service Target

Use this page to add or remove services to which the recertification policy applies. You must specify at least one service for the recertification policy. You cannot associate more than one recertification policy with a service. This notebook page is displayed only for an account recertification.

Services table

Contains a list of services to which the recertification policy applies. You can only view and select services under the business unit of the policy. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box adjacent to the service.

To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view the service details.

Description

Identifies a brief description of the service.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a service.

Remove

Click to remove one or more selected services.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule

Use this page to schedule when recertification occurs, either on a specific date and time on the calendar, or at a specified interval.

Schedule type

Select whether recertification occurs on a given day, or after an interval of time since the last recertification.

Calendar

Run recertification on a specific date and time.

Rolling

Recertify targets that have not been recertified within a specified time interval. This field only appears for an account or user recertification. If you select **Rolling**, you must also type the number of days for the time interval in the **Rolling interval in days** field.

Evaluation frequency

Select one of these schedule intervals to run recertification:

Daily

Recertifies targets every day. After you select this option, click the clock icon to specify a time in the **At this time** field.

Weekly

Recertifies targets once a week. After you select this option, select a day from the list in the **On this day of the week** field. Then, click the clock icon to specify a time in the **At this time** field.

Monthly

Recertifies targets once a month. After you select this option, select a date from the list in the **On this day of the month** field. Then, click the clock icon to specify a time in the **At this time** field.

Hourly

Recertifies targets every hour. After you select this option, select a time from the list in the **At this minute** field.

Annually

Recertifies targets on a specific day of the year that you specify. After you select this option, select a month from the list in the **Month** and a date from the list in the **On this day of the month** field. Then, click the clock icon to specify a time in the **At this time** field.

During a specific month

Recertifies targets on a month that you specify. After you select this option, select a month from the list in the **Month** and a day of the week from the list in the **On this day of the week** field. Then, click the clock icon to specify a time in the **At this time** field.

Quarterly

Recertifies targets on a specific day of the quarter that you specify. After you select this option, select a day from the list in the **On this day** field. Then, click the clock icon to specify a time in the **At this time** field.

Semi-Annually

Recertifies targets on a specific day of the half year that you specify. After you select this option, select a day from the list in the **On this day** field. Then, click the clock icon to specify a time in the **At this time** field.

Related information

For more information, see the [IBM Knowledge Center](#).

Policy

Use this page to specify who approves an account or access recertification, who receives notification, and other actions.

Configuration mode

Select whether approval is based on the specified fields, or use the workflow designer to configure approval.

Simple

Use the fields below to specify the policy.

Who approves recertification

Specifies a participant who receives notification and an activity item when recertification is due. Ensure that the approvers you select have access to the View Activities task.

Action when recertification is rejected

Specifies an action, such as suspend or delete, that occurs when a participant declines to recertify an account.

Send rejection e-mail to

Specifies a recipient, such as a manager, who is notified when recertification is declined.

Days until recertification is due

Specifies a value for the number of days that the participant has to respond to the recertification request. If the participant does not respond to the recertification request in the specified time, the recertification is overdue and an overdue action can be taken.

Action when recertification is overdue

Specifies an action, such as reject or approve, that occurs when the recertification participant does not respond to the recertification request in the specified time. If you select **Take no action**, the activity remains as an overdue activity after the due date has passed.

User type

Specifies the scope of the recertification policy to apply only to people of a certain type on the given policy schedule.

Advanced

Use the workflow designer to configure who approves recertification, who receives notification, and other actions for the recertification policy. Policy definitions that you create in the workflow designer cannot later be modified using the simple method.

Workflows can be as simple as requiring only one approval, or they can be as complex as requiring multiple approvals with RFIs, loops, and so on. Manual activities that are defined in the workflow populates an individual participant's To Do list as each process in the workflow is completed. At any point, the system administrator can view any user's To Do list and act as the Participant, overriding the approval authority.

To define a workflow, drag and drop the design nodes from the node palette onto the workflow design space and connect them with transition lines.

After you place a design node on the workflow design space, double-click the node to configure its properties.

Workflow design interface

The workflow designer has these areas:

Workflow Name

Displays the name of the workflow.

Service Type

Displays the name of the service type.

Node palette

Displays all available nodes in the left pane of the interface.

Design space

Displays the nodes that you are working with in the large pane of the interface.

High Contrast

Select this check box to display the workflow design interface without color representing the design nodes.

Properties

Click this button to view configurable properties of the workflow node.

Update

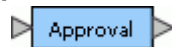
Click this button to refresh the view of the workflow design space.

Save

Saves the changes that you made.

Workflow design nodes

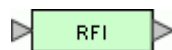
The following workflow design nodes are available:

Approval

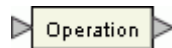
Use this node to define the person who must approve a request or activity before workflow processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Mail

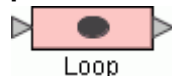
Use this node to configure e-mail notification.

RFI

Use this node to request information from a person. For example, you might need a manager to provide contact information for a new employee before the process of issuing the employee an e-mail account can complete. The person must respond with the information before workflow processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Operation

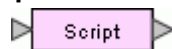
Use this node to initiate an operation workflow that has been defined previously. This workflow can be initiated at any point during the primary workflow.

Loop

Use this node to repeat a specified activity while or until a specified condition is met.

Extension

Use this node to specify a workflow extension to manage people and accounts.

Script

Use this node to specify a JavaScript script that the runs when processing the workflow activities.

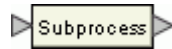
Work Order



Use this node to e-mail a request notification for a manual activity. For example, you might use this node in a workflow to request an ID badge for a new employee. Work order participants are not required to have a IBM Security Identity Manager account. They must, however, have an e-mail address that is stored in the IBM Security Identity Manager directory server.

The **Continue on Participant Resolution Failure** option controls whether or not a workflow process should continue if participant resolution fails.

Subprocess



Use this node to call a previously defined workflow sequence. Several previously defined workflows can serve as subprocesses for a new workflow.

Related information

For more information, see the [IBM Knowledge Center](#).

Recertification E-mail

Use this page to specify the e-mail template that provides recertification notices to participants.

Recertification E-mail table

Lists the templates that can be used for recertification notification. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a template.

Name

Identifies the notification template by name.

Subject

Identifies the subject of the notification template.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

Related information

For more information, see the [IBM Knowledge Center](#).

Create Recertification E-mail

Use this page to create an e-mail notification template.

Template name

Provides the name of the notification template.

Subject

Provides the subject of the e-mail that is generated, using the template.

Plaintext body

Provide the main content of the notification message, in plaintext format. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Provide the XHTML body of the notification message. The content in this section can include images and hyperlinks.

Related information

For more information, see the [IBM Knowledge Center](#).

Rejection E-mail

Use this page to specify the e-mail template that provides rejection notices to participants.

Rejection E-mail table

Lists the templates that can be used for notification of rejected recertification. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a template.

Name

Identifies the notification template by name.

Subject

Identifies the subject of the notification template.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

Related information

For more information, see the [IBM Knowledge Center](#).

Create Rejection E-mail

Use this page to create an e-mail notification template.

Template name

Provides the name of the notification template.

Subject

Provides the subject of the e-mail that is generated, using the template.

Plaintext body

Provide the main content of the notification message, in plaintext format. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Provide the XHTML body of the notification message. The content in this section can include images and hyperlinks.

Related information

For more information, see the [IBM Knowledge Center](#).

View Default Notice

Use this page to view the details that are related to the default e-mail notification.

Template name

Provides the name of the notification template.

Subject

Provides the subject of the e-mail that is generated, using the template.

Plaintext body

Provide the main content of the notification message, in plaintext format. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Provide the XHTML body of the notification message. The content in this section can include images and hyperlinks.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Recertification Pages

Use these pages to specify information about an access recertification.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Target

Use this page to add or remove an access to which the recertification policy applies. You must specify at least one access for the recertification policy. You cannot associate more than one recertification policy with an access. This notebook page only is displayed for an access recertification.

Access Target table

Contains a list of access targets to which the recertification policy applies. You can only view and select accesses under the business unit of the policy. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an access. To select one or more accesses, select the check box adjacent to the access. To select all accesses, select the check box at the top of the column.

Access Name

Identifies the name of the access. Click the name of the access to view the access details.

Description

Identifies a brief description of the access.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add an access.

Remove

Click to remove one or more selected accesses.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule

Use this page to schedule when recertification occurs, either on a specific date and time on the calendar, or at a specified interval.

Schedule type

Select whether recertification occurs on a given day, or after an interval of time since the last recertification.

Calendar

Run recertification on a specific date and time.

Rolling

Recertify targets that have not been recertified within a specified time interval. This field only appears for an account or user recertification. If you select **Rolling**, you must also type the number of days for the time interval in the **Rolling interval in days** field.

Evaluation frequency

Select one of these schedule intervals to run recertification:

Daily

Recertifies targets every day. After you select this option, click the clock icon to specify a time in the **At this time** field.

Weekly

Recertifies targets once a week. After you select this option, select a day from the list in the **On this day of the week** field. Then, click the clock icon to specify a time in the **At this time** field.

Monthly

Recertifies targets once a month. After you select this option, select a date from the list in the **On this day of the month** field. Then, click the clock icon to specify a time in the **At this time** field.

Hourly

Recertifies targets every hour. After you select this option, select a time from the list in the **At this minute** field.

Annually

Recertifies targets on a specific day of the year that you specify. After you select this option, select a month from the list in the **Month** and a date from the list in the **On this day of the month** field. Then, click the clock icon to specify a time in the **At this time** field.

During a specific month

Recertifies targets on a month that you specify. After you select this option, select a month from the list in the **Month** and a day of the week from the list in the **On this day of the week** field. Then, click the clock icon to specify a time in the **At this time** field.

Quarterly

Recertifies targets on a specific day of the quarter that you specify. After you select this option, select a day from the list in the **On this day** field. Then, click the clock icon to specify a time in the **At this time** field.

Semi-Annually

Recertifies targets on a specific day of the half year that you specify. After you select this option, select a day from the list in the **On this day** field. Then, click the clock icon to specify a time in the **At this time** field.

Related information

For more information, see the [IBM Knowledge Center](#).

Policy

Use this page to specify who approves an account or access recertification, who receives notification, and other actions.

Configuration mode

Select whether approval is based on the specified fields, or use the workflow designer to configure approval.

Simple

Use the fields below to specify the policy.

Who approves recertification

Specifies a participant who receives notification and an activity item when recertification is due. Ensure that the approvers you select have access to the View Activities task.

Action when recertification is rejected

Specifies an action, such as suspend or delete, that occurs when a participant declines to recertify an account.

Send rejection e-mail to

Specifies a recipient, such as a manager, who is notified when recertification is declined.

Days until recertification is due

Specifies a value for the number of days that the participant has to respond to the recertification request. If the participant does not respond to the recertification request in the specified time, the recertification is overdue and an overdue action can be taken.

Action when recertification is overdue

Specifies an action, such as reject or approve, that occurs when the recertification participant does not respond to the recertification request in the specified time. If you select **Take no action**, the activity remains as an overdue activity after the due date has passed.

User type

Specifies the scope of the recertification policy to apply only to people of a certain type on the given policy schedule.

Advanced

Use the workflow designer to configure who approves recertification, who receives notification, and other actions for the recertification policy. Policy definitions that you create in the workflow designer cannot later be modified using the simple method.

Workflows can be as simple as requiring only one approval, or they can be as complex as requiring multiple approvals with RFIs, loops, and so on. Manual activities that are defined in the workflow populates an individual participant's To Do list as each process in the workflow is completed. At any point, the system administrator can view any user's To Do list and act as the Participant, overriding the approval authority.

To define a workflow, drag and drop the design nodes from the node palette onto the workflow design space and connect them with transition lines.

After you place a design node on the workflow design space, double-click the node to configure its properties.

Workflow design interface

The workflow designer has these areas:

Workflow Name

Displays the name of the workflow.

Service Type

Displays the name of the service type.

Node palette

Displays all available nodes in the left pane of the interface.

Design space

Displays the nodes that you are working with in the large pane of the interface.

High Contrast

Select this check box to display the workflow design interface without color representing the design nodes.

Properties

Click this button to view configurable properties of the workflow node.

Update

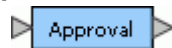
Click this button to refresh the view of the workflow design space.

Save

Saves the changes that you made.

Workflow design nodes

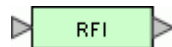
The following workflow design nodes are available:

Approval

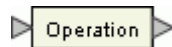
Use this node to define the person who must approve a request or activity before workflow processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Mail

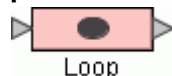
Use this node to configure e-mail notification.

RFI

Use this node to request information from a person. For example, you might need a manager to provide contact information for a new employee before the process of issuing the employee an e-mail account can complete. The person must respond with the information before workflow processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Operation

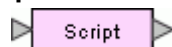
Use this node to initiate an operation workflow that has been defined previously. This workflow can be initiated at any point during the primary workflow.

Loop

Use this node to repeat a specified activity while or until a specified condition is met.

Extension

Use this node to specify a workflow extension to manage people and accounts.

Script

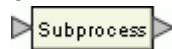
Use this node to specify a JavaScript script that the runs when processing the workflow activities.

Work Order

Use this node to e-mail a request notification for a manual activity. For example, you might use this node in a workflow to request an ID badge for a new employee. Work order participants are not required to have an IBM Security Identity Manager account. They must, however, have an e-mail address that is stored in the IBM Security Identity Manager directory server.

The **Continue on Participant Resolution Failure** option controls whether or not a workflow process should continue if participant resolution fails.

Subprocess



Use this node to call a previously defined workflow sequence. Several previously defined workflows can serve as subprocesses for a new workflow.

Related information

For more information, see the [IBM Knowledge Center](#).

Recertification E-mail

Use this page to specify the e-mail template that provides recertification notices to participants.

Recertification E-mail table

Lists the templates that can be used for recertification notification. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a template.

Name

Identifies the notification template by name.

Subject

Identifies the subject of the notification template.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

Related information

For more information, see the [IBM Knowledge Center](#).

Create Recertification E-mail

Use this page to create an e-mail notification template.

Template name

Provides the name of the notification template.

Subject

Provides the subject of the e-mail that is generated, using the template.

Plaintext body

Provide the main content of the notification message, in plaintext format. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Provide the XHTML body of the notification message. The content in this section can include images and hyperlinks.

Related information

For more information, see the [IBM Knowledge Center](#).

Rejection E-mail

Use this page to specify the e-mail template that provides rejection notices to participants.

Rejection E-mail table

Lists the templates that can be used for notification of rejected recertification. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a template.

Name

Identifies the notification template by name.

Subject

Identifies the subject of the notification template.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

Related information

For more information, see the [IBM Knowledge Center](#).

Create Rejection E-mail

Use this page to create an e-mail notification template.

Template name

Provides the name of the notification template.

Subject

Provides the subject of the e-mail that is generated, using the template.

Plaintext body

Provide the main content of the notification message, in plaintext format. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Provide the XHTML body of the notification message. The content in this section can include images and hyperlinks.

Related information

For more information, see the [IBM Knowledge Center](#).

View Default Notice

Use this page to view the details that are related to the default e-mail notification.

Template name

Provides the name of the notification template.

Subject

Provides the subject of the e-mail that is generated, using the template.

Plaintext body

Provide the main content of the notification message, in plaintext format. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Provide the XHTML body of the notification message. The content in this section can include images and hyperlinks.

Related information

For more information, see the [IBM Knowledge Center](#).

User Recertification Pages

User recertification policies combine accounts, group membership, and role membership recertification activities belonging to a user into a single activity. Use these pages to specify information about a user recertification policy.

Related information

For more information, see the [IBM Knowledge Center](#).

User Target

Use this page to specify the type of user to which this policy applies. This notebook page is available only for a user recertification policy.

Type of users to which the policy applies

Select a type of user within the organization, such as a person or business partner person.

Related information

For more information, see the [IBM Knowledge Center](#).

Resource Target

Use this page to specify the resources to which this policy applies. This notebook page is only available for a user recertification policy.

Recertify membership for the following roles

Select the roles to which you want the user recertification to apply.

All

Select this option to recertify all roles for the users being recertified.

None

Select this option if you do not want to recertify roles for the users being recertified.

Specified roles

Select this option to specify one or more roles for the users being recertified in a subsequent step.

Recertify the following accounts

Select the accounts to which you want the user recertification to apply. The following options are available:

All

Select this option to recertify all accounts for the users being recertified.

None

Select this option if you do not want to recertify accounts for the users being recertified.

Accounts on specified services

Select this option to specify one or more services in a subsequent step. The recertification applies to all accounts on the services you select for the users being recertified.

Recertify the following groups

Select the groups to which you want the user recertification to apply. The following options are available:

All

Select this option to recertify all groups for the users being recertified.

All groups on specified accounts

Select this option if you want to recertify all groups for the users being recertified.

None

Select this option if you do not want to recertify groups for the users being recertified.

Specified groups

Select this option to specify one or more groups for the users being recertified in a subsequent step.

Related information

For more information, see the [IBM Knowledge Center](#).

Role Target

Use this page to specify the list of roles to which this policy applies. This notebook page is only available for a user recertification policy when you choose to select specified roles.

Roles table

Lists the static organizational roles. You can add one or more static organizational roles that you want the policy to apply to. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Role Name

Identifies the name of the role.

Role Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

You can use these buttons:

Add

Click to add a role to the list. A search panel opens from which you can select the appropriate roles.

Remove

Click to remove one or more roles from the list.

Related information

For more information, see the [IBM Knowledge Center](#).

Account Target

Use this page to specify services for the recertification policy. The policy applies to all accounts on the services you specify for any users that are included in this policy. This notebook page is only available for a user recertification policy when you choose to select accounts on specified services.

Accounts table

Lists the services. You can add one or more services to the table. The policy applies to all accounts on the services you select for any users included in the policy. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box adjacent to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service.

Description

Provides a brief description of the service.

Business Unit

Identifies the business unit associated with the service. Click the link to view business unit details.

You can use these buttons:

Add

Click to add a service to the list. A search panel opens from which you can select the appropriate services.

Remove

Click to remove one or more services from the list.

Related information

For more information, see the [IBM Knowledge Center](#).

Group Target

Use this page to specify the groups for which this recertification policy applies. This notebook page is available only for a user recertification policy when you choose to select specified groups.

Groups table

Lists the groups matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box next to the group. To select all groups, select the check box at the top of the column.

Group Name

Displays the name of the group.

Description

Displays information about the intended purpose of the group.

Service Name

Identifies the service associated with the group. Click the name of the service to view details about the service.

You can use these buttons:

Add

Click to add a group to the list. A search panel opens from which you can select the appropriate groups.

Remove

Click to remove one or more groups from the list.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule

Use this page to schedule when recertification occurs, either on a specific date and time on the calendar, or at a specified interval.

Schedule type

Select whether recertification occurs on a given day, or after an interval of time since the last recertification.

Calendar

Run recertification on a specific date and time.

Rolling

Recertify targets that have not been recertified within a specified time interval. This field only appears for an account or user recertification. If you select **Rolling**, you must also type the number of days for the time interval in the **Rolling interval in days** field.

Evaluation frequency

Select one of these schedule intervals to run recertification:

Daily

Recertifies targets every day. After you select this option, click the clock icon to specify a time in the **At this time** field.

Weekly

Recertifies targets once a week. After you select this option, select a day from the list in the **On this day of the week** field. Then, click the clock icon to specify a time in the **At this time** field.

Monthly

Recertifies targets once a month. After you select this option, select a date from the list in the **On this day of the month** field. Then, click the clock icon to specify a time in the **At this time** field.

Hourly

Recertifies targets every hour. After you select this option, select a time from the list in the **At this minute** field.

Annually

Recertifies targets on a specific day of the year that you specify. After you select this option, select a month from the list in the **Month** and a date from the list in the **On this day of the month** field. Then, click the clock icon to specify a time in the **At this time** field.

During a specific month

Recertifies targets on a month that you specify. After you select this option, select a month from the list in the **Month** and a day of the week from the list in the **On this day of the week** field. Then, click the clock icon to specify a time in the **At this time** field.

Quarterly

Recertifies targets on a specific day of the quarter that you specify. After you select this option, select a day from the list in the **On this day** field. Then, click the clock icon to specify a time in the **At this time** field.

Semi-Annually

Recertifies targets on a specific day of the half year that you specify. After you select this option, select a day from the list in the **On this day** field. Then, click the clock icon to specify a time in the **At this time** field.

Related information

For more information, see the [IBM Knowledge Center](#).

Policy (User Target)

Use this page to specify who approves a user recertification, who receives notification, and other actions.

Configuration mode

Select whether approval is based on the specified fields, or to use the workflow designer to configure approval.

Simple

Use these fields to specify the policy:

Who approves recertification

Specifies a participant who receives notification and an activity item when recertification is due. If you select **Specified user**, **Specified organizational role** or **Specified group**, an additional field is displayed for you to search for and specify a specific user, role, or group that is not in the list. Ensure that the approvers you select have access to the View Activities task.

Action when recertification is rejected

Specifies an action that occurs when the recertification is rejected.

Suspend accounts and mark others

Suspends all accounts associated with the user and marks other resources as rejected for recertification.

Remove

Removes all accounts and other resources associated with the user.

Mark as rejected for recertification

Marks all accounts and other resources as rejected for recertification.

Send rejection e-mail to

Specifies a recipient, such as a manager, who is notified when recertification is declined.

Days until recertification is due

Specifies a value for the number of days that the participant has to respond to the recertification request. If the participant does not respond to the recertification request in the specified time, the recertification is overdue and an overdue action can be taken.

Action when recertification is overdue

Specifies an action, such as reject all or approve all, that occurs when the recertification participant does not respond to the recertification request in the specified time. If you select **Take no action**, the activity will remain as an overdue activity after the due date has passed.

Advanced

Use the workflow designer to configure who approves recertification, who receives notification, and other actions for the recertification policy. Policy definitions that you create in the workflow designer cannot later be modified using the simple method.

Workflows can be as simple as requiring only one approval, or they can be as complex as requiring multiple approvals with RFIs, loops, and so on. Manual activities that are defined in the workflow populate an individual participant's To Do list as each process in the workflow is completed. At any point, the system administrator can view any user's To Do list and act as the Participant, overriding the approval authority.

To define a workflow, drag the design nodes from the node palette onto the workflow design space, and then connect them with transition lines.

After you place a design node on the workflow design space, double-click the node to configure its properties.

Workflow design interface

The workflow designer has these areas:

Workflow Name

Displays the name of the workflow.

Service Type

Displays the name of the service type.

Node palette

Displays all available nodes in the left pane of the interface.

Design space

Displays the nodes that you are working with in the large pane of the interface.

High Contrast

Select this check box to display the workflow design interface without color representing the design nodes.

Properties

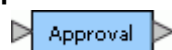
Click this button to view configurable properties of the workflow node.

Update

Click this button to refresh the view of the workflow design space.

Workflow design nodes

The following workflow design nodes are available:

Approval

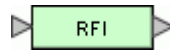
Use this node to define the person who must approve a request or activity before workflow processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Mail



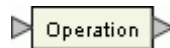
Use this node to configure e-mail notification.

RFI



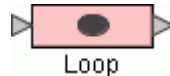
Use this node to request information from a person. For example, you might need a manager to provide contact information for a new employee before the process of issuing the employee an e-mail account can complete. The person must respond with the information before workflow processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Operation



Use this node to initiate an operation workflow that has been defined previously. This workflow can be initiated at any point during the primary workflow.

Loop



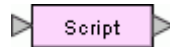
Use this node to repeat a specified activity while or until a specified condition is met.

Extension



Use this node to specify a workflow extension to manage people and accounts.

Script



Use this node to specify a JavaScript script that the runs when processing the workflow activities.

Work Order



Use this node to e-mail a request notification for a manual activity. For example, you might use this node in a workflow to request an ID badge for a new employee. Work order participants are not required to have a IBM Security Identity Manager account. They must, however, have an e-mail address that is stored in the IBM Security Identity Manager directory server.

The **Continue on Participant Resolution Failure** option controls whether a workflow process continues if participant resolution fails.

Packaged Approval



Use this node to evaluate roles and entitlements together. Packaged approval activity supports output parameters so that the decisions can be used in the remainder of the workflow. You can also define an interval of time in which the person must respond to the request before it is escalated. You can also use the No-timeout option, which will cause the To Do item to remain in the Participant's To Do activity list if the Participant does not take any action after the timeout period.

Related information

For more information, see the [IBM Knowledge Center](#).

Recertification E-mail

Use this page to specify the e-mail template that provides recertification notices to participants.

Recertification E-mail table

Lists the templates that can be used for recertification notification. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a template.

Name

Identifies the notification template by name.

Subject

Identifies the subject of the notification template.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

Related information

For more information, see the [IBM Knowledge Center](#).

Create Recertification E-mail

Use this page to create an e-mail notification template.

Template name

Provides the name of the notification template.

Subject

Provides the subject of the e-mail that is generated, using the template.

Plaintext body

Provide the main content of the notification message, in plaintext format. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Provide the XHTML body of the notification message. The content in this section can include images and hyperlinks.

Related information

For more information, see the [IBM Knowledge Center](#).

Rejection E-mail

Use this page to specify the e-mail template that provides rejection notices to participants.

Rejection E-mail table

Lists the templates that can be used for notification of rejected recertification. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a template.

Name

Identifies the notification template by name.

Subject

Identifies the subject of the notification template.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

Related information

[For more information, see the IBM Knowledge Center.](#)

Create Rejection E-mail

Use this page to create an e-mail notification template.

Template name

Provides the name of the notification template.

Subject

Provides the subject of the e-mail that is generated, using the template.

Plaintext body

Provide the main content of the notification message, in plaintext format. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Provide the XHTML body of the notification message. The content in this section can include images and hyperlinks.

Related information

[For more information, see the IBM Knowledge Center.](#)

View Default Notice

Use this page to view the details that are related to the default e-mail notification.

Template name

Provides the name of the notification template.

Subject

Provides the subject of the e-mail that is generated, using the template.

Plaintext body

Provide the main content of the notification message, in plaintext format. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Provide the XHTML body of the notification message. The content in this section can include images and hyperlinks.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Roles

Use this page to find and add roles that you want to recertify membership on.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Role name or description searches for a role with a name or description that contains text that is entered in the **Search information** field.

Business unit searches for a role associated with a business unit that contains text that is entered in the **Search information** field.

Roles table

Lists the roles matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Name

Identifies the name of the role.

Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Groups

Use this page to search for and select groups for recertification for the service you specified.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Group name or description searches for groups with a name or description that contains text that is entered in the **Search information** field.

Business unit searches for business units in which the business unit name contains the text that is entered in the **Search information** field.

Groups table

Lists the groups matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box next to the group. To select all groups, select the check box at the top of the column.

Group Name

Displays name group's name. Click the name of the group to view group details.

Description

Displays information about the intended purpose of the group.

Access Name

Identifies the name of the access for the group, if an access has been created for the group.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Groups

Use this page to search for and select groups for recertification for the service you specified.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Group name or description searches for groups with a name or description that contains text that is entered in the **Search information** field.

Business unit searches for business units in which the business unit name contains the text that is entered in the **Search information** field.

Groups table

Lists the groups matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box next to the group. To select all groups, select the check box at the top of the column.

Group Name

Identifies the group's name. Click the name of the group to view group details.

Description

Displays information about the intended purpose of the group.

View

Identifies the view of tasks that users have in this group.

Business Unit

Identifies the business unit in which the group is specified. Click the name of the business unit to view business unit details.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a Service

Use this page to find the service for the groups that you want to recertify.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Service searches for service names that contain the text that is entered in the **Search information** field.

Business unit searches for business units in which the business unit name contains the text that is entered in the **Search information** field.

Service type

Select a service type from the list.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Services table

Lists the services matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box adjacent to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view the service details.

Description

Provides information about the intended purpose of the service.

Service Type

Identifies the type of service.

Business Unit

Identifies the business unit associated with the service. Click the name of the business unit to view business unit details.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a Service

Use this page to find the service that you want.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Service searches for service names that contain the text that is entered in the **Search information** field.

Business unit searches for business units in which the business unit name contains the text that is entered in the **Search information** field.

Service type

Select a service type from the list.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Services table

Lists the services that match the search criteria that you specified. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box next to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view the service details.

Description

Identifies a brief description of the service.

Service Type

Identifies the type of service.

Business Unit

Identifies the business unit associated with the service.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Accesses

Use this page to find the accesses to associate with a recertification policy.

Access information

Select an access type from the list. The contents of the list are defined by the system administrator.

The search is based on the access type that you select from the list. The list items might vary, depending on which access type you selected from the **Access type** list. For example, if you select **Application**, a new list with its dependent access types is displayed. Similarly, if you select **All**, no new list is displayed.

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Access type

Select an access type from the list. Select **All** to display all of the accesses dependent on an access type and click **Search**.

Accesses table

Lists the accesses matching the specified criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an access. To select one or more accesses, select the check box next to the access. To select all accesses, select the check box at the top of the column.

Access Name

Identifies the name of the access. Click the name of the access to view the access details.

Service Name

Identifies the name of the service where the access is defined. Click the name of the service to view the service details.

Access Type

Identifies the type of access, and consists of these types:

- Application
- AccessRole
- MailGroup
- SharedFolder
- A custom-defined access type

The column displays the access type hierarchy in a colon-separated string format. For example, Application:ERP Application:Supplier or AccessRole:Manager:Finance.

Access Description

Provides additional information about the access.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Manage Recertification Policies

Use this notebook to modify details related to a recertification policy. The notebook tabs depend on the recertification target type you have selected.

Related information

For more information, see the [IBM Knowledge Center](#).

User Recertification Pages

User recertification policies combine accounts, group membership, and role membership recertification activities belonging to a user into a single activity. Use these pages to specify information about a user recertification policy.

General

Use this page to specify general information about a recertification policy.

Name

Provides the name of the recertification policy. You must specify a name for the recertification policy.

Description

Provides information about the intended purpose of the recertification policy.

Policy status

Click **Enabled** to use the recertification policy and make it active, or click **Disabled** to make the policy inactive.

Business unit

Displays the name of the business unit associated with the policy.

Scope of this policy in relation to its business unit

Select the range within the business unit you have selected for this policy.

Apply this policy to the business unit and subunits

Applies the policy to the business unit and any subunits.

Apply this policy only to the business unit

Applies the policy only to the business unit. The policy does not apply to any resources in subunits of the business unit.

Policy recertifies

View the type of recertification policy.

Accesses

Applies to access entitlements.

Accounts

Applies to services that provide access to accounts.

Users

Applies to all the roles, accounts and groups belonging to a user.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

User Target

Use this page to specify the type of user to which this policy applies. This notebook page is only available for a user recertification policy.

Type of users to which the policy applies

Select a type of user within the organization, such as a person or business partner person.

Related information

For more information, see the [IBM Knowledge Center](#).

Role Target

Use this page to modify the list of roles to which this policy applies. This notebook page is only available for a user recertification.

Recertify membership for the following roles

Choose the roles to which you want the user recertification to apply.

All

Select this option to recertify all roles for the users being recertified.

None

Select this option if you do not want to recertify roles for the users being recertified.

Specified roles

Select this option to specify one or more roles for the users being recertified.

Roles table

When you select **Specified roles**, the **Roles** table is displayed. You can specify which static organizational roles you want the policy to apply to. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Role Name

Identifies the name of the role.

Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a role to the list. A search panel opens from which you can select the appropriate roles.

Remove

Click to remove one or more roles from the list.

Related information

For more information, see the [IBM Knowledge Center](#).

Account Target

Use this page to specify services for the recertification policy. The policy applies to all accounts on the services you specify for any users that are included in this policy. This notebook page is only available for a user recertification policy.

Recertify the following accounts

Choose the accounts to which you want the user recertification to apply:

All

Select this option to recertify all accounts for the users being recertified.

None

Select this option if you do not want to recertify accounts for the users being recertified.

Accounts on specified services

Select this option to specify one or more services. The recertification applies to all accounts owned on the services you select for the users being recertified .

Accounts table

When you select **Accounts on specified services**, the **Accounts** table is displayed. You can add or remove one or more services. The policy applies to all accounts on the services you select for any users included in the policy. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box adjacent to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view details about the service.

Description

Provides information about the service.

Business Unit

Identifies the business unit associated with the service. Click the link to view business unit details.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a service to the list. A search panel opens from which you can select the appropriate services.

Remove

Click to remove one or more services from the list.

Related information

For more information, see the [IBM Knowledge Center](#).

Group Target

Use this page to modify the groups for which this recertification policy applies. This notebook page is only available for a user recertification policy.

Recertify the following groups

Choose the groups to which you want the user recertification to apply.

All

Select this option to recertify all groups for the users being recertified.

All groups on specified accounts

Select this option if you want to recertify all groups for the accounts you specify on the Account Target page.

None

Select this option if you do not want to recertify groups for the users being recertified.

Specified groups

Select this option to specify one or more groups for the users being recertified.

Groups table

When you select **Specified groups**, the **Groups** table is displayed. You can specify which groups you want the policy to apply to. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box next to the group. To select all groups, select the check box at the top of the column.

Group Name

Displays the name of the group.

Description

Displays information about the intended purpose of the group.

Service Name

Identifies the service associated with the group. Click the name of the service to view details about the service.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a group to the list. A search panel opens from which you can select the appropriate groups.

Remove

Click to remove one or more groups from the list.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule

Use this page to schedule when recertification occurs, either on a specific date and time on the calendar, or at a specific interval.

Schedule type

Select whether recertification occurs on a given day, or after an interval of time since the last recertification.

Calendar

Run recertification on a specific date and time.

Rolling

Recertify targets that have not been recertified within a specified time interval. This field only appears for an account or user recertification. If you select **Rolling**, you must also type the number of days for the time interval in the **Rolling interval in days** field.

Evaluation frequency

Select one of these schedule intervals to run recertification:

Daily

Recertifies targets every day. After you select this option, click the clock icon to specify a time in the **At this time** field.

Weekly

Recertifies targets once a week. After you select this option, select a day from the list in the **On this day of the week** field. Then, click the clock icon to specify a time in the **At this time** field.

Monthly

Recertifies targets once a month. After you select this option, select a date from the list in the **On this day of the month** field. Then, click the clock icon to specify a time in the **At this time** field.

Hourly

Recertifies targets every hour. After you select this option, select a time from the list in the **At this minute** field.

Annually

Recertifies targets on a specific day of the year that you specify. After you select this option, select a month from the list in the **Month** and a date from the list in the **On this day of the month** field. Then, click the clock icon to specify a time in the **At this time** field.

During a specific month

Recertifies targets on a month that you specify. After you select this option, select a month from the list in the **Month** and a day of the week from the list in the **On this day of the week** field. Then, click the clock icon to specify a time in the **At this time** field.

Quarterly

Recertifies targets on a specific day of the quarter that you specify. After you select this option, select a day from the list in the **On this day** field. Then, click the clock icon to specify a time in the **At this time** field.

Semi-Annually

Recertifies targets on a specific day of the half year that you specify. After you select this option, select a day from the list in the **On this day** field. Then, click the clock icon to specify a time in the **At this time** field.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Policy

Use this page to specify who approves a user recertification, who receives notification, and other actions.

Configuration mode

Select whether approval is based on the specified fields, or to use the workflow designer to configure approval.

Simple

Use these fields to specify the policy:

Who approves recertification

Specifies a participant who receives notification and an activity item when recertification is due. If you select **Specified user**, **Specified organizational role** or **Specified group**, an additional field is displayed for you to search for and specify a specific user, role, or group that is not in the list. Ensure that the approvers you select have access to the View Activities task.

Action when recertification is rejected

Specifies an action that occurs when the recertification is rejected.

Suspend accounts and mark others

Suspends all accounts associated with the user and marks other resources as rejected for recertification.

Remove

Removes all accounts and other resources associated with the user.

Mark as rejected for recertification

Marks all accounts and other resources as rejected for recertification.

Send rejection e-mail to

Specifies a recipient, such as a manager, who is notified when recertification is declined.

Days until recertification is due

Specifies a value for the number of days that the participant has to respond to the recertification request. If the participant does not respond to the recertification request in the specified time, the recertification is overdue and an overdue action can be taken.

Action when recertification is overdue

Specifies an action, such as reject all or approve all, that occurs when the recertification participant does not respond to the recertification request in the specified time. If you select **Take no action**, the activity will remain as an overdue activity after the due date has passed.

Advanced

Use the workflow designer to configure who approves recertification, who receives notification, and other actions for the recertification policy. Policy definitions that you create in the workflow designer cannot later be modified using the simple method.

Workflows can be as simple as requiring only one approval, or they can be as complex as requiring multiple approvals with RFIs, loops, and so on. Manual activities that are defined in the workflow populate an individual participant's To Do list as each process in the workflow is completed. At any point, the system administrator can view any user's To Do list and act as the Participant, overriding the approval authority.

To define a workflow, drag the design nodes from the node palette onto the workflow design space, and then connect them with transition lines.

After you place a design node on the workflow design space, double-click the node to configure its properties.

Workflow design interface

The workflow designer has these areas:

Workflow Name

Displays the name of the workflow.

Service Type

Displays the name of the service type.

Node palette

Displays all available nodes in the left pane of the interface.

Design space

Displays the nodes that you are working with in the large pane of the interface.

High Contrast

Select this check box to display the workflow design interface without color representing the design nodes.

Properties

Click this button to view configurable properties of the workflow node.

Update

Click this button to refresh the view of the workflow design space.

Workflow design nodes

The following workflow design nodes are available:

Approval



Use this node to define the person who must approve a request or activity before workflow processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Mail



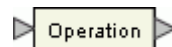
Use this node to configure e-mail notification.

RFI



Use this node to request information from a person. For example, you might need a manager to provide contact information for a new employee before the process of issuing the employee an e-mail account can complete. The person must respond with the information before workflow processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Operation



Use this node to initiate an operation workflow that has been defined previously. This workflow can be initiated at any point during the primary workflow.

Loop



Loop

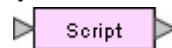
Use this node to repeat a specified activity while or until a specified condition is met.

Extension



Use this node to specify a workflow extension to manage people and accounts.

Script



Use this node to specify a JavaScript script that the runs when processing the workflow activities.

Work Order



Use this node to e-mail a request notification for a manual activity. For example, you might use this node in a workflow to request an ID badge for a new employee. Work order participants are not required to have an IBM Security Identity Manager account. They must, however, have an e-mail address that is stored in the IBM Security Identity Manager directory server.

The **Continue on Participant Resolution Failure** option controls whether a workflow process continues if participant resolution fails.

Packaged Approval



Use this node to evaluate roles and entitlements together. Packaged approval activity supports output parameters so that the decisions can be used in the remainder of the workflow. You can also define an interval of time in which the person must respond to the request before it is escalated. You can also use the No-timeout option, which will cause

the To Do item to remain in the Participant's To Do activity list if the Participant does not take any action after the timeout period.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Recertification E-mail

Use this page to modify the e-mail template that provides recertification notices to participants.

Recertification E-mail table

Lists the templates that can be used for recertification notification. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a template.

Name

Identifies the notification template by name.

Subject

Identifies the subject of the notification template.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

Related information

For more information, see the [IBM Knowledge Center](#).

Rejection E-mail

Use this page to modify the e-mail template that provides rejection notices to participants.

Rejection E-mail table

Lists the templates that can be used for notification of rejected recertification. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a template.

Name

Identifies the notification template by name.

Subject

Identifies the subject of the notification template.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

Related information

For more information, see the [IBM Knowledge Center](#).

Account Recertification Pages

Use these pages to specify information about an account recertification.

General

Use this page to specify general information about a recertification policy.

Name

Provides the name of the recertification policy. You must specify a name for the recertification policy.

Description

Provides information about the intended purpose of the recertification policy.

Policy status

Click **Enabled** to use the recertification policy and make it active, or click **Disabled** to make the policy inactive.

Business unit

Displays the name of the business unit associated with the policy.

Scope of this policy in relation to its business unit

Select the range within the business unit you have selected for this policy.

Apply this policy to the business unit and subunits

Applies the policy to the business unit and any subunits.

Apply this policy only to the business unit

Applies the policy only to the business unit. The policy does not apply to any resources in subunits of the business unit.

Policy recertifies

View the type of recertification policy.

Accesses

Applies to access entitlements.

Accounts

Applies to services that provide access to accounts.

Users

Applies to all the roles, accounts and groups belonging to a user.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Service Target

Use this page to add or remove services to which the recertification policy applies. You must specify at least one service for the recertification policy. You cannot associate more than one recertification policy with a service. This notebook page is only available for an account recertification.

Services table

Lists the services to which the recertification policy applies. You can only view and select services under the business unit of the policy. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box adjacent to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view the service details.

Description

Provides information about the intended purpose of the service.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a service.

Remove

Click to remove one or more selected services.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule

Use this page to schedule when recertification occurs, either on a specific date and time on the calendar, or at a specific interval.

Schedule type

Select whether recertification occurs on a given day, or after an interval of time since the last recertification.

Calendar

Run recertification on a specific date and time.

Rolling

Recertify targets that have not been recertified within a specified time interval. This field only appears for an account or user recertification. If you select **Rolling**, you must also type the number of days for the time interval in the **Rolling interval in days** field.

Evaluation frequency

Select one of these schedule intervals to run recertification:

Daily

Recertifies targets every day. After you select this option, click the clock icon to specify a time in the **At this time** field.

Weekly

Recertifies targets once a week. After you select this option, select a day from the list in the **On this day of the week** field. Then, click the clock icon to specify a time in the **At this time** field.

Monthly

Recertifies targets once a month. After you select this option, select a date from the list in the **On this day of the month** field. Then, click the clock icon to specify a time in the **At this time** field.

Hourly

Recertifies targets every hour. After you select this option, select a time from the list in the **At this minute** field.

Annually

Recertifies targets on a specific day of the year that you specify. After you select this option, select a month from the list in the **Month** and a date from the list in the **On this day of the month** field. Then, click the clock icon to specify a time in the **At this time** field.

During a specific month

Recertifies targets on a month that you specify. After you select this option, select a month from the list in the **Month** and a day of the week from the list in the **On this day of the week** field. Then, click the clock icon to specify a time in the **At this time** field.

Quarterly

Recertifies targets on a specific day of the quarter that you specify. After you select this option, select a day from the list in the **On this day** field. Then, click the clock icon to specify a time in the **At this time** field.

Semi-Annually

Recertifies targets on a specific day of the half year that you specify. After you select this option, select a day from the list in the **On this day** field. Then, click the clock icon to specify a time in the **At this time** field.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Policy

Use this page to specify who approves an account or access recertification, who receives notification, and other actions.

Configuration mode

Select whether approval is based on the specified fields, or to use the workflow designer to configure approval.

Simple

Use these fields to specify the policy:

Who approves recertification

Specifies a participant who receives notification and an activity item when recertification is due. If you select **Specified user**, **Specified organizational role** or **Specified group**, an additional field is displayed for you to search for and specify a specific user, role, or group that is not in the list. Ensure that the approvers you select have access to the View Activities task.

Action when recertification is rejected

Specifies an action, such as suspend or delete, that occurs when a participant declines to recertify an account.

Send rejection e-mail to

Specifies a recipient, such as a manager, who is notified when recertification is declined.

Days until recertification is due

Specifies a value for the number of days that the participant has to respond to the recertification request. If the participant does not respond to the recertification request in the specified time, the recertification is overdue and an overdue action can be taken.

Action when recertification is overdue

Specifies an action, such as reject or approve, that occurs when the recertification participant does not respond to the recertification request in the specified time. If you select **Take no action**, the activity remains as an overdue activity after the due date has passed.

User type

Specifies the scope of the recertification policy to only apply to people of a certain type on the given policy schedule.

Advanced

Use the workflow designer to configure who approves recertification, who receives notification, and other actions for the recertification policy. Policy definitions that you create in the workflow designer cannot later be modified using the simple method.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Recertification E-mail

Use this page to modify the e-mail template that provides recertification notices to participants.

Recertification E-mail table

Lists the templates that can be used for recertification notification. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a template.

Name

Identifies the notification template by name.

Subject

Identifies the subject of the notification template.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

Related information

For more information, see the [IBM Knowledge Center](#).

Rejection E-mail

Use this page to modify the e-mail template that provides rejection notices to participants.

Rejection E-mail table

Lists the templates that can be used for notification of rejected recertification. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a template.

Name

Identifies the notification template by name.

Subject

Identifies the subject of the notification template.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Recertification Pages

Use these pages to specify information about an access recertification.

General

Use this page to specify general information about a recertification policy.

Name

Provides the name of the recertification policy. You must specify a name for the recertification policy.

Description

Provides information about the intended purpose of the recertification policy.

Policy status

Click **Enabled** to use the recertification policy and make it active, or click **Disabled** to make the policy inactive.

Business unit

Displays the name of the business unit associated with the policy.

Scope of this policy in relation to its business unit

Select the range within the business unit you have selected for this policy.

Apply this policy to the business unit and subunits

Applies the policy to the business unit and any subunits.

Apply this policy only to the business unit

Applies the policy only to the business unit. The policy does not apply to any resources in subunits of the business unit.

Policy recertifies

View the type of recertification policy.

Accesses

Applies to access entitlements.

Accounts

Applies to services that provide access to accounts.

Users

Applies to all the roles, accounts and groups belonging to a user.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Target

Use this page to add or remove access targets to which the recertification policy applies. You must specify at least one access for the recertification policy. You cannot associate more than one recertification policy with an access. This notebook page only is displayed for an access recertification.

Access Target table

Lists the access targets to which the recertification policy applies. You can only view and select accesses under the business unit of the policy. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an access. To select one or more accesses, select the check box adjacent to the access. To select all accesses, select the check box at the top of the column.

Access Name

Identifies the name of the access. Click the name of the access to view the access details.

Description

Provides information about the intended purpose of the access.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add an access.

Remove

Click to remove one or more selected accesses.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule

Use this page to schedule when recertification occurs, either on a specific date and time on the calendar, or at a specific interval.

Schedule type

Select whether recertification occurs on a given day, or after an interval of time since the last recertification.

Calendar

Run recertification on a specific date and time.

Rolling

Recertify targets that have not been recertified within a specified time interval. This field only appears for an account or user recertification. If you select **Rolling**, you must also type the number of days for the time interval in the **Rolling interval in days** field.

Evaluation frequency

Select one of these schedule intervals to run recertification:

Daily

Recertifies targets every day. After you select this option, click the clock icon to specify a time in the **At this time** field.

Weekly

Recertifies targets once a week. After you select this option, select a day from the list in the **On this day of the week** field. Then, click the clock icon to specify a time in the **At this time** field.

Monthly

Recertifies targets once a month. After you select this option, select a date from the list in the **On this day of the month** field. Then, click the clock icon to specify a time in the **At this time** field.

Hourly

Recertifies targets every hour. After you select this option, select a time from the list in the **At this minute** field.

Annually

Recertifies targets on a specific day of the year that you specify. After you select this option, select a month from the list in the **Month** and a date from the list in the **On this day of the month** field. Then, click the clock icon to specify a time in the **At this time** field.

During a specific month

Recertifies targets on a month that you specify. After you select this option, select a month from the list in the **Month** and a day of the week from the list in the **On this day of the week** field. Then, click the clock icon to specify a time in the **At this time** field.

Quarterly

Recertifies targets on a specific day of the quarter that you specify. After you select this option, select a day from the list in the **On this day** field. Then, click the clock icon to specify a time in the **At this time** field.

Semi-Annually

Recertifies targets on a specific day of the half year that you specify. After you select this option, select a day from the list in the **On this day** field. Then, click the clock icon to specify a time in the **At this time** field.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Policy

Use this page to specify who approves an account or access recertification, who receives notification, and other actions.

Configuration mode

Select whether approval is based on the specified fields, or to use the workflow designer to configure approval.

Simple

Use these fields to specify the policy:

Who approves recertification

Specifies a participant who receives notification and an activity item when recertification is due. If you select **Specified user**, **Specified organizational role** or **Specified group**, an additional field is displayed for you to search for and specify a specific user, role, or group that is not in the list. Ensure that the approvers you select have access to the View Activities task.

Action when recertification is rejected

Specifies an action, such as suspend or delete, that occurs when a participant declines to recertify an account.

Send rejection e-mail to

Specifies a recipient, such as a manager, who is notified when recertification is declined.

Days until recertification is due

Specifies a value for the number of days that the participant has to respond to the recertification request. If the participant does not respond to the recertification request in the specified time, the recertification is overdue and an overdue action can be taken.

Action when recertification is overdue

Specifies an action, such as reject or approve, that occurs when the recertification participant does not respond to the recertification request in the specified time. If you select **Take no action**, the activity remains as an overdue activity after the due date has passed.

User type

Specifies the scope of the recertification policy to only apply to people of a certain type on the given policy schedule.

Advanced

Use the workflow designer to configure who approves recertification, who receives notification, and other actions for the recertification policy. Policy definitions that you create in the workflow designer cannot later be modified using the simple method.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Recertification E-mail

Use this page to modify the e-mail template that provides recertification notices to participants.

Recertification E-mail table

Lists the templates that can be used for recertification notification. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a template.

Name

Identifies the notification template by name.

Subject

Identifies the subject of the notification template.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

Related information

For more information, see the [IBM Knowledge Center](#).

Rejection E-mail

Use this page to modify the e-mail template that provides rejection notices to participants.

Rejection E-mail table

Lists the templates that can be used for notification of rejected recertification. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a template.

Name

Identifies the notification template by name.

Subject

Identifies the subject of the notification template.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

Related information

For more information, see the [IBM Knowledge Center](#).

Policy Recertification Pages

Use these pages to specify information about a policy recertification.

General

Use this page to specify general information about a recertification policy.

Name

Provides the name of the recertification policy. You must specify a name for the recertification policy.

Description

Provides information about the intended purpose of the recertification policy.

Policy status

Click **Enabled** to use the recertification policy and make it active, or click **Disabled** to make the policy inactive.

Business unit

Displays the name of the business unit associated with the policy.

Scope of this policy in relation to its business unit

Select the range within the business unit you have selected for this policy.

Apply this policy to the business unit and subunits

Applies the policy to the business unit and any subunits.

Apply this policy only to the business unit

Applies the policy only to the business unit. The policy does not apply to any resources in subunits of the business unit.

Policy recertifies

View the type of recertification policy.

Accesses

Applies to access entitlements.

Accounts

Applies to services that provide access to accounts.

Users

Applies to all the roles, accounts and groups belonging to a user.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Policy Target

Use this page to specify the filter for separation of duty policies, role designs, or provisioning policies that need to be recertified.

Select the type of policy target that need to be recertified.

All separation of duty policies

Applies to all the separation of duty policies.

All role designs

Applies to all role designs.

All provisioning policies

Applies to all provisioning policies.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule

Use this page to schedule when recertification occurs, either on a specific date and time on the calendar, or at a specific interval.

Schedule type

Select whether recertification occurs on a given day, or after an interval of time since the last recertification.

Calendar

Run recertification on a specific date and time.

Rolling

Recertify targets that have not been recertified within a specified time interval. This field only appears for an account or user recertification. If you select **Rolling**, you must also type the number of days for the time interval in the **Rolling interval in days** field.

Evaluation frequency

Select one of these schedule intervals to run recertification:

Daily

Recertifies targets every day. After you select this option, click the clock icon to specify a time in the **At this time** field.

Weekly

Recertifies targets once a week. After you select this option, select a day from the list in the **On this day of the week** field. Then, click the clock icon to specify a time in the **At this time** field.

Monthly

Recertifies targets once a month. After you select this option, select a date from the list in the **On this day of the month** field. Then, click the clock icon to specify a time in the **At this time** field.

Hourly

Recertifies targets every hour. After you select this option, select a time from the list in the **At this minute** field.

Annually

Recertifies targets on a specific day of the year that you specify. After you select this option, select a month from the list in the **Month** and a date from the list in the **On this day of the month** field. Then, click the clock icon to specify a time in the **At this time** field.

During a specific month

Recertifies targets on a month that you specify. After you select this option, select a month from the list in the **Month** and a day of the week from the list in the **On this day of the week** field. Then, click the clock icon to specify a time in the **At this time** field.

Quarterly

Recertifies targets on a specific day of the quarter that you specify. After you select this option, select a day from the list in the **On this day** field. Then, click the clock icon to specify a time in the **At this time** field.

Semi-Annually

Recertifies targets on a specific day of the half year that you specify. After you select this option, select a day from the list in the **On this day** field. Then, click the clock icon to specify a time in the **At this time** field.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Policy (Policy Target)

Use this page to specify who approves a recertification, who receives notification, and other actions.

Configuration mode

Select whether approval is based on the specified fields, or use the workflow designer to configure approval.

Simple

Use the fields below to specify the policy:

Who approves recertification

Specifies an approver who receives notification and a To-Do item when recertification is due. If you select **Specified user**, **Specified organizational role** or **Specified group**, an additional field is displayed for you to search for and select a specific user, role, or group that is not in the list. Ensure that the approvers you select are able to access the To-Do list.

Action when recertification is rejected

Specifies an action, such as suspend or delete, that occurs when an approver declines to recertify an account.

Send rejection e-mail to

Specifies a recipient, such as a manager, who is notified when recertification is declined. If you select **Specified user**, **Specified organizational role** or **Specified group**, an additional field is displayed for you to search for and select a specific user, role, or group that is not in the list.

Days until recertification is due

Specifies a value for the number of days that the approver has to respond to the recertification request. If the approver does not respond to the recertification request in the specified time, the recertification is overdue and an overdue action can be taken.

Action when recertification is overdue

Specifies an action, such as reject all or approve all, that occurs when the approver does not respond to the recertification request in the specified time. If you select **Take no action**, the activity remains as an overdue activity after the due date has passed.

If you select **Escalate**, the activity is displayed in the To-Do list of the escalation participant. The **Escalate** option displays a list of the following escalation participants:

Policy owner is the owner who owns the recertification policy.

Organizational role is a person who can have multiple roles in an organization.

Specified group is a particular group in an organization to which the escalation is made when recertification is overdue.

Specified user is a particular user to whom the escalation is made when recertification is overdue.

Manager of approver participants is the manager of the user or group who is recertifying the policy or role designs.

User type

Specifies the scope of the recertification policy to apply only to people of a certain type on the given policy schedule.

Related information

For more information, see the [IBM Knowledge Center](#).

Recertification E-mail

Use this page to modify the e-mail template that provides recertification notices to participants.

Recertification E-mail table

Lists the templates that can be used for recertification notification. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a template.

Name

Identifies the notification template by name.

Subject

Identifies the subject of the notification template.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

Related information

For more information, see the [IBM Knowledge Center](#).

Rejection E-mail

Use this page to modify the e-mail template that provides rejection notices to participants.

Rejection E-mail table

Lists the templates that can be used for notification of rejected recertification. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a template.

Name

Identifies the notification template by name.

Subject

Identifies the subject of the notification template.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

Related information

For more information, see the [IBM Knowledge Center](#).

Modify Recertification E-mail

Use this page to modify an e-mail notification template.

Template name

Provides the name of the notification template.

Subject

Provides the subject of the e-mail that is generated, using the template.

Plaintext body

Provide the main content of the notification message, in plaintext format. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Provide the XHTML body of the notification message. The content in this section can include images and hyperlinks.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a Service

Use this page to find the service that you want.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Service searches for service names that contain the text that is entered in the **Search information** field.

Business unit searches for business units in which the business unit name contains the text that is entered in the **Search information** field.

Service type

Select a service type from the list.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Services table

Lists the services that match the search criteria that you specified. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box next to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view the service details.

Description

Identifies a brief description of the service.

Service Type

Identifies the type of service.

Business Unit

Identifies the business unit associated with the service.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Accesses

Use this page to find the accesses to associate with a recertification policy.

Access information

Select an access type from the list. The contents of the list are defined by the system administrator.

The search is based on the access type that you select from the list. The list items might vary, depending on which access type you selected from the **Access type** list. For example, if you select **Application**, a new list with its dependent access types is displayed. Similarly, if you select **All**, no new list is displayed.

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Access type

Select an access type from the list. Select **All** to display all of the accesses dependent on an access type and click **Search**.

Accesses table

Lists the accesses matching the specified criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an access. To select one or more accesses, select the check box next to the access. To select all accesses, select the check box at the top of the column.

Access Name

Identifies the name of the access. Click the name of the access to view the access details.

Service Name

Identifies the name of the service where the access is defined. Click the name of the service to view the service details.

Access Type

Identifies the type of access, and consists of these types:

- Application
- AccessRole
- MailGroup
- SharedFolder
- A custom-defined access type

The column displays the access type hierarchy in a colon-separated string format. For example, `Application:ERP Application:Supplier` or `AccessRole:Manager:Finance`.

Access Description

Provides additional information about the access.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Design Workflow

Manage Account Request Workflows

Manage Account Request Workflows

Use this page to create, change, or delete account request workflows.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Workflow searches for workflow names or descriptions that contain the text that is entered in the **Search information** field.

Service searches for workflows that are referenced by provisioning policies for service instances matching the specified search criteria that is entered in the **Search information** field. Workflows that are not referenced by any provisioning policies are not displayed. Workflows that are referenced only by provisioning policies that specify a service type or all services are also not displayed.

Account Request Workflows table

Lists the account request workflows matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a workflow. To select one or more workflows, select the check box adjacent to the workflow. To select all workflows, select the check box at the top of the column.

Workflow Name

Identifies the name of the workflow. Click the name to view or change the workflow.

Description

Provides a brief description of the workflow.

Business Unit

Identifies the business unit that is associated with the workflow. Click the link for more information about the business unit.

Service Type

Identifies the name of the type of service to which the workflow applies. A value of ***All** means that the workflow applies to all service types. This column header changes dynamically, depending on the workflow type.

Service Names

Identifies the name of the service instances that are entitled by the workflow. This column header changes dynamically, depending on the workflow type.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Use these buttons:

Create

Click to create a new workflow.

Change

Click to change the selected workflow.

Delete

Click to delete one or more selected workflows. You cannot delete the default account request workflow, which is used by the default provisioning policies.

Related information

[For more information, see the IBM Knowledge Center.](#)

Manage Account Request Workflows

Use this notebook to specify details related to the account request workflows. Click each page to view general information and activities for the workflow. In advanced mode, you can use the workflow designer to specify a workflow.

Related information

[For more information, see the IBM Knowledge Center.](#)

General

Use this page to specify general information about a workflow. If you are viewing an existing workflow and you do not have access control item permission to change the workflow, the information on this page is displayed in read-only mode.

Name

Type a name to identify the workflow.

Description

Type a description of the intended purpose of the workflow.

Business unit

Indicates the business unit. Click **Search** to locate and select a business unit. This field is read-only when you are making a change to a workflow.

Service type

Select a service type from the list. This list includes all of the installed service types that do not represent an identity feed. This field is read-only when you are making a change to a workflow.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related information

[For more information, see the IBM Knowledge Center.](#)

Activities

Use this page to create the workflow activities, such as approvals, e-mail notifications, and requests for information. If you do not have access control item permission to change the workflow, the information on this page is displayed in read-only mode.

Select method for defining activities

Select **Simple** to select workflow activities from the fields in the **Simple Activities Definition** table, or select **Advanced** to use the workflow designer to configure the activities.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Simple

The **Simple Activities Definition** table displays the activities in a workflow. The activities are listed in the order in which they are to be performed. If you have permission to create or change the workflow, you can add, delete, and change the activities in the table. You can also change the order of activities within the table.

Select the type of activity that you want to add and click **Go**. The [specific Activities page](#) is displayed.

Select

Specifies an activity. To select one or more activities, select the check box adjacent to the activity. To select all activities, select the check box at the top of the column.

Order

Identifies the order in which an activity runs. An activity at the top of the list runs before an activity that is lower in the list.

Activity Name

Identifies the name of an activity. If the workflow already contains activities, they are displayed in the table. Click the name of the activity to view or change the information about the activity.

Participant

Identifies the user or group of users who are responsible for managing the activity.

Escalation Time in Days

Identifies the number of days that the participant must act before an account or access request escalates to the escalation participant.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Change

Click to change a selected activity.

Delete

Click to delete one or more selected activities. The activities are immediately deleted from the list. If you click **Delete** and then decide to keep the activities, click **Cancel** to exit and retain the activities in the workflow.

Move up

Click to change the order in which an activity runs. The activity must be selected.

Move down

Click to change the order in which an activity runs. The activity must be selected.

Advanced

Use the workflow designer Java applet to define activities for the workflow. Activities that you create in the workflow designer cannot later be modified using the simple method.

Workflows can be as simple as requiring only one approval, or they can be as complex as requiring multiple approvals with RFIs, loops, and so on. Manual activities that are defined in the workflow populates an individual participant's To Do list as each process in the workflow is completed. At any point, the system administrator can view any user's To Do list and act as the Participant, overriding the approval authority.

To define a workflow, drag and drop the design nodes from the node palette onto the workflow design space and connect them with transition lines.

After you place a design node on the workflow design space, double-click the node to configure its properties.

Workflow design interface

The workflow designer has these areas:

Workflow Name

Displays the name of the workflow.

Service Type

Displays the name of the service type.

Node palette

Displays all available nodes in the left pane of the interface.

Design space

Displays the nodes that you are working with in the large pane of the interface.

High Contrast

Select this check box to display the workflow design interface without color representing the design nodes.

Properties

Click this button to view configurable properties of the workflow node.

Update

Click this button to refresh the view of the workflow design space.

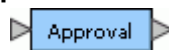
Save

Saves the changes that you made.

Workflow design nodes

The following workflow design nodes are available:

Approval



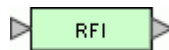
Use this node to define the person who must approve a request or activity before workflow processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Mail



Use this node to configure e-mail notification.

RFI



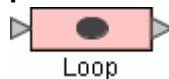
Use this node to request information from a person. For example, you might need a manager to provide contact information for a new employee before the process of issuing the employee an e-mail account can complete. The person must respond with the information before workflow processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Operation



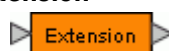
Use this node to initiate an operation workflow that has been defined previously. This workflow can be initiated at any point during the primary workflow.

Loop



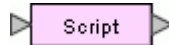
Use this node to repeat a specified activity while or until a specified condition is met.

Extension



Use this node to specify a workflow extension to manage people and accounts.

Script



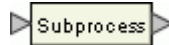
Use this node to specify a JavaScript script that the runs when processing the workflow activities.

Work Order



Use this node to e-mail a request notification for a manual activity. For example, you might use this node in a workflow to request an ID badge for a new employee. Work order participants are not required to have an IBM Security Identity Manager account. They must, however, have an e-mail address that is stored in the IBM Security Identity Manager directory server.

Subprocess



Use this node to call a previously defined workflow sequence. Several previously defined workflows can serve as subprocesses for a new workflow.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Account Request Workflows

Use this page to create, change, or delete account request workflows.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Workflow searches for workflow names or descriptions that contain the text that is entered in the **Search information** field.

Service searches for workflows that are referenced by provisioning policies for service instances matching the specified search criteria that is entered in the **Search information** field. Workflows that are not referenced by any provisioning policies are not displayed. Workflows that are referenced only by provisioning policies that specify a service type or all services are also not displayed.

Account Request Workflows table

Lists the account request workflows matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a workflow. To select one or more workflows, select the check box adjacent to the workflow. To select all workflows, select the check box at the top of the column.

Workflow Name

Identifies the name of the workflow. Click the name to view or change the workflow.

Description

Provides a brief description of the workflow.

Business Unit

Identifies the business unit that is associated with the workflow. Click the link for more information about the business unit.

Service Type

Identifies the name of the type of service to which the workflow applies. A value of ***All** means that the workflow applies to all service types. This column header changes dynamically, depending on the workflow type.

Service Names

Identifies the name of the service instances that are entitled by the workflow. This column header changes dynamically, depending on the workflow type.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Use these buttons:

Create

Click to create a new workflow.

Change

Click to change the selected workflow.

Delete

Click to delete one or more selected workflows. You cannot delete the default account request workflow, which is used by the default provisioning policies.

Related information

[For more information, see the IBM Knowledge Center.](#)

Manage Account Request Workflows

Use this notebook to specify details related to the account request workflows. Click each page to view general information and activities for the workflow. In advanced mode, you can use the workflow designer to specify a workflow.

Related information

[For more information, see the IBM Knowledge Center.](#)

General

Use this page to specify general information about a workflow. If you are viewing an existing workflow and you do not have access control item permission to change the workflow, the information on this page is displayed in read-only mode.

Name

Type a name to identify the workflow.

Description

Type a description of the intended purpose of the workflow.

Business unit

Indicates the business unit. Click **Search** to locate and select a business unit. This field is read-only when you are making a change to a workflow.

Service type

Select a service type from the list. This list includes all of the installed service types that do not represent an identity feed. This field is read-only when you are making a change to a workflow.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related information

[For more information, see the IBM Knowledge Center.](#)

Activities

Use this page to create the workflow activities, such as approvals, e-mail notifications, and requests for information. If you do not have access control item permission to change the workflow, the information on this page is displayed in read-only mode.

Select method for defining activities

Select **Simple** to select workflow activities from the fields in the **Simple Activities Definition** table, or select **Advanced** to use the workflow designer to configure the activities.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Simple

The **Simple Activities Definition** table displays the activities in a workflow. The activities are listed in the order in which they are to be performed. If you have permission to create or change the workflow, you can add, delete, and change the activities in the table. You can also change the order of activities within the table.

Select the type of activity that you want to add and click **Go**. The [specific Activities page](#) is displayed.

Select

Specifies an activity. To select one or more activities, select the check box adjacent to the activity. To select all activities, select the check box at the top of the column.

Order

Identifies the order in which an activity runs. An activity at the top of the list runs before an activity that is lower in the list.

Activity Name

Identifies the name of an activity. If the workflow already contains activities, they are displayed in the table. Click the name of the activity to view or change the information about the activity.

Participant

Identifies the user or group of users who are responsible for managing the activity.

Escalation Time in Days

Identifies the number of days that the participant must act before an account or access request escalates to the escalation participant.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Change

Click to change a selected activity.

Delete

Click to delete one or more selected activities. The activities are immediately deleted from the list. If you click **Delete** and then decide to keep the activities, click **Cancel** to exit and retain the activities in the workflow.

Move up

Click to change the order in which an activity runs. The activity must be selected.

Move down

Click to change the order in which an activity runs. The activity must be selected.

Advanced

Use the workflow designer Java applet to define activities for the workflow. Activities that you create in the workflow designer cannot later be modified using the simple method.

Workflows can be as simple as requiring only one approval, or they can be as complex as requiring multiple approvals with RFIs, loops, and so on. Manual activities that are defined in the workflow populates an individual participant's To Do list as each process in the workflow is completed. At any point, the system administrator can view any user's To Do list and act as the Participant, overriding the approval authority.

To define a workflow, drag and drop the design nodes from the node palette onto the workflow design space and connect them with transition lines.

After you place a design node on the workflow design space, double-click the node to configure its properties.

Workflow design interface

The workflow designer has these areas:

Workflow Name

Displays the name of the workflow.

Service Type

Displays the name of the service type.

Node palette

Displays all available nodes in the left pane of the interface.

Design space

Displays the nodes that you are working with in the large pane of the interface.

High Contrast

Select this check box to display the workflow design interface without color representing the design nodes.

Properties

Click this button to view configurable properties of the workflow node.

Update

Click this button to refresh the view of the workflow design space.

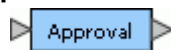
Save

Saves the changes that you made.

Workflow design nodes

The following workflow design nodes are available:

Approval



Use this node to define the person who must approve a request or activity before workflow processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Mail



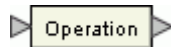
Use this node to configure e-mail notification.

RFI



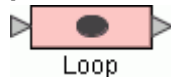
Use this node to request information from a person. For example, you might need a manager to provide contact information for a new employee before the process of issuing the employee an e-mail account can complete. The person must respond with the information before workflow processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Operation



Use this node to initiate an operation workflow that has been defined previously. This workflow can be initiated at any point during the primary workflow.

Loop



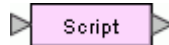
Use this node to repeat a specified activity while or until a specified condition is met.

Extension



Use this node to specify a workflow extension to manage people and accounts.

Script



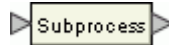
Use this node to specify a JavaScript script that the runs when processing the workflow activities.

Work Order



Use this node to e-mail a request notification for a manual activity. For example, you might use this node in a workflow to request an ID badge for a new employee. Work order participants are not required to have an IBM Security Identity Manager account. They must, however, have an e-mail address that is stored in the IBM Security Identity Manager directory server.

Subprocess



Use this node to call a previously defined workflow sequence. Several previously defined workflows can serve as subprocesses for a new workflow.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Access Request Workflows

Manage Access Request Workflows

Use this page to create, change, or delete access request workflows.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Workflow searches for workflow names or descriptions that contain the text that is entered in the **Search information** field.

Access searches for workflows that specify accesses that have an access name or description that contains the text that is entered in the **Search information** field.

Access Request Workflows table

Lists the workflows matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a workflow. To select one or more workflows, select the check box adjacent to the workflow. To select all workflows, select the check box at the top of the column.

Workflow Name

Identifies the name of the workflow. Click the name to view or change the workflow.

Description

Provides a brief description of the workflow.

Business Unit

Identifies the business unit that is associated with the workflow. Click the link for more information about the business unit.

Service Type

Identifies the name of the type of service to which the workflow applies. A value of ***All** means that the workflow applies to all service types. This column header changes dynamically, depending on the workflow type.

Access Names

Identifies the name of the accesses that are entitled by the workflow. This column header changes dynamically, depending on the workflow type.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Use these buttons:

Create

Click to create a new workflow.

Change

Click to change the selected workflow.

Delete

Click to delete one or more selected workflows.

Manage Access Request Workflows

Use this notebook to specify details related to the access request workflows. Click each page to view general information and activities for the workflow. In advanced mode, you can use the workflow designer to specify a workflow.

General

Use this page to specify general information about a workflow. If you are viewing an existing workflow and you do not have access control item permission to change the workflow, the information on this page is displayed in read-only mode.

Name

Type a name to identify the workflow.

Description

Type a description of the intended purpose of the workflow.

Business unit

Indicates the business unit. Click **Search** to locate and select a business unit. This field is read-only when you are making a change to a workflow.

Service type

Select a service type from the list. This list includes all of the installed service types that do not represent an identity feed. This field is read-only when you are making a change to a workflow.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related information

For more information, see the [IBM Knowledge Center](#).

Activities

Use this page to create the workflow activities, such as approvals, e-mail notifications, and requests for information. If you do not have access control item permission to change the workflow, the information on this page is displayed in read-only mode.

Select method for defining activities

Select **Simple** to select workflow activities from the fields in the **Simple Activities Definition** table, or select **Advanced** to use the workflow designer to configure the activities.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Simple

The **Simple Activities Definition** table displays the activities in a workflow. The activities are listed in the order in which they are to be performed. If you have permission to create or change the workflow, you can add, delete, and change the activities in the table. You can also change the order of activities within the table.

Select the type of activity that you want to add and click **Go**. The [specific Activities page](#) is displayed.

Select

Specifies an activity. To select one or more activities, select the check box adjacent to the activity. To select all activities, select the check box at the top of the column.

Order

Identifies the order in which an activity runs. An activity at the top of the list runs before an activity that is lower in the list.

Activity Name

Identifies the name of an activity. If the workflow already contains activities, they are displayed in the table. Click the name of the activity to view or change the information about the activity.

Participant

Identifies the user or group of users who are responsible for managing the activity.

Escalation Time in Days

Identifies the number of days that the participant must act before an account or access request escalates to the escalation participant.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Change

Click to change a selected activity.

Delete

Click to delete one or more selected activities. The activities are immediately deleted from the list. If you click **Delete** and then decide to keep the activities, click **Cancel** to exit and retain the activities in the workflow.

Move up

Click to change the order in which an activity runs. The activity must be selected.

Move down

Click to change the order in which an activity runs. The activity must be selected.

Advanced

Use the workflow designer Java applet to define activities for the workflow. Activities that you create in the workflow designer cannot later be modified using the simple method.

Workflows can be as simple as requiring only one approval, or they can be as complex as requiring multiple approvals with RFIs, loops, and so on. Manual activities that are defined in the workflow populates an individual participant's To Do list as each process in the workflow is completed. At any point, the system administrator can view any user's To Do list and act as the Participant, overriding the approval authority.

To define a workflow, drag and drop the design nodes from the node palette onto the workflow design space and connect them with transition lines.

After you place a design node on the workflow design space, double-click the node to configure its properties.

Workflow design interface

The workflow designer has these areas:

Workflow Name

Displays the name of the workflow.

Service Type

Displays the name of the service type.

Node palette

Displays all available nodes in the left pane of the interface.

Design space

Displays the nodes that you are working with in the large pane of the interface.

High Contrast

Select this check box to display the workflow design interface without color representing the design nodes.

Properties

Click this button to view configurable properties of the workflow node.

Update

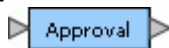
Click this button to refresh the view of the workflow design space.

Save

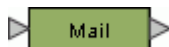
Saves the changes that you made.

Workflow design nodes

The following workflow design nodes are available:

Approval

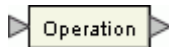
Use this node to define the person who must approve a request or activity before workflow processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Mail

Use this node to configure e-mail notification.

RFI

Use this node to request information from a person. For example, you might need a manager to provide contact information for a new employee before the process of issuing the employee an e-mail account can complete. The person must respond with the information before workflow processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Operation

Use this node to initiate an operation workflow that has been defined previously. This workflow can be initiated at any point during the primary workflow.

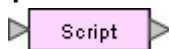
Loop

Loop

Use this node to repeat a specified activity while or until a specified condition is met.

Extension

Use this node to specify a workflow extension to manage people and accounts.

Script

Use this node to specify a JavaScript script that the runs when processing the workflow activities.

Work Order



Use this node to e-mail a request notification for a manual activity. For example, you might use this node in a workflow to request an ID badge for a new employee. Work order participants are not required to have an IBM Security Identity Manager account. They must, however, have an e-mail address that is stored in the IBM Security Identity Manager directory server.

Subprocess



Use this node to call a previously defined workflow sequence. Several previously defined workflows can serve as subprocesses for a new workflow.

Related information

For more information, see the [IBM Knowledge Center](#).

Activities

Use this page to create or change an approval, mail, or request for information activity.

Related information

For more information, see the [IBM Knowledge Center](#).

For more information, refer to the [information center](#).

Approval Activity

Use this page to specify an activity for approving account or access requests. If you do not have access control item permission to change the workflow, the information on this page is displayed in read-only mode.

Activity name

Specify a name for the approval activity.

Approver type

Select the participant who approves the request. Ensure that the approval participants that you select are able to access the To-Do list.

User name

To locate and select a user as the approver, click **Search**. This field is displayed only when you select **Specified user**.

Organizational role

To locate and select an organizational role as the approver, click **Search**. This field is displayed only when you select **Organizational role**.

Group

To locate and select a group as the approver, click **Search**. This field is displayed only when you select **Group**.

Escalation time in days

Specify the number of days in which the approver must act before the approval activity escalates to the escalation participant.

Escalation participant type

Select the escalation participant who approves an escalated request. Ensure that the escalation participants that you select are able to access the To-Do list.

User name

To locate and select a user as the escalation participant, click **Search**. This field is displayed only when you select **Specified user**.

Organizational role

To locate and select an organizational role as the escalation participant, click **Search**. This field is displayed only when you select **Organizational role**.

Group

To locate and select a group as the escalation participant, click **Search**. This field is displayed only when you select **Group**.

Related information

For more information, see the [IBM Knowledge Center](#).

For more information, refer to the [information center](#).

Mail Activity

Use this page to specify the contents and recipient of an e-mail message. You can also create, change, or delete e-mail templates used for defining contents of mail activities. If you do not have access control item permission to change the workflow, the information on this page is displayed in read-only mode.

Activity name

Specify a name for the mail activity.

Recipient type

Select a recipient for the mail activity.

User name

Click **Search** to locate and select a user as the recipient. This field is displayed only when you select **Specified user**.

Organizational role

Click **Search** to locate and select an organizational role as the recipient. This field is displayed only when you select **Organizational role**.

Group

Click **Search** to locate and select a group as the recipient. This field is displayed only when you select **Group**.

Load from Template

Click to select the mail template from which to load the content and to perform other mail template management tasks. After the contents are loaded into the page from a mail template, editing the content in the mail activity affects only the mail activity, but not the template.

Subject

Specify a description of the activity to the recipient of the mail notification.

Plaintext body

Specify the main content of the e-mail message to the recipient that describes the outcome of the activity, in plain text format. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Specify the main content of the e-mail message to the recipient that describes the outcome of the activity, in XHTML format. The content in this section can include images and hyper links.

Related information

For more information, see the [IBM Knowledge Center](#).

For more information, refer to the [information center](#).

Request for Information Activity

Use this page to specify the account attributes to be provided by the specified participant. If you do not have access control item permission to change the workflow, the information on this page is displayed in read-only mode.

Activity name

Specify a name for the request for information activity.

Account type

Select the service type of the account for which information is to be provided. This list includes all of the installed service types that do not represent an identity feed. This field is read-only when you are making a change to a workflow.

The information displayed in the **Account Attributes** table varies, depending on the service type selection.

Account Attributes table

Lists account attributes, which vary by service type. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account attribute. To select one or more account attributes, select the check box adjacent to the account attribute. To select all account attributes, select the check box at the top of the column.

Fields to Provide

Identifies the account attributes.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Participant type

Select the participants who are responsible for managing the activity. Ensure that the participants that you select are able to access the To-Do list and that they have permission to view the account attributes.

User name

Click **Search** to locate and select a user as the participant. This field is displayed only when you select **Specified user**.

Organizational role

Click **Search** to locate and select an organizational role as the participant. This field is displayed only when you select **Organizational role**.

Group

Click **Search** to locate and select a group as the participant. This field is displayed only when you select **Group**.

Escalation time in days

Specify the number of days that the participant must act before the request for information activity escalates to the escalation participant.

Escalation participant type

Select the escalation participant who receives the request for information. Ensure that the escalation participants that you select are able to access the To-Do list and that they have permission to view the account attributes.

User name

Click **Search** to locate and select a user as the escalation participant. This field is displayed only when you select **Specified user**.

Organizational role

Click **Search** to locate and select an organizational role as the escalation participant. This field is displayed only when you select **Organizational role**.

Group

Click **Search** to locate and select a group as the escalation participant. This field is displayed only when you select **Group**.

Related information

For more information, see the [IBM Knowledge Center](#).

For more information, refer to the [information center](#).

Mail Activity Templates

Use this page to select the mail template from which to load the contents of the mail activity. You can also use this page to perform other mail template management tasks.

Mail Activity Templates table

Contains the templates from which to load the contents of the mail activity. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a template. Click the radio button in this column adjacent to the template to select a template.

Name

Identifies the name of the template. Click the name of the template to view or change the template details.

Subject

Identifies the activity to the recipient of the mail notification.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Use these buttons:

Create

Click to create a template.

Create like

Click to create a template that is like a selected template. When you are done, if you do not change the value of the **Template name** field, the changed template is saved with "Copy of" as part of the template name.

Change

Click to change a selected template.

Delete

Click to delete a selected template.

OK

Click to load the content from the selected template and save any additional template changes that have been made.

Related information

For more information, see the [IBM Knowledge Center](#).

For more information, refer to the [information center](#).

Mail Activity Template

Use this page to define or change a mail notification template.

Template name

Specify the name of the mail template.

Subject

Specify a description of the activity to the recipient of the mail notification.

Plaintext body

Specify the main content of the e-mail message to the recipient that describes the outcome of the activity, in plain text format. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Specify the main content of the e-mail message to the recipient that describes the outcome of the activity, in XHTML format. The content in this section can include images and hyper links.

Related information

For more information, see the [IBM Knowledge Center](#).

For more information, refer to the [information center](#).

Set system security

Configure Forgotten Password Settings

Use this page to enable forgotten password authentication, configure the challenge questions, and set the number of questions that must be answered.

Note: This task is effective only if a WebSphere account repository is specified. This field is located on the ITIM Service **Manage Services > Change a Service > Service Information** page. This repository can be ITIM Service or a service managed by the IBM Security Identity Manager server. If no registry is specified, the forgotten password option is not available on the **Login** page.

Enable forgotten password authentication

Select this check box to enable the use of forgotten password authentication. If you enable the authentication, the login page provides a **Forgot your password?** prompt for users who forget their passwords. A user who provides the correct responses to the questions receives a new, automatically generated password. If the check box is cleared, no prompt occurs on the login page. Users must contact the help desk assistants or system administrators for help in resetting their passwords.

Login Behavior

When the user successfully answers the questions

Select the login behavior:

Change password and log in to system

Prompts the user to change the password and then logs the user in to the system.

Reset and email password

Resets the password, and sends the new password to the email address of the user.

Message suspending account for failed answers

Type the message the user receives after failing to enter the correct answers.

Send message to email address

Type the email address to receive messages.

Challenge Behavior

Select whether the user or the administrator defines challenge questions.

Users define their own questions

Select to enable users to provide their questions.

Number of questions user sets up

Type the number of questions that the user must provide.

Number of correct answers user must enter

Type the number of correct answers that the user must provide to gain access to the system.

Administrator provides predefined questions

Select to define the set of questions that the users must answer and the language in which the question is displayed. When this radio button is selected, the Specify Forgotten Password Question section is displayed.

Specify Forgotten Password Question

Click to expand this section, to specify the question that you want users to answer.

New challenge question

Type the question that you want users to answer and click **Add**.

Locale

Select the language in which the question is displayed and click **Add**.

Challenge questions table

The **Challenge questions** table contains the list of questions that you have added and that you can choose to have users answer. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select this check box to select an existing question.

Locale

Displays the language used in the question.

Question

Displays the text of a question.

Click **Remove** to remove a selected question.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

User has a choice of predefined questions?

No, answer all questions

Displays all predefined questions, which the user must answer correctly.

Yes, user selects which questions to answer

Displays the number of questions that the user selects and must answer correctly after forgetting a password. Type the number of questions that the user selects.

No, answer a subset of questions that the system provides

Displays a random subset of predefined questions, which the user must answer correctly after forgetting a password.

Number of questions user sets up

Type the number of questions that the user configures.

Number of correct answers user must enter

Type the number of questions that the user must correctly answer. This field is available, if the user must answer a subset of questions that the system provides.

Challenge answer rules

Maximum length

The maximum allowed length of an answer to the challenge question.

Maximum repeated characters

A maximum number of times a character can be repeated in the answer to the challenge question.

Disallow user ID

Select the check box to disallow the user ID as answer to the challenge question.

Require unique answers

Select the check box to allow only unique answers to all the challenge questions.

Answer cannot match question

Select the check box to restrict the answer that is same as the challenge question.

For the new values to take effect, you must log out and log in again.

Note: By default, users can bypass the challenge questions. You can force the user to respond to the challenge questions by modifying the property `ui.challengeResponse.bypassChallengeResponse` in the `ui.properties` file. To force user response, set the value to `false`. For more information, see the `ui.properties` topic in the Supplemental property files section of the *IBM Security Identity Manager Reference Guide*.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Set Security Properties

Use this page to configure password administration settings and login account settings.

Password Settings

Enable password editing

Select this check box to enable users to type a value when changing their own passwords. Additionally, help desk assistants, service owners, and administrators can type a value when changing their own passwords, and also the passwords for other individuals. You can also select a check box by using the Tab key to give focus to the check box and then pressing the space bar.

Note: In some cases, the user cannot change the password, even when **Enable password editing** is selected. In these cases, the system automatically generates a new password. For example, some accounts are placed in a credential vault, and configured such that their credentials must be checked in and checked out. For these accounts, users cannot change the password, regardless of the value of the password editing configuration setting on this page.

Hide generated passwords for others

Select this check box to hide generated passwords for others. This check box is unavailable if password editing is enabled.

Enable password synchronization

Select this check box to synchronize any subsequent password changes on all of the individual accounts for a user. If this check box is selected, one password change is synchronized on all individual accounts for the user. Password synchronization does not affect sponsored accounts. If this check box is cleared, the user must select each account and change its password individually.

Set password on user during user creation

Select this check box to set the password for a user, at the time the user is created.

Password retrieval expiration period in hours

Type an interval, in hours, in which a user must retrieve a password, before the password expires.

Identity Manager Login Account Settings

Identity account password expiration period in days

Type an interval, in days, after which the password expires for a IBM Security Identity Manager account. The default value of 0 indicates that the account password never expires.

Note: If Identity Manager is configured to use an authentication repository other than ITIM Service, you cannot specify password expiration. In this case, the configuration setting for password expiration is read only.

Maximum number of incorrect login attempts

Type the number of incorrect login attempts that can occur before a IBM Security Identity Manager account is suspended. The default value of 0 indicates that there is no limit.

Note: If Identity Manager is configured to use an authentication repository other than ITIM Service, you cannot specify the maximum number of incorrect login attempts. In this case, the configuration setting for the maximum number of incorrect login attempts is read only.

Group Settings

Automatically populate Identity Manager groups

Select this checkbox to automatically put the IBM Security Identity Manager accounts of newly named service owners in the default Service Owner group. The automatic action is enabled or disabled immediately. You do not need to restart IBM Security Identity Manager. For example,

membership in a group can take place when you create or modify a service, specifying a service owner.

Additionally, the IBM Security Identity Manager accounts of newly named managers are automatically put in the default Manager group. For example, this population can occur when you create or modify a user who is a subordinate, specifying the manager of the user.

Automatic group membership is not supported when the service owner is a role.

Default Settings for Provisioning Policy When a New Service is Created

Select the default setting for provisioning policies when new services are created. You might not want to create a default policy when a new service is created if the amount of time to evaluate the default policy for all users is significant.

Yes, create a policy for manually requesting accounts

Select this option to require that users manually request account entitlement.

Yes, create a policy to automatically create accounts, and later enable the policy

Select this option to allow for automatic provisioning of new accounts to users. You must subsequently enable the policy to provision new accounts.

Yes, create a policy to automatically create accounts as soon as the policy exists

Select this option to allow for automatic provisioning of new accounts to users. Provisioning of new accounts occurs as soon as the policy exists, and the Default Account Request Workflow is associated with the provisioning policy.

No, I will manually configure a policy later

Select this option if you want to configure a provisioning policy at a later time.

You might manually configure a provisioning policy if you need to set up account defaults or identity policies for this service. Later, you can change the provisioning to automatic.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

[For more information, see the IBM Knowledge Center.](#)

Select Group

Use the **Select Group** page to search for a group.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Group name or description

Searches for groups with a name or description that contains text that is entered in the **Search information** field.

Business unit

Searches for business units in which the business unit name contains the text that is entered in the **Search information** field.

Groups table

Lists the groups matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box next to the group. To select all groups, select the check box at the top of the column.

Group Name

Identifies the name of the group.

You can use these menu items:

Manage Members

Click to see which users are members in the selected group. You can also add or remove members from the selected group.

Add Members

Click to add members to the selected group.

Description

Displays information about the intended purpose of the group.

View

Identifies the view of tasks that users have in this group.

Business Unit

Identifies the business unit in which the group is specified.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new group.

Change

Click to change the description or membership for the selected group.

Delete

Click to remove the selected group from the system.

Export Access Data

Click to open the **Export Access Data** page, and export the group access data. The **Export Access Data** button is not active until you select some accesses to activate it. Only the group access that you selected are exported.

Import Access Data

Click to open the **Import Access Data** page to import the access data for a group access. You can also import access data for a set of groups.

Refresh

Click to refresh the list of items in the table.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

[For more information, see the IBM Knowledge Center.](#)

Create a Group

Use the **Create a Group** wizard to create additional groups and add members to the groups.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

[For more information, see the IBM Knowledge Center.](#)

General Information

Use this page to specify information about a group.

Group Name

Type a unique, user-friendly name for the new group. It is important to specify meaningful group names because, in some cases, users might have only this information to guide a group membership decision for an account.

View

Select the view of tasks.

Description

Type information about the group's intended purpose. It is important to specify meaningful descriptions because, in some cases, users might only have this information to guide a group membership decision for an account.

Business Unit

Specify the business unit. To locate available business units, click **Search**.

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Group Membership

Use this page to specify which users are members of a group.

Group Membership table

Lists the users that you can select as members of the group. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

User Name

Identifies the full name of the user. Click the name to see the user's information profile.

User ID

Identifies the user ID for the user. This field is available after you add a user to the group.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a member to the group.

Remove

Click to remove a selected member.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule Add Member Operation

Use this page to submit a request. This page is available after you add one or more members to a group.

Immediate

Runs the request immediately after you click the button to complete the task.

Effective date

Runs the request at a day and hour that you specify. After you select this option, click the calendar icon to specify the scheduled day, and click the clock icon to specify the scheduled hour.

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

[For more information, see the IBM Knowledge Center.](#)

Add Members

Use this page to add members to a group.

System account information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Attribute

Click **User name** or **User ID** to search by the user's name or ID.

System Accounts table

Contains the users matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

User Name

Identifies the user's full name. Click the name of the user to view the user's personal profile.

User ID

Identifies the user ID of the account owner.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

[For more information, see the IBM Knowledge Center.](#)

Select a Service

Use this page to find the service with the groups that you want to manage.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Service searches for service names or descriptions that contain the text that is entered in the **Search information** field.

Business unit searches for business units in which the business unit name contains the text that is entered in the **Search information** field.

Service type

Select a service type from the list. The list contains the service types that have groups enabled that are installed by the administrator. Select **All** from the list to display all of the services that have groups enabled that are managed by IBM Security Identity Manager.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Services table

Lists the services matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select a service, click the radio button adjacent to the service.

Service Name

Identifies the name of the service.

Description

Provides information about the intended purpose of the service.

Service Type

Identifies the type of service.

Note: Accesses that are defined on the original service are not available for the hosted service, and those accesses cannot be requested by users in different organizations.

Business Unit

Identifies the business unit in which the service is created.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Group

Use the **Select Group** page to search for a group or access definition.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Group name or description searches for groups in which the group name contains the text that is entered in the **Group information** field.

Access name searches for the name of the access definition that is associated with the group that is entered in the **Group information** field.

Group type

Select the type from the menu to limit the search. The default selection is to search all groups.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Groups table

Lists the groups matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box next to the group. To select all groups, select the check box at the top of the column.

Group Name

Identifies the name of the group.

You can use these menu items:

Manage Members

Click to see which users are members in the selected group. You can also add or remove members from the selected group.

Add Members

Click to add members to the selected group.

Access Recertification Status

Identifies the recertification status for access definitions for the group.

Description

Displays information about the intended purpose of the group.

Group Type

Identifies the type of group. For example, on a UNIX or AIX system, group types might include UNIX groups or AIX roles. On a Windows system, group types might include Security groups or Distribution groups.

Access Name

Identifies the name of the access for the group. Click the access name for details about the access.

Access Status

Indicates whether access is enabled or disabled.

Access Type

Identifies the type of access, such as a shared folder.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new group.

Change

Click to change the information for the selected group.

Delete

Click to remove one or more selected groups from the system.

Export Access Data

Click to open the **Export Access Data** page, and export the group access data. The **Export Access Data** button is not active until you select some accesses to activate it. Only the group access that you selected are exported.

Import Access Data

Click to open the **Import Access Data** page to import the access data for a group access. You can also import access data for a set of remote groups.

Refresh

Click to refresh the list of items in the table.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Create a Group

Use the **Create a Group** wizard to create a group on a managed resource and add members to the group.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Type

Use this page to select the type of group that you want to create. This page is displayed only if the service supports more than one type of group.

Group Type table

Lists the groups matching the specified search criteria.. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group type. To select a group type, click the radio button adjacent to the group type.

Group Type

Identifies the type of group. For examples, on a UNIX or AIX system, group types might include UNIX groups or AIX roles. On a Windows system, group types might include Security groups or Distribution groups.

Description

Displays information about the intended purpose of the group.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

General Information

Use this page to specify information about the group you are creating.

The fields on these pages might vary, depending on the service that you selected on the previous page and how you have customized the profile page. Required fields are marked with an asterisk (*).

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

AIX General Information

Use this page to specify information about a group based on the group type you have selected.

The fields on these pages might vary, depending on the group type that you selected and how you have customized the profile page.

Related concepts

Advanced Search

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

AIX Group General Information

Use this page to specify information about a group. The fields on this page might vary, depending on how you have customized the profile page. Required fields are marked with an asterisk (*).

The following are examples of the fields that you might find on the **General Information** page.

Group Name

Type a unique, user-friendly name for the new group. It is important to specify meaningful group names because, in some cases, users might have only this information to guide a group membership decision for an account. The group name is restricted to a maximum of eight characters, and no spaces are permitted. Group names must not begin with any of the following characters:

- dash (-)
- plus sign (+)
- at sign (@)
- tilde (~)

You cannot use the keywords ALL or default in a group name. Additionally, do not use any of the following characters within a group name string:

- colon (:)
- double quote (")
- pound sign (#)
- comma (,)
- equal sign (=)
- back slash (\)
- slash (/)
- question mark (?)
- single quote (')
- back quote (`)

Group ID number

Type number that corresponds to a specific group name. The group ID number is an integer that uniquely identifies each group to the operating system. You can often substitute the group ID in commands that accept a group name as a value. The system automatically assigns a value, if the field is left empty.

Administrative group

Select this check box to create the group as an administrative group.

Group administrators

Add users that can perform administrative tasks for the group.

To add a user to the list of group administrators, type the *user name* in the entry field and click **Add**.

To remove a users from the list of group administrators, select the user name from the list of administrators and click **Delete**.

Group projects

Define a list of projects to which the user's processes can be assigned. The project names must be valid project names as defined on the operating system.

To add projects to the list of group projects, type the *project name* in the entry field and click **Add**.

To remove a users from the list of group projects, select the project name from the list of projects and click **Delete**.

Click **Finish** when you are done with this task.

Related concepts

Advanced Search

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

AIX Role General Information

Use this page to specify information about a group. The fields on this page might vary, depending on how you have customized the profile page. Required fields are marked with an asterisk (*).

The following are examples of the fields that you might find on the **General Information** page.

AIX role name

Type a name for the role. To prevent inconsistencies, restrict role names to characters with the POSIX portable file name character set. You cannot use the keywords ALL or default as a role name. You cannot use the keywords ALL or default in a group name. Additionally, do not use any of the following characters within a group name string:

- colon (:)
- double quote (")
- pound sign (#)
- comma (,)
- equal sign (=)
- back slash (\)
- slash (/)
- question mark (?)
- single quote (')
- back quote (`)

Authorizations

List the additional authorizations required for this role beyond those defined by the roles in the rolelist attribute. The value is a list of authorization names.

To add authorizations , type the *authorization name* in the entry field and click **Add**.

To remove authorizations , select the authorization name from the list of authorizations and click **Delete**.

Roles implied

List the roles implied by this role. The value is a list of role names. Use **Search** to add roles or **Delete** to remove them.

List of groups

List the groups to which a user needs to belong, to effectively use this role. This attribute is for information only and does not automatically make the user a member of the list of groups. The value is a list of group names. Use **Search** to add groups or **Delete** to remove them.

Visibility

Specifies the role's visibility status to the system. The Value parameter is an integer. Possible values are:

Enabled and selectable

The role is enabled, displayed, and selectable. Authorizations contained in this role are applied to the user.

Enabled but not selectable

The role is enabled and displayed as existing, but not selectable through a visual interface. Authorizations contained in this role are applied to the user.

Disabled

The role is disabled. Authorizations contained in this role are not applied to the user.

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

HP-UX General Information

Use this page to specify information about a group. The fields on this page might vary, depending on how you have customized the profile page. Required fields are marked with an asterisk (*).

The following are examples of the fields that you might find on the **General Information** page.

Group Name

Type a unique, user-friendly name for the new group. It is important to specify meaningful group names because, in some cases, users might have only this information to guide a group membership decision for an account. The group name cannot include a colon (:) or newline (\n).

Group ID number

A number that corresponds to a specific group name. The group ID number is a non-negative decimal integer that uniquely identifies each group to the operating system. You can often substitute the group ID in commands that accept a group name as a value. The system automatically assigns a value, if the field is left empty.

Allow duplicate GIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP General Information

Use this page to specify information about a group. The fields on this page might vary, depending on how you have customized the profile page. Required fields are marked with an asterisk (*).

The following are examples of the fields that you might find on the **General Information** page.

Group Name

Type a name that uniquely identifies the group object within the container. This is the group relative distinguished name (RDN) attribute value for common name (CN).

Container

Select the distinguished name within LDAP in which to create the group object. Click on **Search** to select from the available containers.

Description

Specify information about the intended purpose of the group.

Full name

Identify additional names of the group object or CN values.

To add , type the *name* in the entry field and click **Add**.

To remove a name, select the name from the list and click **Delete**.

Owner

Specify the distinguished name of the person who owns the account that is associated with the group.

To add an owner, type the *owner dn* in the entry field and click **Add**.

To remove an owner, select the name and click **Delete**.

Business category

Specify the type of business in which the entry is engaged.

To add a category, type the *business category* in the entry field and click **Add**.

To remove a category, select the name and click **Delete**.

Organization name

Specify the name of the organization.

To add an organization, type the *organization name* in the entry field and click **Add**.

To remove an organization, select the name and click **Delete**.

Organizational unit name

Specify the name of an organizational unit.

To add an organizational unit, type the *organizational unit name* in the entry field and click **Add**.

To remove an organizational unit, select the name and click **Delete**.

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Linux General Information

Use this page to specify information about a group. The fields on this page might vary, depending on how you have customized the profile page. Required fields are marked with an asterisk (*).

The following are examples of the fields that you might find on the **General Information** page.

Group Name

Type a unique, user-friendly name for the new group. It is important to specify meaningful group names because, in some cases, users might have only this information to guide a group membership decision for an account. The group name must begin with a lower case letter or an underscore.

Characters can only be lower case letters, underscores (_), dashes (-), and dollar signs (\$). No other characters are permitted.

Group ID number

Type number that corresponds to a specific group name. The group ID number is a non-negative decimal integer that uniquely identifies each group to the operating system. You can often substitute the group ID in commands that accept a group name as a value. The system automatically assigns a value, if the field is left empty.

Allow duplicate GIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Solaris General Information

Use this page to specify information about a group. The fields on this page might vary, depending on how you have customized the profile page. Required fields are marked with an asterisk (*).

The following are examples of the fields that you might find on the **General Information** page.

Group Name

Type a unique, user-friendly name for the new group. It is important to specify meaningful group names because, in some cases, users might have only this information to guide a group membership decision for an account. The group name is restricted to a maximum of eight characters and cannot include a colon (:), or newline (\n).

Group ID number

Type a number that corresponds to a specific group name. The group ID number is a non-negative decimal integer that uniquely identifies each group to the operating system. You can often substitute the group ID in commands that accept a group name as a value. The system automatically assigns a value, if the field is left empty.

Allow duplicate GIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

[For more information, see the IBM Knowledge Center.](#)

Access information

Use the **Access information** page to specify access information for a group of users, including the name, type, description, and owner. You can also specify access approval, notification options, and other business metadata for accesses.

Define an Access

Select this check box to activate the fields that are required to define an access. Clearing this check box clears the access.

Note: If you clear this check box, the information that is contained in the fields is cleared only when the operation is completed.

Access Status

Enable Access

Select this option to enable and to include the access in the access list.

Enable Common Access

Select this option to enable and to include the access in a common access list that is visible to users.

Disable Access

Select this option to disable access.

Access name

Type a name to identify the access.

Select access type

Select an access type from the tree structure. You can expand or collapse a node in the tree to view and select an access type.

Access description

Provide more information about the access.

Access owner

Specify the user who has access ownership. To see a list of owners, click **Search**.

Approval workflow

Specify whether no approval or specific approval is required to grant access.

Notify users when access is provisioned and available for use

Select this check box to ensure that users are notified when access is provisioned.

Notify users when access is de-provisioned

Select this check box to ensure that users are notified when access is de-provisioned.

Icon URL

Provide a uniform resource identifier (URI) string for the icon. A preview of the icon is displayed that is based on the following conditions:

- If an icon URL is not specified, and the category image exists, then the preview displays the category image. An information message is displayed that this image is used.
- If an icon URL is not specified, and the category image does not exist, then the preview displays a message that there is no image.
- If an icon URL is specified, then the referenced image is displayed.

For more information, see the [Customizing an access card in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Search terms

Type the search strings that you want to add to return specific search terms. You can use multiple values for the search terms.

Use these buttons for the search terms:

Add

Click to add a search term.


Delete

Click to delete one or more search terms.

Additional information

Displays information about the access card by default. It is a free form information about the access item that the administrator considers useful.

Badges

Specify one or more badges for an access item that is associated with this service. Click the twistie icon  next to **Badges** to specify one or more badges. You can add a maximum of five badges for an access item.

Use these buttons for the badges:

Add

Click to add a badge. The button becomes inactive after a maximum of five badges are assigned to an access item.

Remove

Click to remove a badge. The button is not active until a badge is added.

Select a check box next to a badge to modify or delete it.

Badge text

Type a short text string for the badge. For example, High risk.

To customize the value of a badge text, add a \$ prefix to it. For example, \$Risk. You can customize only the value of a badge text when it is prefixed with \$. For example, \$Risk=High Risk. You cannot customize a badge text if it is not prefixed with \$.

You might want to configure the `CustomLabels.properties` file to customize the value for the badge text. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Badge class

Select a specific CSS class from the list to apply to the badge text. You can customize a badge class, where you can specify your own styles to be displayed in the **Badge class** list. For example, a CSS class can consist of font type, size, color, or other formatting styles, which you can apply to the specified badge text.

You might want to customize a badge CSS style to suit your requirements. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Preview

A preview displays the badge text that is based on the badge class you selected.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Group Membership

Use this page to specify which accounts are members of a group.

Group Membership table

Lists the accounts that are members of the group. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box next to the group. To select all groups, select the check box at the top of the column.

User Name

Identifies the user's full name. Click the name of the user to view the user's personal profile.

User ID

Identifies the string of characters that uniquely identifies a user to a system. This field is available after you add an account to the group.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add one or more members to the group.

Remove

Click to remove one or more selected members from the group.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Schedule Add Member Operation

Use this page to submit a request. This page is available after you add one or more members to a group.

Immediate

Runs the request immediately after you click the button to complete the task.

Effective date

Runs the request at a day and hour that you specify. After you select this option, click the calendar icon to specify the scheduled day, and click the clock icon to specify the scheduled hour.

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Advanced Search

Use this page to specify the criteria to search for an account.

Account type

Displays the account type for the service on which the account exists. You cannot change the account type.

User ID

Type the user ID.

Status

Select whether to search all accounts, or only active or inactive accounts.

Compliance Status

Select whether to search all accounts, or only compliant or noncompliant accounts or those accounts that have no compliance status specified.

Owner

Select an account owner. To locate an owner to search by, click **Add**. If multiple owners are listed, to narrow the search select the owners that you do not want to search by and click **Remove**.

Add another search field

Select additional attributes to qualify your search.

You can use these buttons:

Search

Click to search for an account.

Search filter

Click to specify an LDAP filter for your search criteria.

Change a group

Use this page to change the general information or the access information about the group.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

General Information

Use this page to change information about a group.

The fields on these pages might vary, depending on the service that you selected and how you have customized the profile page.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

AIX General Information

Use this page to change information about a group.

The fields on these pages might vary, depending on the group type that you selected and how you have customized the profile page.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

AIX Group General Information

Use this page to change information about a group. The fields on this page might vary, depending on how you have customized the profile page. Required fields are marked with an asterisk (*).

The following are examples of the fields that you might find on the **General Information** page.

Group Name

Displays the unique, user-friendly name for the group. You cannot change it.

Group ID number

Displays the unique number that corresponds to a specific group name and identifies each group to the operating system. You can often substitute the group ID in commands that accept a group name as a value. You cannot change it.

Administrative group

Select or clear this check box to change whether the group is an administrative group.

Group administrators

Add or remove users that can perform administrative tasks for the group.

To add a user to the list of group administrators, type the *user name* in the entry field and click **Add**.

To remove a users from the list of group administrators, select the user name from the list of administrators and click **Delete**.

Group projects

Add or remove projects to which the user's processes can be assigned. The project names must be valid project names as defined on the operating system.

To add projects to the list of group projects, type the *project name* in the entry field and click **Add**.

To remove a users from the list of group projects, select the project name from the list of projects and click **Delete**.

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

AIX Role General Information

Use this page to change information about a group. The fields on this page might vary, depending on how you have customized the profile page. Required fields are marked with an asterisk (*).

The following are examples of the fields that you might find on the **General Information** page.

AIX role name

Displays the role's name. You cannot change it.

Authorizations

Lists the additional authorizations required for this role beyond those defined by the roles in the rolist attribute. The value is a list of authorization names.

To add authorizations , type the *authorization name* in the entry field and click **Add**.

To remove authorizations , select the authorization name from the list of authorizations and click **Delete**.

Roles implied

Lists the roles implied by this role. The value is a list of role names. Use **Search** to add roles or **Delete** to remove them.

List of groups

Lists the groups to which a user needs to belong, to effectively use this role. This attribute is for information only and does not automatically make the user a member of the list of groups. The value is a list of group names. Use **Search** to add groups or **Delete** to remove them.

Visibility

Specifies the role's visibility status to the system.

Enabled and selectable

The role is enabled, displayed, and selectable. Authorizations contained in this role are applied to the user.

Enabled but not selectable

The role is enabled and displayed as existing, but not selectable through a visual interface. Authorizations contained in this role are applied to the user.

Disabled

The role is disabled. Authorizations contained in this role are not applied to the user.

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

[For more information, see the IBM Knowledge Center.](#)

HP-UX General Information

Use this page to change information about a group. The fields on this page might vary, depending on how you have customized the profile page.

The following are examples of the fields that you might find on the **General Information** page.

Group Name

Displays the unique, user-friendly name for the new group. You cannot change it.

Group ID number

Displays the unique number that corresponds to a specific group name and identifies each group to the operating system. You can often substitute the group ID in commands that accept a group name as a value.



CAUTION: Do not change this attribute because doing so compromises system security.

Allow duplicate GIDs?

Select or clear this check box to change whether to allow the group ID to be duplicated (non-unique).

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

[For more information, see the IBM Knowledge Center.](#)

LDAP General Information

Use this page to change information about a group. The fields on this page might vary, depending on how you have customized the profile page.

The following are examples of the fields that you might find on the **General Information** page.

Group Name

Uniquely identifies the name of the group object within the container. This is the group relative distinguished name (RDN) attribute value for common name (CN). You cannot change it.

Container

Identifies the distinguished name within LDAP in which the group object was created. You cannot change it.

Description

Specifies information about the group's intended purpose.

To add information to the description, type the *text* in the entry field and click **Add**.

To remove information from the description, select the text and click **Delete**.

Full name

Identifies additional names of the group object or CN values.

To add , type the *name* in the entry field and click **Add**.

To remove a name, select the name from the list and click **Delete**.

Owner

Identifies the distinguished name of the person who owns the account that is associated with the group.

To add an owner, type the *owner dn* in the entry field and click **Add**.

To remove an owner, select the name and click **Delete**.

Business category

Identifies the type of business in which the entry is engaged.

To add a category, type the *business category* in the entry field and click **Add**.

To remove a category, select the name and click **Delete**.

Organization name

Identifies the name of the organization.

To add an organization, type the *organization name* in the entry field and click **Add**.

To remove an organization, select the name and click **Delete**.

Organizational unit name

Identifies the name of an organizational unit.

To add an organizational unit, type the *organizational unit name* in the entry field and click **Add**.

To remove an organizational unit, select the name and click **Delete**.

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Linux General Information

Use this page to change information about a group. The fields on this page might vary, depending on how you have customized the profile page.

The following are examples of the fields that you might find on the **General Information** page.

Group Name

Displays the unique, user-friendly name for the new group. You cannot change it.

Group ID number

Displays the unique number that corresponds to a specific group name and identifies each group to the operating system. You can often substitute the group ID in commands that accept a group name as a value.



CAUTION: Do not change this attribute because doing so compromises system security.

Allow duplicate GIDs?

Select or deselect this check box to change whether to allow the group ID to be duplicated (non-unique).

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Solaris General Information

Use this page to change information about a group. The fields on this page might vary, based on how you have customized the profile page.

The following are examples of the fields that you might find on the **General Information** page.

Group Name

Displays the unique, user-friendly name for the new group. You cannot change it.

Group ID number

Displays the unique number that corresponds to a specific group name and identifies each group to the operating system. You can often substitute the group ID in commands that accept a group name as a value.



CAUTION: Do not change this attribute because doing so compromises system security.

Allow duplicate GIDs?

Select or deselect this check box to change whether to allow the group ID to be duplicated (non-unique).

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Non-manageable Group General Information

Use this page to view information about the group. You cannot change any information on this page.

The following group name field is displayed on the General Information page.

Group Name

Displays the unique, user-friendly name for the new group. You cannot change it.

Click **Finish** when you are done with this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Access information

Use the **Access information** page to change access information for a group of users, including the name, type, description, and owner. You can also change access approval, notification options, and other business metadata for accesses.

Define an Access

Select this check box to activate the fields that are required to define an access. Clearing this check box clears the access.

Note: If you clear this check box, the information that is contained in the fields is cleared only when the operation is completed.

Access Status

Enable Access

Select this option to enable and to include the access in the access list.

Enable Common Access

Select this option to enable and to include the access in a common access list that is visible to users.

Disable Access

Select this option to disable access.

Access type

Identifies the access type.

Change Access type

Select an access type from the tree structure. You can expand or collapse a node in the tree to view and select an access type.

Access name

Type a name to identify the access.

Access description

Provide more information about the access.

Access owner

Specify the user who has access ownership. To see a list of owners, click **Search**.

Approval workflow

Specify whether no approval or specific approval is required to grant access.

Notify users when access is provisioned and available for use

Select this check box to ensure that users are notified when access is provisioned.

Notify users when access is de-provisioned

Select this check box to ensure that users are notified when access is de-provisioned.

Icon URL

Provide a uniform resource identifier (URI) string for the icon. A preview of the icon is displayed that is based on the following conditions:

- If an icon URL is not specified, and the category image exists, then the preview displays the category image. An information message is displayed that this image is used.
- If an icon URL is not specified, and the category image does not exist, then the preview displays a message that there is no image.
- If an icon URL is specified, then the referenced image is displayed.

For more information, see the [Customizing an access card in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Search terms

Type the search strings that you want to add to return specific search terms. You can use multiple values for the search terms.

Use these buttons for the search terms:

Add

Click to add a search term.


Delete

Click to delete one or more search terms.

Additional information

Displays information about the access card by default. It is a free form information about the access item that the administrator considers useful.

Badges

Specify one or more badges for an access item that is associated with this service. Click the twistie icon  next to **Badges** to specify one or more badges. You can add a maximum of five badges for an access item.

Use these buttons for the badges:

Add

Click to add a badge. The button becomes inactive after a maximum of five badges are assigned to an access item.

Remove

Click to remove a badge. The button is not active until a badge is added.

Select a check box next to a badge to modify or delete it.

Badge text

Type a short text string for the badge. For example, High risk.

To customize the value of a badge text, add a \$ prefix to it. For example, \$Risk. You can customize only the value of a badge text when it is prefixed with \$. For example, \$Risk=High Risk. You cannot customize a badge text if it is not prefixed with \$.

You might want to configure the `CustomLabels.properties` file to customize the value for the badge text. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Badge class

Select a specific CSS class from the list to apply to the badge text. You can customize a badge class, where you can specify your own styles to be displayed in the **Badge class** list. For example, a CSS class can consist of font type, size, color, or other formatting styles, which you can apply to the specified badge text.

You might want to customize a badge CSS style to suit your requirements. For more information, see the [Customizing badges on access cards in the Request Access wizard](#) section in the IBM Security Identity Manager product documentation.

Preview

A preview displays the badge text that is based on the badge class you selected.

Add Members

Use this page to locate the accounts that you want to add to the group.

Account information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

User ID searches for accounts with user IDs that contain the text that is entered in the **Account information** field.

Owner searches for accounts in which the account owner's full name contains the text that is entered in the **Account information** field.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Accounts table

Lists the accounts matching the specified search in the **Account information** field. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box adjacent to the account. To select all accounts, select the check box at the top of the column.

State

Indicates the compliancy state of the account.

Blank (no symbol)

Indicates the account is compliant.



Indicates that the account was returned from a reconciliation, which means it was not checked against the existing provisioning policies.



Indicates that the account can exist for the user, but that one or more of the account attributes do not comply with the existing provisioning policies.



Indicates either that the account is not supposed to exist because the user is not allowed to have access to the specified resource, or that a provisioning policy is not defined for the resource.

User ID

Identifies the user ID associated with the account. Click the user ID to review the account information.

Owner

Identifies the full name of the user who owns the account. Click the name of the user to view the user's personal profile.

Ownership Type

Identifies the ownership type of the account.

Status

Indicates whether the account is active or inactive.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Change Group

Use this page to change a group description or to change the view of tasks for the group. You cannot change the name of the group.

Group name

Displays the name of the group.

View

Identifies the view of tasks that users have in this group.

Description

Displays information about the intended purpose of the group.

Business unit

Identifies the business unit in which the group is specified.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

View Membership

Use this page to view a list of the current group members. You can also add or remove members from the list.

System account information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category..

User Name searches for the user's full name that contains text that is entered in the **System account information** field.

User ID searches for the user ID that contains text that is entered in the **System account information** field.

Group Membership table

Lists the current users who are members of the group. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

User Name

Identifies the user's full name. Click the name of the user to view the user's personal profile.

User ID

Identifies the user ID.

You can use these buttons:

Add

Click to add a member to the group.

Remove

Click to remove a member from the group.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

[For more information, see the IBM Knowledge Center.](#)

Group Details

Use this page to show details related to the selected group. All fields are read-only. You cannot change any information related to the group.

Group name

Displays the name of the group.

View

Identifies the view of tasks that users have in this group.

Description

Displays information about the intended purpose of the group.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

[For more information, see the IBM Knowledge Center.](#)

Membership

Use this page to view the members of the selected group.

User Name

Identifies the user's full name. Click the name of the user to view the user's personal profile.

User ID

Identifies the user ID that is associated with the user.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

[For more information, see the IBM Knowledge Center.](#)

Manage Access Control Items

Use this page to locate access control items for a business unit. You can create, change, or delete access control items, and add or remove access control item owners.

Business unit

Specifies the business unit. To locate an available business unit, type information about the unit and click **Search**.

ACI Owners

Click to add groups or remove groups that are authorized to manage access controls in the selected business unit.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Access Control Items table

Lists the access control items matching the specified search criteria that you specified in the selected business unit. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the check box in this column to select the access control item. Selecting the check box at the top of the column selects all access control items.

Name

Identifies the access control item. Click the name of the access control item to change information about the access control item.

Protection Category

Displays the type of entity to which the access control item applies.

Type

Displays the specific type of a specified system object category.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these menu items:

Create

Click to create an access control item.

Change

Click to change a selected access control item.

Delete

Click to delete a selected access control item.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

[For more information, see the IBM Knowledge Center.](#)

ACI Owners

Use this page to add or remove groups that are authorized to configure access control items in a business unit and its subunits.

Owners table

Lists the groups that are authorized to configure access control items. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box adjacent to the group. To select all groups, select the check box at the top of the column.

Group Name

Identifies a group that can manage access control items.

Business Unit

Identifies the business unit to which the group belongs.

You can use these buttons:

Add

Click to add a group to the list.

Remove

Click to remove a selected group from the list.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Create Access Control Item

Use the **Create an Access Control Item** wizard to create an access control item for operations and permissions on system objects.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to create an access control item. Specify information about this access control item in the fields on this page.

Name

Type the name of the access control item that you are creating.

Protection Category

Select a system object category to specify permissions for a user.

Type

Displays the specific type of a specified system object category. This field is not available for some system object categories.

Apply object protection on this business unit

Specify the current business unit. Click **Search** to locate a business unit. If you select **Global operation**, the search returns only organizations.

all of its sub units

Select the check box to apply the access control item to subordinate units in the selected business unit.

Access control items for **Global operation**, **Report**, and **Recertification Policy** always apply to subordinate units. Therefore, this field is not available if you select these protection categories.

Apply protection to

If you select **Report** or **Global operation** as the protection category, this field is not available.

Select one of the following choices:

All objects in the selected category or class

Applies the access control item to all objects in a category or class.

A subset of objects that satisfies the filter criteria

Type the filtering rule that selects the objects. This field is available if you specify a subset of objects. For example, type (1=CA) to select all people with a location attribute 1 with value CA (for California).

Click **Next** to go to the next page.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Operations

Specify permissions for each operation that users are authorized to perform. The list of operations contains both custom static operations and nonstatic operations.

Operations table

Lists the operations available for the selected category. If you want all operations to have the same permission, select the permission from the **Select all permissions** list. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Operation

Specifies an operation, such as add or modify.

Permission

Identifies the permission for the operation. Select a permission from the list.

Grant

Permission is explicitly granted for performing the operation.

Deny

Permission is denied for performing the operation. Use the Deny selection sparingly, because an explicit denial overrides all other choices. Consider using the None selection instead of the Deny selection.

Generally, if a user is granted permission to view or modify an attribute, the user can also see the attribute on the user interface even if read permission is denied. For example, if an access control item grants permission to define an access group, a member of the access control item can also view the access group list, regardless of whether the operation to view group members is granted or denied.

None

The permission is not granted or denied, which is interpreted as an implicit denial.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Next** to go to the next page.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

[For more information, see the IBM Knowledge Center.](#)

Permissions

Add or remove permissions for each attribute that users are authorized to read or write. Attribute permissions are not applicable to static operations.

Attributes table

Lists the set of attributes that users are authorized to work with. If you want all attributes to have the same permission, select the permission from the **Select all read** list or **Select all write** list.

To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Attribute

Specifies an attribute of the object. For example, the attribute for a person object might be the given name of the user. For an account object, the attribute might be the maximum age that an account remains valid after a password expires.

Read

Select a permission from the list. If you set **Deny** or **None** for an attribute that is displayed in a table on the user interface, users can see the attribute. However, they cannot obtain its detailed information.

Write

Select a permission from the list.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Next** to go to the next page.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Membership

Select the focus for a specific entity access that is governed by this access control item.

The fields vary depending on the protection category that you specified on the **General** page. The protection categories are:

Account

Select one or more of the following choices as the focus for the *account* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The account owner

Select this check box to add the account owner to the membership of this access control item.

The manager of the account owner

Select this check box to add the manager of the account owner to the membership of this access control item.

The owner of the service that the account resides on

Select this check box to add the owner of the service on which the account is to the membership of this access control item.

The owner of any access defined on the service that the account is on

Select to add the owner of the access that is defined on the service on which the account is to the membership of this access control item.

The sponsor of the business partner organization in which the account resides

Select this check box to add the sponsor of the business partner organization in which the account is to the membership of this access control item.

The administrator of the domain in which the account is

Select this check box to add the administrator of the domain in which the account is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove it.

Account Default Template

Select one or more of the following choices as the focus for the *account default template* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the account default template resides

Select this check box to add the supervisor of the business unit in which the account default template is to the membership of this access control item.

The owner of the service for which account defaults are being defined

Select this check box to add the owner of the service for which account defaults are being defined to the membership of this access control item.

The owner of any access defined on the service for which account defaults are being defined

Select to add the owner of the access that is defined on the service for which account defaults are being defined to the membership of this access control item.

The sponsor of the business partner organization in which the account default template is

Select this check box to add the sponsor of the business partner organization in which the account default template is to the membership of this access control item.

The administrator of the domain in which the account default template resides

Select this check box to add the administrator of the domain in which the account default template is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Admin Domain

Select one or more of the following choices as the focus for the *admin domain* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the admin domain resides

Select this check box to add the supervisor of the business unit in which the admin domain is to the membership of this access control item.

The sponsor of the business partner organization in which the admin domain resides

Select this check box to add the sponsor of the business partner organization in which the admin domain is to the membership of this access control item.

The administrator of the admin domain

Select this check box to add the administrator of the admin domain to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove it.

Business Partner Organization

Select one or more of the following choices as the focus for the *business partner organization* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the business partner organization resides

Select this check box to add the supervisor of the business unit in which the business partner organization is to the membership of this access control item.

The sponsor of the business partner organization

Select this check box to add the sponsor of the business partner organization to the membership of this access control item.

The administrator of the domain in which the business partner organization resides

Select this check box to add the administrator of the domain in which the business partner organization is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Business Partner Person

Select one or more of the following choices as the focus for the *business partner person* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The profile owner

Select this check box to add the profile owner to the membership of this access control item.

The manager of the profile owner

Select this check box to add the manager of the profile owner to the membership of this access control item.

The sponsor of the business partner organization in which the business partner person resides

Select this check box to add the sponsor of the business partner organization in which the business partner person is to the membership of this access control item.

The administrator of the domain in which the business partner person resides

Select this check box to add the administrator of the domain in which the business partner person is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Credential**All users in the system**

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The account owner

Select this check box to add the account owner to the membership of this access control item.

The manager of the account owner

Select this check box to add the manager of the account owner to the membership of this access control item.

The owner of the service that the account resides on

Select this check box to add the owner of the service on which the account is to the membership of this access control item.

The owner of any access defined on the service that the account resides on

Select to add the owner of the access that is defined on the service on which the account is to the membership of this access control item.

The sponsor of the business partner organization in which the account resides

Select this check box to add the sponsor of the business partner organization in which the account is to the membership of this access control item.

The administrator of the domain in which the account resides

Select this check box to add the administrator of the domain in which the account is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Credential Lease**All users in the system**

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The account owner

Select this check box to add the account owner to the membership of this access control item.

The manager of the account owner

Select this check box to add the manager of the account owner to the membership of this access control item.

The owner of the service that the account resides on

Select this check box to add the owner of the service on which the account is to the membership of this access control item.

The sponsor of the business partner organization in which the account resides

Select this check box to add the sponsor of the business partner organization in which the account is to the membership of this access control item.

The administrator of the domain in which the account resides

Select this check box to add the administrator of the domain in which the account is to the membership of this access control item.

The credential lessee

Select this check box to add the credential lessee to the membership of this access control item.

The manager of the credential lessee

Select this check box to add the manager of the credential lessee to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Credential Pool**All users in the system**

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The owner of the credential pool

Select this check box to add the owner of the credential pool to the membership of this access control item.

The supervisor of the business unit in which the credential pool resides

Select this check box to add the supervisor of the business unit in which the credential pool is to the membership of this access control item.

The owner of the service that the credential pool refers to

Select this check box to add the service owner to which the credential pool refers to the membership of this access control item.

The sponsor of the business partner organization in which the credential pool resides

Select this check box to add the sponsor of the business partner organization in which the credential pool is to the membership of this access control item.

The administrator of the domain in which the credential pool resides

Select this check box to add the administrator of the domain in which the credential pool is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Dynamic Organizational Role

Select one or more of the following choices as the focus for the *dynamic organizational role* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the dynamic organizational role resides

Select this check box to add the supervisor of the business unit in which the dynamic organizational role is to the membership of this access control item.

The owners of the role

Select this check box to add one or more role owners to the membership of this access control item.

The sponsor of the business partner organization in which the dynamic organizational role resides

Select this check box to add the sponsor of the business partner organization in which the dynamic organizational role is to the membership of this access control item.

The administrator of the domain in which the dynamic organizational role resides

Select this check box to add the administrator of the domain in which the dynamic organizational role is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Global Operation

Select one or both of the following choices as the focus for the *Global operation* that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Identity Manager User

Select one or more of the following choices as the focus for the *Identity Manager user* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The Identity Manager user

Select this check box to add the Identity Manager user to the membership of this access control item.

The manager of the Identity Manager user

Select this check box to add the manager of the Identity Manager user to the membership of this access control item.

The owner of the Identity Manager service

Select this check box to add the owner of the Identity Manager service to the membership of this access control item.

The sponsor of the business partner organization in which the Identity Manager user resides

Select this check box to add the sponsor of the business partner organization in which the Identity Manager user is to the membership of this access control item.

The administrator of the domain in which the Identity Manager user resides

Select this check box to add the administrator of the domain in which the Identity Manager user is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Identity Policy

Select one or more of the following choices as the focus for the *identity policy* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the identity policy resides

Select this check box to add the supervisor of the business unit in which the identity policy is to the membership of this access control item.

The sponsor of the business partner organization in which the identity policy resides

Select this check box to add the sponsor of the business partner organization in which the identity policy is to the membership of this access control item.

The administrator of the domain in which the identity policy resides

Select this check box to add the administrator of the domain in which the identity policy is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

ITIM Group

Select one or more of the following choices as the focus for the *ITIM group* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the ITIM group resides

Select this check box to add the supervisor of the business unit in which the ITIM group is to the membership of this access control item.

The sponsor of the business partner organization in which the ITIM group resides

Select this check box to add the sponsor of the business partner organization in which the ITIM group is to the membership of this access control item.

The administrator of the domain in which the ITIM group resides

Select this check box to add the administrator of the domain in which the ITIM group is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Location

Select one or more of the following choices as the focus for the *location* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the location

Select this check box to add the supervisor of the location to the membership of this access control item.

The sponsor of the business partner organization in which the location resides

Select this check box to add the sponsor of the business partner organization in which the location is to the membership of this access control item.

The administrator of the domain in which the location resides

Select this check box to add the administrator of the domain in which the location is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Organizational Unit

Select one or more of the following choices as the focus for the *organizational unit* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the organizational unit

Select this check box to add the supervisor of the organizational unit to the membership of this access control item.

The sponsor of the business partner organization in which the organizational unit resides

Select this check box to add the sponsor of the business partner organization in which the organizational unit is to the membership of this access control item.

The administrator of the domain in which the organizational unit resides

Select this check box to add the administrator of the domain in which the organizational unit is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Password Policy

Select one or more of the following choices as the focus for the *password policy* entity access that is governed by this access control item.

All users in the system

When you select this item, all other items are unavailable.

The supervisor of the business unit in which the password policy resides

Select this check box to add the supervisor of the business unit in which the password policy is to the membership of this access control item.

The sponsor of the business partner organization in which the password policy resides

Select this check box to add the sponsor of the business partner organization in which the password policy is to the membership of this access control item.

The administrator of the domain in which the password policy resides

Select this check box to add the administrator of the domain in which the password policy is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Person

Select one or more of the following choices as the focus for the *person* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The profile owner

Select this check box to add the profile owner to the membership of this access control item.

The manager of the profile owner

Select this check box to add the manager of the profile owner to the membership of this access control item.

The sponsor of the business partner organization in which the person resides

Select this check box to add the sponsor of the business partner organization in which the person is to the membership of this access control item.

The administrator of the domain in which the person resides

Select this check box to add the administrator of the domain in which the person is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Provisioning Policy

Select one or more of the following choices as the focus for the *provisioning policy* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the provisioning policy resides

Select this check box to add the supervisor of the business unit in which the provisioning policy is to the membership of this access control item.

The sponsor of the business partner organization in which the provisioning policy resides

Select this check box to add the sponsor of the business partner organization in which the provisioning policy is to the membership of this access control item.

The administrator of the domain in which the provisioning policy resides

Select this check box to add the administrator of the domain in which the provisioning policy is to the membership of this access control item.

Users who are members of these groups

Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Recertification Policy

Select one or more of the following choices as the focus for the *recertification policy* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the recertification policy resides

Select this check box to add the supervisor of the business unit in which the recertification policy is to the membership of this access control item.

The sponsor of the business partner organization in which the recertification policy resides

Select this check box to add the sponsor of the business partner organization in which the recertification policy is to the membership of this access control item.

The administrator of the domain in which the recertification policy resides

Select this check box to add the administrator of the domain in which the recertification policy is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Report

Select one or more of the following choices as the focus for the *report* entity access that is governed by this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Separation of Duty Policy

Select one or more of the following choices as the focus for the *separation of duty policy* entity access governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The owner of the policy

Select this check box to add the policy owner to the membership of this access control item.

The supervisor of the business unit in which the separation of duty policy resides

Select this check box to add the supervisor of the business unit in which the separation of duty policy is to the membership of this access control item.

The sponsor of the business partner organization in which the separation of duty policy resides

Select this check box to add the sponsor of the business partner organization in which the separation of duty policy is to the membership of this access control item.

The administrator of the domain in which the separation of duty policy resides

Select this check box to add the administrator of the domain in which the separation of duty policy is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Service

Select one or more of the following choices as the focus for the *service* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the service resides

Select this check box to add the supervisor of the business unit in which the service is to the membership of this access control item.

The owner of the service

Select this check box to add the service owner to the membership of this access control item.

The owner of any access defined on the service

Select this check box to add the owner of the access that is defined on the service to the membership of this access control item.

The sponsor of the business partner organization in which the service resides

Select this check box to add the sponsor of the business partner organization in which the service is to the membership of this access control item.

The administrator of the domain in which the service resides

Select this check box to add the administrator of the domain in which the service is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Service Group

Select one or more of the following choices as the focus for the *service group* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the service group resides

Select this check box to add the supervisor of the business unit in which the service group is to the membership of this access control item.

The owner of the service on which the groups exist

Select this check box to add the owner of the service on which the groups exist to the membership of this access control item.

The owner of any access defined on a group

Select this check box to add the owner of the access that is defined on the group to the membership of this access control item.

The sponsor of the business partner organization in which the service group resides

Select this check box to add the sponsor of the business partner organization in which the service group is to the membership of this access control item.

The administrator of the domain in which the service group resides

Select this check box to add the administrator of the domain in which the service group is to the membership of this access control item.

Users who are members of these groups

Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Service Selection Policy

Select one or more of the following choices as the focus for the *service selection policy* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the service selection policy resides

Select this check box to add the supervisor of the business unit in which the service selection policy is to the membership of this access control item.

The sponsor of the business partner organization in which the service selection policy resides

Select this check box to add the sponsor of the business partner organization in which the service selection policy is to the membership of this access control item.

The administrator of the domain in which the service selection policy resides

Select this check box to add the administrator of the domain in which the service selection policy is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Shared Access Policy**All users in the system**

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the shared access policy resides

Select this check box to add the supervisor of the business unit in which the shared access policy is to the membership of this access control item.

The sponsor of the business partner organization in which the shared access policy resides

Select this check box to add the sponsor of the business partner organization in which the shared access policy is to the membership of this access control item.

The administrator of the domain in which the shared access policy resides

Select this check box to add the administrator of the domain in which the shared access policy is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Static Organizational Role

Select one or more of the following choices as the focus for the *static organizational role* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the static organizational role resides

Select this check box to add the supervisor of the business unit in which the static organizational role is to the membership of this access control item.

The owners of the role

Select this check box to add one or more role owners to the membership of this access control item.

The sponsor of the business partner organization in which the static organizational role resides

Select this check box to add the sponsor of the business partner organization in which the static organizational role is to the membership of this access control item.

The administrator of the domain in which the static organizational role resides

Select this check box to add the administrator of the domain in which the static organizational role is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Workflow Design

Select one or more of the following choices as the focus for the *workflow design* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the workflow design resides

Select this check box to add the supervisor of the business unit in which the workflow design is to the membership of this access control item.

The sponsor of the business partner organization in which the workflow design resides

Select this check box to add the sponsor of the business partner organization in which the workflow design is to the membership of this access control item.

The administrator of the domain in which the workflow design resides

Select this check box to add the administrator of the domain in which the workflow design is to the membership of this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Membership table

Lists the groups to which the access control item applies. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box next to the group. To select all groups, select the check box at the top of the column.

Group name

Displays the name of the group.

Description

Displays information about the intended purpose of the group.

You can use these buttons:

Add

Click to add a group to the list.

Remove

Click to remove a selected group from the list.

Click **Finish** when you complete this task.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Change Access Control Item

Use this notebook to change an access control item for general information, operations, permissions, and membership. The tabs in the notebook vary, depending on the protection category that is specified for the access control item.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to change information about an access control item, such as the name of the access control item. The fields vary, depending on the protection category that is specified for the access control item. Most fields are read-only.

Name

Type the name of the access control item.

Protection Category

Displays the type of entity to which the access control item applies.

Type

Displays the specific type of a specified system object category. This field is not available for some system object categories.

Apply object protection on this business unit

Displays a specific business unit to which this access control item applies. Click **Search** to locate a business unit. If you select **Global operation**, the search returns only organizations.

and all of its sub units

Indicates whether the access control item applies to subordinate units within the selected business unit.

Access control items for **Global operation**, **Report**, and **Recertification Policy** always apply to subordinate units. Therefore, this field is not available if you select these protection categories.

Apply protection to

If you select **Report** or **Global operation** as the protection category, this field is not available.

Indicates that protection is applied to one of the following:

All objects in the selected category or class

Apply the access control item to all objects in a category or class.

A subset of objects that satisfy the filter criteria

Use a filtering rule to select a subset of objects. For example, type (1=CA) to select all people with a location attribute 1 with value CA (for California).

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Operations

Specify permissions for each operation that users are authorized to perform. The list of operations contains both custom static operations and nonstatic operations.

Operations table

Lists the operations that you can change. If you want all operations to have the same permission, select the permission from the **Select all permissions** list. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Operation

Specifies an operation, such as add or modify.

Permission

Identifies the permission for the operation. Select a permission from the list.

Grant

Permission is explicitly granted for performing the operation.

Deny

Permission is denied for performing the operation. Use the Deny selection sparingly, because an explicit denial overrides all other choices. Consider using the None selection instead of the Deny selection.

Generally, if a user is granted permission to view or modify an attribute, the user can also see the attribute on the user interface even if read permission is denied. For example, if an access control item grants permission to define an access group, a member of the access control item can also view the access group list, regardless of whether the operation to view group members is granted or denied.

None

The permission is not granted or denied, which is interpreted as an implicit denial.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Permissions

Select a permission value for each attribute. You can add or remove permissions for each attribute that users are authorized to read or write. Attribute permissions are not applicable to static operations.

Attributes table

Lists the set of attributes that users are authorized to work with. If you want all attributes to have the same permission, select the permission from the **Select all read** list or **Select all write** list. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Attribute

Specifies an attribute of the object. For example, the attribute for a person object might be the given name of the user. For an account object, the attribute might be the maximum age that an account remains valid after a password expires.

Read

Select a permission from the list.

Write

Select a permission from the list.

You can select one of these values in the list:

Grant

Permission is explicitly granted for performing the operation.

Deny

Permission is denied for performing the operation. Use the Deny selection sparingly, because an explicit denial overrides all other choices. Consider using the None selection instead of the Deny selection. If you deny the read operation for an attribute that appears in a table on the user interface, users can see the attribute, but cannot obtain its detailed information.

Generally, if a user is granted permission to view or modify an attribute, the user can also see the attribute on the user interface even if read permission is denied. For example, if an access control item grants permission to define an access group, a member of the access control item can also view the access group list, regardless of whether the operation to view group members is granted or denied.

None

The permission is not granted or denied, which is interpreted as an implicit denial. If you implicitly deny the read operation for an attribute that appears in a table on the user interface, users can see the attribute, but cannot obtain its detailed information.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Membership

Use this page to change which users the access control item governs.

The fields vary, depending on the protection category that you specified on the **General** page. The protection categories are:

Account

Select one or more of the following choices as the focus for the *account* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The account owner

Select this check box to add the account owner to the membership of this ACI.

The manager of the account owner

Select this check box to add the manager of the account owner to the membership of this ACI.

The owner of the service that the account resides on

Select this check box to add the owner of the service on which the account resides to the membership of this ACI.

The owner of any access defined on the service that the account resides on

Select this check box to add the owner of the access that is defined on the service on which the account resides to the membership of this ACI.

The sponsor of the business partner organization in which the account resides

Select this check box to add the sponsor of the business partner organization in which the account resides to the membership of this ACI.

The administrator of the domain in which the account resides

Select this check box to add the administrator of the domain in which the account resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Account Default Template

Select one or more of the following choices as the focus for the *account default template* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the account default template resides

Select this check box to add the supervisor of the business unit in which the account default template resides to the membership of this ACI.

The owner of the service for which account defaults are being defined

Select this check box to add the owner of the service for which account defaults are being defined to the membership of this ACI.

The owner of any access defined on the service for which account defaults are being defined

Select this check box to add the owner of the access that is defined on the service for which account defaults are being defined to the membership of this ACI.

The sponsor of the business partner organization in which the account default template resides

Select this check box to add the sponsor of the business partner organization in which the account default template resides to the membership of this ACI.

The administrator of the domain in which the account default template resides

Select this check box to add the administrator of the domain in which the account default template resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Admin Domain

Select one or more of the following choices as the focus for the *admin domain* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the admin domain resides

Select this check box to add the supervisor of the business unit in which the admin domain resides to the membership of this ACI.

The sponsor of the business partner organization in which the admin domain resides

Select this check box to add the sponsor of the business partner organization in which the admin domain resides to the membership of this ACI.

The administrator of the admin domain

Select this check box to add the administrator of the admin domain to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Business Partner Organization

Select one or more of the following choices as the focus for the *business partner organization* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the business partner organization resides

Select this check box to add the supervisor of the business unit in which the business partner organization resides to the membership of this ACI.

The sponsor of the business partner organization

Select this check box to add the sponsor of the business partner organization to the membership of this ACI.

The administrator of the domain in which the business partner organization resides

Select this check box to add the administrator of the domain in which the business partner organization resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Business Partner Person

Select one or more of the following choices as the focus for the *business partner person* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The profile owner

Select this check box to add the profile owner to the membership of this ACI.

The manager of the profile owner

Select this check box to add the manager of the profile owner to the membership of this ACI.

The sponsor of the business partner organization in which the business partner person resides

Select this check box to add the sponsor of the business partner organization in which the business partner person resides to the membership of this ACI.

The administrator of the domain in which the business partner person resides

Select this check box to add the administrator of the domain in which the business partner person resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Dynamic Organizational Role

Select one or more of the following choices as the focus for the *dynamic organizational role* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the dynamic organizational role resides

Select this check box to add the supervisor of the business unit in which the dynamic organizational role resides to the membership of this ACI.

The owners of the role

Select this check box to add one or more role owners to the membership of this ACI.

The sponsor of the business partner organization in which the dynamic organizational role resides

Select this check box to add the sponsor of the business partner organization in which the dynamic organizational role resides to the membership of this ACI.

The administrator of the domain in which the dynamic organizational role resides

Select this check box to add the administrator of the domain in which the dynamic organizational role resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Global Operation

Select one or both of the following choices as the focus for the *Global operation* that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this access control item. When you select this item, all other items are unavailable.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this access control item. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Identity Manager User

Select one or more of the following choices as the focus for the *Identity Manager user* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The Identity Manager user

Select this check box to add the Identity Manager user to the membership of this ACI.

The manager of the Identity Manager user

Select this check box to add the manager of the Identity Manager user to the membership of this ACI.

The owner of the Identity Manager service

Select this check box to add the owner of the Identity Manager service to the membership of this ACI.

The sponsor of the business partner organization in which the Identity Manager user resides

Select this check box to add the sponsor of the business partner organization in which the Identity Manager user resides to the membership of this ACI.

The administrator of the domain in which the Identity Manager user resides

Select this check box to add the administrator of the domain in which the Identity Manager user resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Identity Policy

Select one or more of the following choices as the focus for the *identity policy* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the identity policy resides

Select this check box to add the supervisor of the business unit in which the identity policy resides to the membership of this ACI.

The sponsor of the business partner organization in which the identity policy resides

Select this check box to add the sponsor of the business partner organization in which the identity policy resides to the membership of this ACI.

The administrator of the domain in which the identity policy resides

Select this check box to add the administrator of the domain in which the identity policy resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

ITIM Group

Select one or more of the following choices as the focus for the *ITIM group* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the ITIM group resides

Select this check box to add the supervisor of the business unit in which the ITIM group resides to the membership of this ACI.

The sponsor of the business partner organization in which the ITIM group resides

Select this check box to add the sponsor of the business partner organization in which the ITIM group resides to the membership of this ACI.

The administrator of the domain in which the ITIM group resides

Select this check box to add the administrator of the domain in which the ITIM group resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Location

Select one or more of the following choices as the focus for the *location* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The supervisor of the location

Select this check box to add the supervisor of the location to the membership of this ACI.

The sponsor of the business partner organization in which the location resides

Select this check box to add the sponsor of the business partner organization in which the location resides to the membership of this ACI.

The administrator of the domain in which the location resides

Select this check box to add the administrator of the domain in which the location resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Organizational Unit

Select one or more of the following choices as the focus for the *organizational unit* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The supervisor of the organizational unit

Select this check box to add the supervisor of the organizational unit to the membership of this ACI.

The sponsor of the business partner organization in which the organizational unit resides

Select this check box to add the sponsor of the business partner organization in which the organizational unit resides to the membership of this ACI.

The administrator of the domain in which the organizational unit resides

Select this check box to add the administrator of the domain in which the organizational unit resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Password Policy

Select one or more of the following choices as the focus for the *password policy* entity access that is governed by this access control item.

All users in the system

When you select this item, all other items are unavailable.

The supervisor of the business unit in which the password policy resides

Select this check box to add the supervisor of the business unit in which the password policy resides to the membership of this ACI.

The sponsor of the business partner organization in which the password policy resides

Select this check box to add the sponsor of the business partner organization in which the password policy resides to the membership of this ACI.

The administrator of the domain in which the password policy resides

Select this check box to add the administrator of the domain in which the password policy resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Person

Select one or more of the following choices as the focus for the *person* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The profile owner

Select this check box to add the profile owner to the membership of this ACI.

The manager of the profile owner

Select this check box to add the manager of the profile owner to the membership of this ACI.

The sponsor of the business partner organization in which the person resides

Select this check box to add the sponsor of the business partner organization in which the person resides to the membership of this ACI.

The administrator of the domain in which the person resides

Select this check box to add the administrator of the domain in which the person resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Provisioning Policy

Select one or more of the following choices as the focus for the *provisioning policy* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the provisioning policy resides

Select this check box to add the supervisor of the business unit in which the provisioning policy resides to the membership of this ACI.

The sponsor of the business partner organization in which the provisioning policy resides

Select this check box to add the sponsor of the business partner organization in which the provisioning policy resides to the membership of this ACI.

The administrator of the domain in which the provisioning policy resides

Select this check box to add the administrator of the domain in which the provisioning policy resides to the membership of this ACI.

Users who are members of these groups

Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Recertification Policy

Select one or more of the following choices as the focus for the *recertification policy* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Report

Select one or more of the following choices as the focus for the *report* entity access that is governed by this access control item.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Separation of Duty Policy

Select one or more of the following choices as the focus for the *separation of duty policy* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The owner of the policy

Select this check box to add the policy owner to the membership of this ACI.

The supervisor of the business unit in which the separation of duty policy resides

Select this check box to add the supervisor of the business unit in which the separation of duty policy resides to the membership of this ACI.

The sponsor of the business partner organization in which the separation of duty policy resides

Select this check box to add the sponsor of the business partner organization in which the separation of duty policy resides to the membership of this ACI.

The administrator of the domain in which the separation of duty policy resides

Select this check box to add the administrator of the domain in which the separation of duty policy resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Service

Select one or more of the following choices as the focus for the *service* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the service resides

Select this check box to add the supervisor of the business unit in which the service resides to the membership of this ACI.

The owner of the service

Select this check box to add the service owner to the membership of this ACI.

The owner of any access defined on the service

Select this check box to add the owner of the access that is defined on the service to the membership of this ACI.

The sponsor of the business partner organization in which the service resides

Select this check box to add the sponsor of the business partner organization in which the service resides to the membership of this ACI.

The administrator of the domain in which the service resides

Select this check box to add the administrator of the domain in which the service resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Service Group

Select one or more of the following choices as the focus for the *service group* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the service group resides

Select this check box to add the supervisor of the business unit in which the service group resides to the membership of this ACI.

The owner of the service on which the groups exist

Select this check box to add the owner of the service on which the groups exist to the membership of this ACI.

The owner of any access defined on a group

Select this check box to add the owner of the access that is defined on the group to the membership of this ACI.

The sponsor of the business partner organization in which the service group resides

Select this check box to add the sponsor of the business partner organization in which the service group resides to the membership of this ACI.

The administrator of the domain in which the service group resides

Select this check box to add the administrator of the domain in which the service group resides to the membership of this ACI.

Users who are members of these groups

Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Service Selection Policy

Select one or more of the following choices as the focus for the *service selection policy* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the service selection policy resides

Select this check box to add the supervisor of the business unit in which the service selection policy resides to the membership of this ACI.

The sponsor of the business partner organization in which the service selection policy resides

Select this check box to add the sponsor of the business partner organization in which the service selection policy resides to the membership of this ACI.

The administrator of the domain in which the service selection policy resides

Select this check box to add the administrator of the domain in which the service selection policy resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Static Organizational Role

Select one or more of the following choices as the focus for the *static organizational role* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the static organizational role resides

Select this check box to add the supervisor of the business unit in which the static organizational role resides to the membership of this ACI.

The owners of the role

Select this check box to add one or more role owners to the membership of this ACI.

The sponsor of the business partner organization in which the static organizational role resides

Select this check box to add the sponsor of the business partner organization in which the static organizational role resides to the membership of this ACI.

The administrator of the domain in which the static organizational role resides

Select this check box to add the administrator of the domain in which the static organizational role resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Workflow Design

Select one or more of the following choices as the focus for the *workflow design* entity access that is governed by this access control item.

All users in the system

Select this check box to add all users to the membership of this ACI. When you select this item, all other items are unavailable.

The supervisor of the business unit in which the workflow design resides

Select this check box to add the supervisor of the business unit in which the workflow design resides to the membership of this ACI.

The sponsor of the business partner organization in which the workflow design resides

Select this check box to add the sponsor of the business partner organization in which the workflow design resides to the membership of this ACI.

The administrator of the domain in which the workflow design resides

Select this check box to add the administrator of the domain in which the workflow design resides to the membership of this ACI.

Users who are members of these groups

Select this check box to add users who are members of the specified groups to the membership of this ACI. Select one or more groups from the table. You can also add or remove groups. Click **Add** to add a group of users, or click **Remove** to remove a group of users.

Group Membership table

Lists the groups to which the access control item applies. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box next to the group. To select all groups, select the check box at the top of the column.

Group Name

Displays the name of the group.

Description

Displays information about the intended purpose of the group.

You can use these buttons:

Add

Click to add a group to the list.

Remove

Click to remove a selected group from the list.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Define Views

Use this page to add, change, or delete views of tasks that users can access.

Name

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Manage Views Results table

Lists the views matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a view. To select one or more views, select the check box adjacent to the view. To select all views, select the check box at the top of the column.

View Name

Identifies the name of the view. Click the name of the view to change the view details.

Description

Provides a brief description of the view.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new view.

Change

Click to change the selected view.

Delete

Click to remove the selected view from the system. You cannot delete the End User view.

Manage Custom Tasks

Click to manage customized tasks that can be defined for a view.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

View Details

Use this notebook to define the tasks that a view might provide.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to specify information about a view.

Name

Type the name of the view.

Description

Type information about the intended purpose of the view.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Configure View

Use this page to make tasks available for users who can access this view.

Click each task that you want to configure, or click the parent node to select all of its subordinate tasks.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related concepts

[Advanced Search](#)

Use this page to specify the criteria to search for an account.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage custom tasks

You can add and manage the custom tasks for your business or organization.

Custom Tasks table

Lists the custom tasks that are already created. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the check box in this column to select the managed task. Selecting the check box at the top of the column selects all access control items.

Identifier

Specifies the name of the custom task. The name is a combination of the task prefix (CUSTOM_) and the user-defined identifier suffix. Click the name of the task to change the custom task details.

Console

Identifies the console for which the task was created.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.

- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a custom task.

Change

Click to change the parameters of the selected custom task.

Delete

Click to remove the selected custom task from the system.

Related information

For more information, see the [product documentation website](#).

Create or change custom tasks

As an administrator, you can create or change custom tasks for your company or organization.

Task Information

To create or change a custom task, specify information about the custom task in the following fields.

Identifier prefix

CUSTOM_ is the predefined prefix and it cannot be changed. It is preset to prevent naming collisions with tasks that IBM provides.

Identifier suffix

Specify the name of the custom task. It cannot contain spaces, quotation marks ("), equal signs (=), or hash tags (#). The combination of the identifier prefix and identifier suffix creates the task identifier. For example, a custom task AUDIT_TAXES is identified as CUSTOM_AUDIT_TAXES with value Custom Audit Taxes. This value displays on the task card in the Identity Service Center. The field cannot be changed after the task is created.

To enable the translation of the task name, provide a translation for the task identifier as a property in ISIM_HOME/data/CustomLabels.properties.

Description

Specify the description of the custom task that you want to display on the task card. To enable the translation of the description, add a prefix \$ to the description string and provide a translation for that property in ISIM_HOME/data/CustomLabels.properties.

URL

Specify the web link that starts your custom task.

Icon

Specify the web link to the image that you want to display on the task card. For example, `http://...jpg`. In addition to setting a web link to an image, you can put the images on the WebSphere Application Server file system. For example, `.../itim/ui/custom/images/myimage.jpg`

Header category

Specify the menu that you want to display on the page header. You can also add custom tasks to the predefined menus that IBM provides.

manageAccess
requestStatusTodo

Console

Identifies the console for which the custom task was created.

Show on home page

Click this check box to display the custom task on the home page.

Start task in new window

Selecting this check box enables the user to view the custom task in a new browser window. By default, when you create a new custom task, this check box is not selected.

If you create or change a custom task without selecting this check box, when the user starts the task in the Identity Service Center, it is started in the inline frame, or iframe, of the browser window that contains the Identity Service Center. However, if you select the check box, when the user starts the task, it is started in a new browser window or tab, depending on the configuration of the browser.

Note: If you create or change a custom task that specifies a URL corresponding to the Security Identity Manager administrative console, you must select this check box.

Task Parameters

Custom tasks table

Lists the custom task parameters that are already created. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the check box in this column to select the task parameter. Selecting the check box at the top of the column selects all custom parameters.

Name

Identifies the custom task parameter.

Value

Displays the value that is assigned to the custom task parameter.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a custom task parameter.

Change

Click to change the parameters of the selected custom task parameter.

Delete

Click to remove the selected custom task parameter from the system.

Related information

For more information, see the [product documentation website](#).

Create or change custom parameters

As an administrator you can create or change custom task parameters that are applied to the custom tasks of your company or organization.

Task parameters are key/value pairs that are associated with a task. When the task is retrieved, the parameters are supplied to the console and can be used to render the task.

Parameter name

Specify or change the name of the parameter you want applied to the custom task.

Parameter value

Specify or change the value that is associated with the parameter.

Related information

For more information, see the [product documentation website](#).

Reports

Options

Use this page to complete a workflow process data report.

Note: When you generate a report, be sure to close the report window in your browser before you generate another report. If you do not close the open report window before generating another report, the data for subsequent reports might not be accurate.

Account Operations

Click this link to define the parameters for a report on account request activity.

Account Operations Performed by an Individual

Click this link to define the parameters for a report on account request activity by an individual.

Approvals and Rejections

Click this link to define the parameters for a report on approval and rejection activity.

Operation Report

Click this link to define the parameters for a report on all operations submitted by an individual.

Pending Approvals

Click this link to define the parameters for a report on pending approvals for requests.

Rejected Report

Click this link to define the parameters for a report that lists all operations submitted by an individual.

User Report

Click this link to define the parameters for a report on all requests, the set of operations that were requested, who the operations were requested for, and who requested them.

This page also indicates the last date and time that IBM Security Identity Manager data was synchronized for a report.

Related information

For more information, see the [IBM Knowledge Center](#).

Account Operations

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

Root Process

Select the type of root process.

Request Type

Specify the type of action requested on an account.

Start Date

Specify a starting date for which you want to obtain information. Use the calendar icon adjacent to the field to specify a date. The default date is one month prior to the current date.

In the resulting report, the Start Date report criteria includes a default time of 12:00 AM.

End Date

Specify an ending date for which you want to obtain information. By specifying values for this field and the **Start Date** field, you can define boundaries for the report data that is returned. Use the calendar icon adjacent to the field to specify a date. The current date is the default date.

In the resulting report, the End Date report criteria includes a default time of 11:59 PM.

Service Type

Select the service type associated with the request.

Service

Click **Search** to specify the name of the service that has requests associated with it.

If a name exists in this field, click **Clear** to specify that any service be used in generating the report.

User ID

Type a user ID for the account.

Status

Select a request status to generate a report containing only those requests of the selected status.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Account Operations Performed by an Individual

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

Submitted by

Click **Search** to specify the name of a user who submitted the request.

If a name exists in this field, click **Clear** to specify that any user be used in generating the report.

Request Type

Specify the type of action requested for an account.

Start Date

Specify a starting date for which you want to obtain information. Use the calendar icon adjacent to the field to specify a date. The default date is one month prior to the current date.

In the resulting report, the Start Date report criteria includes a default time of 12:00 AM.

End Date

Specify an ending date for which you want to obtain information. By specifying values for this field and the **Start Date** field, you can define boundaries for the report data that is returned. Use the calendar icon adjacent to the field to specify a date. The current date is the default date.

In the resulting report, the End Date report criteria includes a default time of 11:59 PM.

Service Type

Select the service type associated with the request.

Service

Click **Search** to specify the name of the service that has requests associated with it.

If a name exists in this field, click **Clear** to specify that any service be used in generating the report.

User ID

Type a user ID for the account.

Status

Select a request status to generate a report containing only those requests of the selected status.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Approvals and Rejections

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

Approver

Click **Search** to specify the name of a user who received the request for approval.

If a name exists in this field, click **Clear** to specify that any user be used in generating the report.

Start Date

Specify a starting date for which you want to obtain information. Use the calendar icon adjacent to the field to specify a date. The default date is one month prior to the current date.

In the resulting report, the Start Date report criteria includes a default time of 12:00 AM.

End Date

Specify an ending date for which you want to obtain information. By specifying values for this field and the **Start Date** field, you can define boundaries for the report data that is returned. Use the calendar icon adjacent to the field to specify a date. The current date is the default date.

In the resulting report, the End Date report criteria includes a default time of 11:59 PM.

Service Type

Select the service type associated with the request.

Service

Click **Search** to specify the name of the service that has requests associated with it.

If a name exists in this field, click **Clear** to specify that any service be used in generating the report.

User ID

Specify the user ID for which you want to obtain information.

Status

Select a request status to generate a report containing only those requests of the selected status.

Approval Activity Name

Specify the approval activity name for which you want to obtain information.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Operation Report

Use this page to narrow the scope of this report by providing search criteria.

Submitted By

Click **Search** to specify the name of a user who submitted the request.

If a name exists in this field, click **Clear** to specify that any user be used in generating the report.

Requestee

Click **Search** to specify the name of a user who received the request.

If a name exists in this field, click **Clear** to specify that any user be used in generating the report.

Operation Name

Select an operation from the list.

Start Date

Specify a starting date for which you want to obtain information. Use the calendar icon adjacent to the field to specify a date. The default date is one month prior to the current date.

In the resulting report, the Start Date report criteria includes a default time of 12:00 AM.

End Date

Specify an ending date for which you want to obtain information. By specifying values for this field and the **Start Date** field, you can define boundaries for the report data that is returned. Use the calendar icon adjacent to the field to specify a date. The current date is the default date.

In the resulting report, the End Date report criteria includes a default time of 11:59 PM.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Pending Approvals

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

Approver

Click **Search** to specify the name of a user who received the request for approval.

If a name exists in this field, click **Clear** to specify that any user be used in generating the report.

Start Date

Specify a starting date for which you want to obtain information. Use the calendar icon adjacent to the field to specify a date. The default date is one month prior to the current date.

In the resulting report, the Start Date report criteria includes a default time of 12:00 AM.

End Date

Specify an ending date for which you want to obtain information. By specifying values for this field and the **Start Date** field, you can define boundaries for the report data that is returned. Use the calendar icon adjacent to the field to specify a date. The current date is the default date.

In the resulting report, the End Date report criteria includes a default time of 11:59 PM.

Service Type

Select the service type associated with the request.

Service

Click **Search** to specify the name of the service.

If a service name exists in this field, click **Clear** to specify that any service be used in generating the report.

User ID

Specify the user ID for which you want to obtain information.

Status

Select a request status to generate a report containing only those requests of the selected status.

Approval Activity Name

Specify the approval activity name for which you want to obtain information.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Rejected Report

Use this page to narrow the scope of this report by providing search criteria.

Submitted By

Click **Search** to specify the name of a user who submitted the request.

If a name exists in this field, click **Clear** to specify that any user be used in generating the report.

Requestee

Click **Search** to specify the name of a user who received the request.

If a name exists in this field, click **Clear** to specify that any user be used in generating the report.

Start Date

Specify a starting date for which you want to obtain information. Use the calendar icon adjacent to the field to specify a date. The default date is one month prior to the current date.

In the resulting report, the Start Date report criteria includes a default time of 12:00 AM.

End Date

Specify an ending date for which you want to obtain information. By specifying values for this field and the **Start Date** field, you can define boundaries for the report data that is returned. Use the calendar icon adjacent to the field to specify a date. The current date is the default date.

In the resulting report, the End Date report criteria includes a default time of 11:59 PM.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

User Report

Use this page to narrow the scope of this report by providing search criteria.

Submitted By

Click **Search** to specify the name of a user who submitted the request.

If a name exists in this field, click **Clear** to specify that any user be used in generating the report.

Requestee

Click **Search** to specify the name of a user who received the request.

If a name exists in this field, click **Clear** to specify that any user be used in generating the report.

Start Date

Specify a starting date for which you want to obtain information. Use the calendar icon adjacent to the field to specify a date. The default date is one month prior to the current date.

In the resulting report, the Start Date report criteria includes a default time of 12:00 AM.

End Date

Specify an ending date for which you want to obtain information. By specifying values for this field and the **Start Date** field, you can define boundaries for the report data that is returned. Use the calendar icon adjacent to the field to specify a date. The current date is the default date.

In the resulting report, the End Date report criteria includes a default time of 11:59 PM.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Options

Use this page to choose the type of report on accounts that you want to run.

Note: When you generate a report, be sure to close the report window in your browser before you generate another report. If you do not close the open report window before generating another report, the data for subsequent reports might not be accurate.

Account Report

Click this link to define the parameters for a report on accounts for a business unit.

Accounts/Access Pending Recertification Report

Click this link to define the parameters for a report on pending recertifications for access definitions and accounts.

Individual Access

Click this link to define the parameters for a report on user access definitions selected by individual account owner, business unit, access, or service.

Individual Accounts

Click this link to define the parameters for a report on accounts and their owners.

Individual Accounts by Role associated with Provisioning Policy

Click this link to define the parameters for a report on accounts and their owners that have a specific role.

Recertification Change History Report

Click this link to define the parameters for a report on recertification history for access definitions and accounts.

Suspended Individuals

Click this link to define the parameters for a report on suspended users.

This page also indicates the last date and time that IBM Security Identity Manager data was synchronized for a report.

Related information

For more information, see the [IBM Knowledge Center](#).

Account Report

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

Service

Click **Search** to specify the name of the service.

If a service name exists in this field, click **Clear** to specify that any service be used in generating the report.

Business Unit

Click **Search** to specify the name of the business unit.

If a business unit name exists in this field, click **Clear** to specify that any business unit be used in generating the report.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Accounts/Access Pending Recertification Report

Use this page to provide filtering criteria and narrow the scope of this report for users who have pending recertification requests.

This report shows access/accounts that have not yet been approved or rejected during the current recertification cycle.

This report requires data to be synchronized with the directory.

Account/Access Owner

Indicates the access or account that has the selected person as owner for which you want to generate the report.

Any indicates all persons to which the login user has access.

Click **Search** to specify the name of the access or account that has pending recertification requests associated with it.

If a name exists in this field, click **Clear** to specify that any access or account be used in generating the report.

Service Type

Select a service type from the list to generate a report associated with the specified service type.

Service

Click **Search** to specify the name of the service.

If a service name exists in this field, click **Clear** to specify that any service be used in generating the report.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Individual Access

Use this page to filter the report for selected account owner, business unit, access, or service criteria.

This report requires data to be synchronized with the directory.

Account Owner

Click **Search** to specify the name of the account owner.

If an owner name exists in this field, click **Clear** to specify that any owner can be used in generating the report.

Business Unit

Click **Search** to specify the name of the business unit.

If a business unit name exists in this field, click **Clear** to specify that any business unit can be used in generating the report.

Access

Indicates the access for which you want to generate a report. **Any** indicates all access is included.

Click **Search** to specify the name of the access.

If an access name exists in this field, click **Clear** to specify that any access can be used in generating the report.

Service

Click **Search** to specify the name of the service that has access associated with it.

If a service name exists in this field, click **Clear** to specify that any service can be used in generating the report.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Individual Accounts

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

Owner

Click **Search** to specify the name of the user who owns the accounts.

If a name exists in this field, click **Clear** to specify that any user be used in generating the report.

Business Unit

Click **Search** to specify the name of the business unit.

If a name exists in this field, click **Clear** to specify that any service be used in generating the report.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Individual Accounts by Role associated with Provisioning Policy

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

This report displays accounts of users that are part of a selected role. The role must be a member of a provisioning policy.

Role

Click **Search** to specify a role. You must specify a role to generate the report.

If a role name exists in this field, click **Clear** to specify that a different role be used in generating the report.

Business Unit

Click **Search** to specify the name of the business unit.

If a business unit name exists in this field, click **Clear** to specify that any business unit be used in generating the report.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Recertification Change History Report

Use this page to provide filtering criteria and narrow the scope of this report for recertification requests.

This report shows the recertification history of accounts and user accesses, either within a specified time range or for the last time recertification occurred.

This report shows only actions taken on accounts or user accesses after running the recertification policy or the administrative recertification task. If the workflow that is associated with the recertification policy fails to run, or a participant cannot be found, the account or access is not updated and no entry is made in this report.

This report requires data to be synchronized with the directory.

Service

Indicates the service for which you want to generate the report.

Click **Search** to specify the name of the service that has recertification requests associated with it.

If a name exists in this field, click **Clear** to specify that any service be used in generating the report.

Access Type

Indicates an access type for which you want to generate the report.

Any includes access to all defined access types

Application includes access to an application such as a Web-based application

Email Group includes access to different mail groups on the corporate mail server

Shared Folder includes access to a shared folder in network storage

The list might also include custom-defined access types.

Account/Access Owner

Indicates the account or access that has the selected person as owner for which you want to generate the report.

Any indicates all persons to which the login user has access.

Click **Search** to specify the name of the access or account that has recertification requests associated with it.

If a name exists in this field, click **Clear** to specify that any access or account be used in generating the report.

Recertification Response

Indicates that the report contains the recertification with one of the following responses:

- **Any** includes all recertification
- **Approve** indicates approved recertification only
- **Approve-Timeout** indicates that the approval time interval has elapsed
- **Reject** indicates rejected recertification only
- **Reject-Timeout** indicates the rejection time interval has elapsed

Show last recertification only

Displays recertification history either between two dates or only the last recertification event.

Select **Yes** to display only the last recertification

Select **No** to display recertification history between two dates that you specify

Start Date

Specify a starting date for which you want to obtain information. Use the calendar icon adjacent to the field to specify a date. The default date is one month prior to the current date.

In the resulting report, the Start Date report criteria includes a default time of 12:00 AM.

End Date

Specify an ending date for which you want to obtain information. By specifying values for this field and the **Start Date** field, you can define boundaries for the report data that is returned. Use the calendar icon adjacent to the field to specify a date. The current date is the default date.

In the resulting report, the End Date report criteria includes a default time of 11:59 PM.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Suspended Individuals

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

Person

Click **Search** to specify the person who submitted the request.

If a name exists in this field, click **Clear** to specify that any user be used in generating the report.

Business Unit

Click **Search** to specify the name of the business unit.

If a business unit name exists in this field, click **Clear** to specify that any business unit be used in generating the report.

End Date

Specify an ending date for which you want to obtain information. Use the calendar icon adjacent to the field to specify a date. The current date is the default date.

In the resulting report, the End Date report criteria includes a default time of 11:59 PM.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Options

Use this page to complete a service data report.

Note: When you generate a report, be sure to close the report window in your browser before you generate another report. If you do not close the open report window before generating another report, the data for subsequent reports might not be accurate.

Reconciliation Statistics

Click this link to define the parameters for a report on the activities that occurred during the last completed reconciliation of a service.

Services

Click this link to define the parameters for a report on existing services.

Summary of Accounts on Service

Click this link to define the parameters for a report on accounts for a specified service.

This page also indicates the last date and time that IBM Security Identity Manager data was synchronized for a report.

Related information

For more information, see the [IBM Knowledge Center](#).

Reconciliation Statistics

Use this page to narrow the scope of this report by providing search criteria.

This report requires a reconciliation to be run on the specified services.

Service

Click **Search** to specify a service. You must specify a service to generate the report.

If a service name exists in this field, click **Clear** to specify that a different service be used in generating the report.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Services

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

Service

Click **Search** to specify the name of the service.

If a service name exists in this field, click **Clear** to specify that any service be used in generating the report.

Service Type

Select a service type from the list to generate a report associated with the specified service type.

Owner

Click **Search** to specify the name of the user who owns the services.

If an owner name exists in this field, click **Clear** to specify that any owner be used in generating the report.

Business Unit

Click **Search** to specify the name of the business unit.

If a business unit name exists in this field, click **Clear** to specify that any business unit be used in generating the report.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Summary of Accounts on Service

Use this page to narrow the scope of this report by providing search criteria.

This report requires a reconciliation to be run on the specified services and data to be synchronized with the directory.

Service

Click **Search** to specify the name of the service that has accounts associated with it.

If a service name exists in this field, click **Clear** to specify that any service be used in generating the report.

Status

Select an account status to generate a report containing only accounts of the status selected.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Options

Use this page to complete an audit and security data report.

Note: When you generate a report, be sure to close the report window in your browser before you generate another report. If you do not close the open report window before generating another report, the data for subsequent reports might not be accurate.

Access Control Information (ACIs)

Click this link to define the parameters for a report on access control items.

Access Report

Click this link to define the parameters for a report on access definitions for a service or access owner.

Audit Events

Click this link to define the parameters for a report on audit events.

Dormant Accounts

Click this link to define the parameters for a report on accounts that have not been used recently. An account that does not have last access information is not considered dormant. This includes new accounts where the last access date is blank. These types of accounts do not show up in a dormant report.

Non-Compliant Accounts

Click this link to define the parameters for a report on noncompliant accounts.

Orphan Accounts

Click this link to define the parameters for a report on accounts that are orphaned.

Policies

Click this link to define the parameters for a report on provisioning policies.

Policies Governing a Role

Click this link to define the parameters for a report on provisioning policies for a specific organizational role.

Recertification Policies Report

Click this link to define the parameters for a report on recertification policies.

Entitlements Granted to an Individual

Click this link to define the parameters for a report on provisioning policies to which users have been entitled.

Suspended Accounts

Click this link to define the parameters for a report on suspended accounts.

Separation of Duty Policy Definition Report

Click this link to define the parameters for a report on separation of duty policies.

This page also indicates the last date and time that IBM Security Identity Manager data was synchronized for a report.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Control Information (ACIs)

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

ACI Name

Indicates the name of the access control.

Context

The context to which the access control item applies.

Object Type

Indicates the object type to which the access control item applies.

ACI Scope

Indicates the extent to which the access control item applies.

Any includes all services

Single includes services in the specified business unit only

Subtree includes services in the specified business unit and all subordinate business units

Business Unit

Click **Search** to specify the name of the business unit to which the access control applies.

If a business unit name exists in this field, click **Clear** to specify that any business unit be used in generating the report.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Report

Use this page to filter the report for selected access, service, or owner criteria.

This report requires data to be synchronized with the directory.

Access Type

Indicates the type of access, such as a shared folder, application, or other access.

Access

Indicates the access for which you want to generate a report. **Any** indicates all access is included.

Click **Search** to specify the name of the access.

If an access name exists in this field, click **Clear** to specify that any access can be used in generating the report.

Service Type

Select a service type from the list to generate a report associated with the specified service type.

Service

Click **Search** to specify the name of the service that has access associated with it.

If a service name exists in this field, click **Clear** to specify that any service can be used in generating the report.

Owner

Click **Search** to specify the name of the access administration owner.

If an owner name exists in this field, click **Clear** to specify that any owner can be used in generating the report.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Audit Events

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

Event Category

Indicates the event category to which the access control applies.

Action

Indicates the action to which the access control applies.

Initiator

Click **Search** to specify the name of the person who initiated the audit event.

If a name exists in this field, click **Clear** to specify that any initiator be used in generating the report.

Start Date

Specify a starting date for which you want to obtain information. Use the calendar icon adjacent to the field to specify a date. The default date is one month prior to the current date.

In the resulting report, the Start Date report criteria includes a default time of 12:00 AM.

End Date

Specify an ending date for which you want to obtain information. By specifying values for this field and the **Start Date** field, you can define boundaries for the report data that is returned. Use the calendar icon adjacent to the field to specify a date. The current date is the default date.

In the resulting report, the End Date report criteria includes a default time of 11:59 PM.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Dormant Accounts

Use this page to narrow the scope of this report by providing search criteria.

This report requires a reconciliation to be run on the specified services and data to be synchronized with the directory. All services are not capable of generating dormant account reports.

Service

Click **Search** to specify the name of the service that has dormant accounts associated with it.

If a name exists in this field, click **Clear** to specify that any service be used in generating the report.

Dormant Period (No of days)

Type the number of days that an account must be dormant in order for it to be added to this report.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Non-Compliant Accounts

Use this page to narrow the scope of this report by providing search criteria.

This report requires a reconciliation to be run on the specified services and data to be synchronized with the directory.

Service

Indicates the name of a service.

Reason

Indicates why an account is noncompliant.

- Any
- Disallowed
- Noncompliant

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Orphan Accounts

Use this page to narrow the scope of this report by providing search criteria.

This report requires a reconciliation to be run on the specified services and data to be synchronized with the directory.

Service

Click **Search** to specify the name of the service that has orphan accounts associated with it.

If a service name exists in this field, click **Clear** to specify that any service be used in generating the report.

Account Status

Select an account status to generate a report containing only accounts of the status selected.

- Any
- Active
- Inactive

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Policies

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

Provisioning Policy Name

Type the name of the provisioning policy for which you want to generate a report.

The filter input for this report uses the LIKE database operator, which is case-sensitive. Therefore, typing A* gives different results than typing a* as the input value.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Policies Governing a Role

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

Role

Click **Search** to select a role such as an administrator role.

If a role name exists in this field, click **Clear** to specify that any role is used.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Recertification Policies Report

Use this page to provide filtering criteria and narrow the scope of this report for recertification policies.

Note: If there are multiple recertification policies with same name, data for those policies are displayed in the same report.

This report shows the recertification policy configuration for the selected service. This report requires data to be synchronized with the directory.

Recertification Policy Target Type

Indicates the target type for which you want to generate the recertification policies report.

- **Any** includes all target types
- **Access Entitlement** indicates an access target
- **Accounts on Service** indicates a service target

Service Type

Indicates the service type for which you want to generate the report.

Click **Search** to specify the name of the service type.

If a name exists in this field, click **Clear** to specify that any service type be used in generating the report.

If you select **Access Entitlement** as the recertification policy target type, this field is not considered in report generation .

Service

Indicates the name of the service for which you want to generate the report.

Click **Search** to specify the name of the service.

If a name exists in this field, click **Clear** to specify that any service be used in generating the report.

If you select **Access Entitlement** as the recertification policy target type, this field is not considered in report generation .

Access Type

Indicates the type of access:

- Any
- Application
- Email Group
- Shared Folder

If you select **Accounts on Service** as the recertification policy target type, this field is not considered in report generation .

Access

Identifies the access definition for which you want to generate the report.

If you select **Accounts on Service** as the recertification policy target type, this field is not considered in report generation .

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Entitlements Granted to an Individual

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

Person

Click **Search** to specify the person who submitted the request.

If a name exists in this field, click **Clear** to specify that any user be used in generating the report.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Suspended Accounts

Use this page to narrow the scope of this report by providing search criteria.

This report requires data to be synchronized with the directory.

User ID

Indicates the user ID for which you want to generate the report.

Person

Indicates the person for which you want to generate the report.

Click **Search** to specify the person.

If a name exists in this field, click **Clear** to specify that any user be used in generating the report.

Service Type

Indicates the service type for which you want to generate the report.

Service

Indicates the service for which you want to generate the report.

Click **Search** to specify the name of the service.

If a service name exists in this field, click **Clear** to specify that any service be used in generating the report.

End Date

Specify an ending date for which you want to obtain information. Use the calendar icon adjacent to the field to specify a date. The current date is the default date.

In the resulting report, the End Date report criteria includes a default time of 11:59 PM.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Separation of Duty Policy Definition

Use this page to provide filtering criteria and narrow the scope of this report for various separation of duty policies.

This report shows various separation of duty policies based on policy name and business unit.

<i>Table 9. Separation of duty policy definition report</i>	
Name	Separation of Duty Policy Definition
Description	A report that lists various separation of duty policies.
Parameters	Enables filtering based on policy name and business unit. The policy name, and business unit parameters must be selected from their respective menus.

Separation of Duty Policy Detail Definition

This report lists owner, rules, and roles associated with a separation of duty policy.

Options

Use this page to generate a custom report that has been designed using the Design Report task. Click the report name to generate the report.

Note: When you generate a report, be sure to close the report window in your browser before you generate another report. If you do not close the open report window before generating another report, the data for subsequent reports might not be accurate.

Related information

For more information, see the [IBM Knowledge Center](#).

Custom Report

Use this page to narrow the scope of this report by providing search criteria and selecting the output format of the report.

Format

Indicates whether the output format of the report is PDF or comma-separated value (CSV) format.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Entity Attributes

Use this page to select entity attributes for use in customized reports.

Entities

Select a IBM Security Identity Manager system entity for which you want to generate the report.

Unmapped Attributes

Identifies unmapped attributes that are associated with the selected entity.

Mapped Attributes

Identifies mapped attributes that are associated with the selected entity.

Use these buttons:

Add

Click to add an attribute to the mapped attributes schema.

Remove

Click to remove an attribute from the mapped attributes schema.

Related information

For more information, see the [IBM Knowledge Center](#).

Custom Report Template

Use this page to create, delete, or import a report template.

Lists the report templates that you can modify or delete. You can also create report templates and add them to this table. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a report template to which the **Delete** button applies. To select one or more report templates, select the check box adjacent to the report template. To select all report templates, select the check box at the top of the column.

Report Name

Identifies the name of a report template.

Click the report name to modify the template.

Note: The report name is treated as a key that is localized. If a localized value is available for the report name, then the localized value is displayed in the Design Report task and in the generated report. If a localized value is not available for the report name, then the report name is displayed the same way that you typed it in this field.

Report Type

Identifies which report designer was used to create the report.

Designer identifies report templates that are created using the IBM Security Identity Manager report designer.

Display Category

Indicates one of the following categories to which the report template applies:

- Requests
- User and Account
- Services
- Audit and Security
- Custom

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a report template and adds it to the table.

Delete

Click to remove the selected report template from the table.

Import

Click to import a report template.

Related information

For more information, see the [IBM Knowledge Center](#).

Design Report

Use this notebook to create or change a report template.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to specify general information about a report.

Report Name

Identifies the name of a report template.

Click the report name to modify the template.

Note: The report name is treated as a key that is localized. If a localized value is available for the report name, then the localized value is displayed in the Design Report task and in the generated report. If a localized value is not available for the report name, then the report name is displayed the same way that you typed it in this field.

Include generated date and time

Select this check box to include the report generation date and time in the report header.

Include generated by user information

Select this check box to include the name of the user who generated the report in the report header.

Show paging information (Page n of m)

Select this check box to include the page numbers in the report header.

Stylesheet

Select the stylesheet to be used by the report.

Report category

Select one of the following categories for the report:

- **Custom** reports are reports that you define.
- **Audit and Security** reports are security and policy reports.
- **Requests** reports are workflow or history reports.
- **Service** reports are additional request-based and account-based reports that are service-specific.
- **User and Accounts** reports are snap shots of the LDAP directory at reporting time.

The category determines where the reporting link is displayed in the task portfolio.

Use these buttons:

Apply

Click to save your changes and continue.

Preview

Click to open a new browser window containing a preview of the report.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Contents

Use this page to add or remove attributes that are displayed as columns of data in a report.

Note: When you, as an administrator, create a custom report, you must also manually create report ACIs and entity ACIs for that custom report. This allows users that are not administrators, such as auditors, to run the custom report and to view data in the custom report.

To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies the attribute to which the **Remove** button applies. To select one or more attributes, select the check box adjacent to the attribute. To select all attributes, select the check box at the top of the column.

Report Column

Indicates the column to be included on the report. Columns represent attributes of a reportable IBM Security Identity Manager entity.

Sort

Indicates whether the column is used for sorting and how the report is sorted by this column. For columns such as `access.type`, which contain keys as values and not as data, sort is not applicable.

Ascending indicates that the column is sorted in ascending order.

Descending indicates that the column is sorted in descending order.

None indicates that the column is not used for sorting.

Sort Order

Indicates the order in which the column is sorted with other columns of data in the report. For columns such as `access.type`, which contain keys as values and not as data, sort order is not applicable.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add an attribute in the mapped schema to be reported as a column in the report.

Remove

Click to remove the selected attribute from the table.

Apply

Click to save your changes and continue.

Preview

Click to open a new browser window containing a preview of the report.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Filter

Apply filter conditions (query statements) to reports to customize the report results according to your requirements. Filter conditions are useful when you have large and complex report schema tables.

Current filter

Contains filters that you can use for generating a custom report. However, it is not mandatory to apply filters to a report.

Function

Provides a list of functions that you can apply to a row in a report:

- None: No character casing must be applied.
- Lower: Lowercase character casing must be applied.
- Upper: Uppercase character casing must be applied.

Entity

Provides a list of report schema tables that are defined by using Security Identity Manager.

Attribute

Provides a list of attributes that are mapped with the entity that you selected earlier. Attributes appear as column names in the report.

Operator

Provides a list of relational operators. Use the following operators to define a relation between two entities:

- Equals
- Like

- Greater than
- Not equal to
- Greater than or equal to
- Less than
- Not like
- Less than or equal to

Note: The Like operator is case-sensitive.

Condition

Provides a list of conditions to use for constructing query statements:

- None: Indicates that no more filter condition can be added to the report.
- AND: Generates results only if all the specified filter conditions meet.
- OR: Generates results if either of the specified filter conditions meet.

Use these buttons:

Add Row

Click this button add the query statement that you defined as a row in the current filter.

Apply

Click to save your changes and continue.

Preview

Click this button to preview the report in a new browser window.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Report Column Details

Use this page to add an attribute from a mapped schema to a report.

Apply Case

Select the option to apply to the column. The available options are:

None does not convert the case of a string.

Lower converts a string to all lowercase characters.

Upper converts a string to all uppercase characters.

Entity

Select an entity from the list, which contains the report schema tables that are defined using the Design Schema task.

Attribute

Select an attributes from the list, which contains the mapped attributes of the selected report schema table.

Column Width

Type an integer value for the maximum width in characters for the column displayed in the report.

Sort

Click a radio button to specify whether the column is used for sorting and how the report is sorted by this column. The available sorting options are:

None indicates that the column is not used for sorting.

Ascending indicates that the column is sorted in ascending order.

Descending indicates that the column is sorted in descending order.

Sort Order

Specify the order in which the column is sorted with other columns of data in the report. This field is not visible when the **None** option is selected from the **Sort** list.

Related information

For more information, see the [IBM Knowledge Center](#).

Data Synchronization

Use this page to manage schedules for data synchronization.

Lists the schedules for synchronizing system data.

Select

Specify a synchronization schedule that you want to delete. To select one or more synchronization schedules, select the check box adjacent to the synchronization schedule. To select all synchronization schedules, select the check box at the top of the column.

Schedule

Describes the defined schedule for data synchronization.

Click the description of the schedule, to modify an existing synchronization schedule.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Next scheduled synchronization

Indicates the day of week, date, and time of the next scheduled synchronization.

Data validity (as of)

Indicates the day of week, date, and time of the most recent valid data synchronization.

Status

Indicates whether or not the most recent data synchronization was successful.

You can use these buttons:

Create

Click to add a data synchronization schedule to the table.

Delete

Click to remove the selected data synchronization schedule from the table.

Run Synchronization Now

Click to perform an immediate synchronization of system data.

Refresh Synchronization Status

Click to refresh the synchronization status information.

Related information

For more information, see the [IBM Knowledge Center](#).

Synchronization Schedule

Use this page to create or modify schedules for data synchronization.

The fields displayed depend on the scheduling option that is selected. Select one of these schedule intervals to synchronize data on the system:

Daily

Synchronizes data every day. After you select this option, click the clock icon to specify a time in the **At this time** field.

Weekly

Synchronizes data once a week. After you select this option, select a day from the **On this day of the week** list and click the clock icon to specify a time in the **At this time** field.

Monthly

Synchronizes data once a month. After you select this option, select a date from the **On this day of the month** list and click the clock icon to specify a time in the **At this time** field.

Hourly

Synchronizes data once an hour. After you select this option, select a time from the **At this time** list.

Annually - On a specific day of the year

Synchronizes data on a specific date and time. After you select this option, select a month from the **Month** list. Then select a date from the **On this day of the month** list and click the clock icon to specify a time in the **At this time** field.

During a specific month

Synchronizes data on a specific month, day, and time. After you select this option, select a month from the **Month** list. Then select a day from the **On this day of the week** list and click the clock icon to specify a time in the **At this time** field.

Related information

For more information, see the [IBM Knowledge Center](#).

Configure System

Manage Service Types

Use this page to create, import, change, or delete service types.

Service Types table

Lists the available service types. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:


Select

Specifies a service type. To select one or more service types, select the check box adjacent to the service type. To select all service types, select the check box at the top of the column.

Service Type

Identifies the name of the service type.

Click the name of the service type to view and change the service type details.

Click the icon () adjacent to the service type to show the tasks that can be performed on the service type. The task that you can perform is dependent on the service type.

Use these menu items to perform a task on the selected service:

Change

Changes a selected service type.

Delete

Deletes the selected service type. If a service instance exists of that service type, you cannot delete a service type .

Account Defaults

Manages account default attributes.

Description

Provides additional identification of the service type.

Status

Indicates whether a service definition profile is available, or the profile import is being processed, or the profile import failed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new service type.

Import

Click to import a service definition profile to create a new service type.

Change

Click to change a selected service type.

Delete

Click to delete the selected service type. You cannot delete a service type if a service instance exists of that service type.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Service Types

Use this notebook to specify information for a service type.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to specify information about a service type.

Service Type Name

Type the name of the service type. The service type name must contain fewer than 227 characters.

If you are changing a service type, you cannot change the service type name.

The CustomLabels.properties resource bundle already contains some predefined values for the **Service Type Name** field. For example, if you type `st` in the **Service Type Name** field, the predefined value in the CustomLabels.properties resource bundle is `State`.

If you do not want to use a predefined value from the CustomLabels.properties resource bundle, you must type the number sign (`#`) before a service type name. For example, if you type `#st` in the **Service Type Name** field, the service type name is interpreted as `st`. In this case, the literal value that you type is the actual service type name and not the predefined value that is stored in the CustomLabels.properties resource bundle.

Description

Displays the information about the purpose of the service type. Even if you are creating a new service type, you cannot change the description.

Service Provider

Select the protocol that IBM Security Identity Manager uses to provision accounts for that service type:

Directory Integrator Adapter

Select Directory Integrator Adapter to specify that this service communicates with IBM Security Directory Integrator for information.

Manual

Select Manual to specify that this service requires a manual operation in response to a work order activity.

Custom Java class

Type the fully qualified name of the Java class that implements the `com.ibm.itim.remoteservices.provider.ServiceProviderFactory` interface.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Service

Use this page to add, change, or remove an LDAP class and LDAP attributes that represent the information that IBM Security Identity Manager associates with a service instance. For example, an attribute might represent the administrative user ID and administrative password on a managed resource, or the Universal Resource Locator (URL) of the resource.

LDAP class

Type the LDAP class for the service type in this field. If you do not know the name of the LDAP class, click **Search** to select an LDAP class from a list.

The LDAP class cannot be a super class of any other class, and it cannot already be used by another service type.

OID

Type the value of an object identifier (OID) if you use your own registered OID. Otherwise, the system automatically generates an OID.

Super class

Click **Search** to specify the parent LDAP class from which to obtain attributes. After attributes are obtained for a super class, entering another super class removes the previous inherited attributes from the working list. However, any custom attributes remain in the working set.

Attributes table

Lists the LDAP attributes for the service type. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an attribute. To select one or more attributes, select the check box adjacent to the attribute. To select all attributes, select the check box at the top of the column.

Attributes that are inherited from the super class cannot be changed or removed.

Attribute Name

Displays the name of the schema attribute. Click the attribute name to update the attribute in the service schema.

Required

Identifies whether this attribute is a required attribute.

Multi-Valued

Identifies whether the value of the attribute can contain multiple values.

Syntax

Identifies the type of value that the attribute can contain, such as binary or integer.

When there are two or more LDAP classes that refer to the same attribute definition, the syntax cannot be changed if the syntax is binary.

You can use these buttons:

Add

Click to add an attribute to the service type.

Change

Click to modify the selected attribute. If a service instance exists, you cannot change an attribute.

Remove

Click to remove the selected attribute. If a service instance exists, you cannot remove an attribute.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Account

Use this page to add, change, or remove an LDAP class and LDAP attributes for the account schema. The class and attributes vary, depending on accounts that the managed resource provides.

LDAP class

Type the LDAP class for the service type in this field. If you do not know the name of the LDAP class that you want to use, click **Search** to select an LDAP class from a list.

OID

Type the value of an object identifier (OID) if you use your own registered OID. Otherwise, the system automatically generates an OID.

The LDAP class cannot be a super class of any other class, and it cannot already be used by another service type.

Super class

Click **Search** to specify the parent LDAP class from which to obtain attributes. After attributes are obtained for a super class, entering another super class removes the previous inherited attributes from the working list. However, any custom attributes remain in the working set.

Attributes table

The **Attributes** table contains the LDAP attributes for the service type. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an attribute. To select one or more attributes, select the check box adjacent to the attribute. To select all attributes, select the check box at the top of the column.

Attributes that are inherited from the super class cannot be changed or removed.

Attribute name

Displays the name of the schema attribute. Click the attribute name to update the attribute in the account schema.

Required

Identifies whether this attribute is a required attribute.

Multi-Valued

Identifies whether the value of the attribute can contain multiple values.

User ID

Indicates which attribute represents the user ID attribute for the account.

Use these buttons:

Add

Click to add an attribute to the service type.

Change

Click to modify the selected attribute. You cannot change an attribute if a service instance exists.

Remove

Click to remove the selected attribute. You cannot remove an attribute if a service instance exists.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Group

Use this page to add, change, or remove a group that is associated with a service type.

Lists the groups that are associated with the service type. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box next to the group. To select all groups, select the check box at the top of the column.

Group Name

Displays the name of the group.

You can use these buttons:

Add

Click to add a group to the service type.

Change

Click to modify the selected group. If a service instance exists, you cannot change a group .

Remove

Click to remove the selected group. If a service instance exists, you cannot remove a group.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Miscellaneous

Use this page to configure additional information for a service type.

Include service type in dormant account reporting

Select this check box to indicate that the service type participates in reports for dormant accounts.

Last access date

Indicates the account attribute of the service type that is used for dormant account reporting. Use the list box to select an attribute of the account schema that is associated with the service type.

This field is inactive when the service type does not participate in dormant account reporting.

Click other tabs to specify additional information.

Related information

For more information, see the [IBM Knowledge Center](#).

Add Group

Use this page to add a group that is associated with a service type.

LDAP class

Click **Search** to specify the LDAP class from which to obtain attributes.

The LDAP class cannot be a super class of any other class, and it cannot already be used by another service type.

OID

Indicates the value of the object identifier (OID) for the LDAP class.

Super class

Indicates the parent LDAP class.

Group ID

Select a group ID from the list.

Group name

Select a group name from the list.

Group description

Select a group description from the list.

Account attribute for this group

Select an account attribute from the list.

Related information

For more information, see the [IBM Knowledge Center](#).

Change Group

Use this page to change a group that is associated with a service type.

LDAP class

Indicates the LDAP class that is selected.

OID

Indicates the value of the object identifier (OID) for the LDAP class.

Super class

Indicates the parent LDAP class.

Group ID

Select a group ID from the list.

Group name

Select a group name from the list.

Group description

Select a group description from the list.

Account attribute for this group

Select an account attribute from the list.

Related information

For more information, see the [IBM Knowledge Center](#).

Select LDAP Class

Use this page to select an LDAP class.

Object class name

Type the name of an LDAP class in the field, or click **Search** to locate the class.

LDAP Class table

Lists the object classes matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select this radio button to select an object class.

Object Class Name

Identifies the name of the LDAP object class.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a Super Class

Use this page to select a super class that serves as a template for subclasses. The subclasses inherit the characteristics of the super class.

Object class name

Type the name of an LDAP class in the field, or click **Search** to locate the class.

Super Class table

Lists the object classes matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select this radio button to select an object class.

Object Class Name

Identifies the name of the LDAP object class.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Add Attribute to Custom Service Schema

Use this page to add an attribute to the schema for the service type.

Attribute name

Type the name of the schema attribute, or click **Search** to locate an existing attribute from the schema.

When you specify a label name for this attribute in the CustomLabels.properties file, the label name must be specified in lowercase letters. The value of the label does not need to be lowercase, but the label name must be lowercase. For example, to specify an attribute name of "MyAttribute," in the CustomLabels.properties file, type: myattribute="MyAttribute". If the label name does not contain all lowercase letters, the value of the label might not be displayed correctly in the user interface.

Search

Finds an existing attribute from the schema.

OID

Indicates the value of an object identifier (OID).

Required

Identifies whether this attribute is a required attribute.

Multi-Valued

Identifies whether the value of the attribute can contain multiple values.

Syntax

Identifies the type of value that the attribute can contain, such as binary or integer.

When there are two or more LDAP classes that refer to the same attribute definition, the syntax cannot be changed if the syntax is binary.

Related information

For more information, see the [IBM Knowledge Center](#).

Change Custom Service Schema Attribute

Use this page to change an attribute to the schema for the service type.

Attribute name

Type a new name for the schema attribute.

When you specify a label name for this attribute in the CustomLabels.properties file, the label name must be specified in lowercase letters. The value of the label does not need to be lowercase, but the label name must be lowercase. For example, to specify an attribute name of "MyAttribute," in the CustomLabels.properties file, type: myattribute="MyAttribute". If the label name does not contain all lowercase letters, the value of the label might not be displayed correctly in the user interface.

Clear

Clears the name of the schema attribute and all dependent data for this attribute.

Search

Finds an existing attribute from the schema.

OID

Indicates the value of an object identifier (OID).

Required

Identifies whether this attribute is a required attribute.

Multi-Valued

Identifies whether the value of the attribute can contain multiple values.

Syntax

Identifies the type of value that the attribute can contain, such as binary or integer.

When there are two or more LDAP classes that refer to the same attribute definition, the syntax cannot be changed if the syntax is binary.

Related information

For more information, see the [IBM Knowledge Center](#).

View Attribute

Use this page to view an attribute for the service type.

Attribute name

Displays the name of the schema attribute.

OID

Indicates the value of an object identifier (OID).

Required

Identifies whether this attribute is a required attribute.

Multi-Valued

Identifies whether the value of the attribute can contain multiple values.

Syntax

Identifies the type of value that the attribute can contain, such as binary or integer.

When there are two or more LDAP classes that refer to the same attribute definition, the syntax cannot be changed if the syntax is binary.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Attribute

Use this page to select a name attribute for the system entity.

Attributes table

Lists the LDAP schema attributes that are associated with the corresponding LDAP class. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates which attribute is selected.

Attribute Name

Identifies the name of the LDAP schema attribute that is associated with the corresponding LDAP class.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Attribute

Use this page to select a name attribute for the system entity.

Object class name

Type the name of an LDAP class in the field, or click **Search** to locate the class.

Attributes table

Lists the LDAP schema attributes that are associated with the corresponding LDAP class. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates which attribute is selected.

Attribute Name

Identifies the name of the LDAP schema attribute that is associated with the corresponding LDAP class.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Import Service Type

Use this page to import the service definition file or adapter profile and to create a service type for the managed resource.

Service Definition File

Type the name of the file to import, or click **Browse** to locate the file.

Click **OK** to import the service definition file. The import occurs asynchronously, which means it might take some time for the service type to load into IBM Security Identity Manager from the properties files and to be available in other pages.

After you import a service type, on the **Manage Service Types** page, click **Refresh** to see the new service type. If the service type is not displayed within a reasonable amount of time, check the log files to determine why the import failed.

Related information

For more information, see the [IBM Knowledge Center](#).

Global Adoption Policies

Use this page to create, change, or delete global adoption policies.

Global Adoption Policies table

Lists the adoption policies that are configured in the system. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an adoption policy. To select one or more adoption policies, select the check box adjacent to the adoption policy. To select all adoption policies, select the check box at the top of the column.

Adoption Policy Name

Identifies the name of the adoption policy. Click the name to change the adoption policy.

Adoption Policy Description

Provides additional information for the adoption policy.

Service Type

Names the service types to which the adoption policy applies. An asterisk (*) indicates all service types.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to creates a new adoption policy.

Change

Click to change the selected adoption policy.

Delete

Click to delete the selected adoption policy.

Related information

[For more information, see the IBM Knowledge Center.](#)

Global Adoption Policies

Use this notebook to specify information about a global adoption policy.

Related information

[For more information, see the IBM Knowledge Center.](#)

General

Use this page to specify general information about a global adoption policy.

Name

Specify the name of the global adoption policy. You must specify a name for the global adoption policy.

Description

Provide additional information about the intended purpose of the global adoption policy.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related information

[For more information, see the IBM Knowledge Center.](#)

Service Type

Use this page to select the service type to which the global adoption policy applies. You must specify at least one service type for the global adoption policy. You cannot associate more than one global adoption policy with a service type.

Service Types table

Lists the service types that apply to the adoption policy. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service type. To select a service type, click the radio button adjacent to the service type to which the global adoption policy applies.

Service Type

Identifies the type of service.

Description

Provides additional information for the service type.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related information

[For more information, see the IBM Knowledge Center.](#)

Rule

Use this page to specify the attributes that the rule uses to match accounts to users.

Specify rule by

Select how you want to specify the rule:

Defining Matches

Select this option to define a rule matching the account attributes directly to person attributes.

After you select this option, select one or more account attributes to match to a user attribute. Click **Add a match field** to specify additional matching criteria for the rule.

Account attribute matches

Select an account attribute from the list. During reconciliation, the value of the account attribute is compared to the value of the user attribute.

User attribute

Select a user attribute from the list. During reconciliation, the value of this user attribute is compared to the value of an attribute of an account on a managed resource.

Remove

Click to remove a matching pair of attributes.

Providing a Script

Select this option to define a custom rule by entering a script.

After you select this option, type a script to define a custom rule matching account attributes to user attributes.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related information

For more information, see the [IBM Knowledge Center](#).

Workflow Notification Properties

Use this page to specify the time intervals for escalation and reminders, and to change e-mail notification templates.

Escalation Limit

The interval of time that elapses before escalating a notification used for workflow events, such as approvals and work orders.

The default interval value is one day. The escalation limit interval cannot be set to less than one day because the system-wide default interval for workflow escalation is one day.

If the value for the escalation limit is specified in the Workflow Designer, then that value overrides the value that is specified in this field. When the escalation limit is reached, the workflow event is moved from the workflow participant to the escalation participant.

Reminder Interval

The number of days that elapses before a notification reminder is sent to the workflow participant. The number of days in this field should be less than the number of days specified in the **Escalation limit** field.

E-mail Notification Templates

Lists the templates that are used for workflow notifications. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a notification template. To select one or more notification templates, select the check box adjacent to the notification template. To select all notification templates, select the check box at the top of the column.

Name

Identifies the name of an e-mail template.

Status

Indicates the status of the corresponding notification template.

- **Enabled** indicates that e-mail notification is sent when the system event occurs.
- **Disabled** indicates that e-mail notification is *not* sent when the system event occurs.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons and menu items:

Change

Click to change the e-mail that the notification sends.

Enable

Click to set the status of the corresponding notification template to **Enabled**.

Disable

Click to set the status of the corresponding notification template to **Disabled**.

Related information

For more information, see the [IBM Knowledge Center](#).

Notification Template

Use this page to add or change information for an e-mail notification template.

Template name

Identifies the name of the notification template.

Subject

Identifies the subject of the mail that is generated, using the template.

Plaintext body

Contains the main content of the notification message. The content in this section cannot contain XHTML content, but it can contain dynamic content tags.

XHTML body

Contains the XHTML body of the notification message. The content in this section can include images and hyper links.

Related information

For more information, see the [IBM Knowledge Center](#).

Post Office

Use this page to store e-mails and forward the collection as a single e-mail.

Enable store forwarding

Indicates whether e-mail aggregation is enabled. Select this check box to store, all e-mail notifications until the time specified in the **Collection Interval** field. At that time, the notifications are aggregated into one e-mail and sent to the recipients. Clear this check box to have e-mail notifications sent to recipient as they are generated.

Collection interval

Indicates the interval in minutes to store e-mail before sending an aggregate e-mail.

The value of the collection interval must be an integer between 5 and 10080.

Subject

Type the subject line of the notification for the e-mails that are stored and then forwarded. Do not enter any new lines in this field.

Plaintext body

Type the main content of the e-mail notification.

XHTML body

Specify the dynamic content of the e-mail notification.

Click the **Test** button to specify an e-mail address to receive a test message.

Related information

For more information, see the [IBM Knowledge Center](#).

Test E-mail

Use this page to send a test message to an e-mail address.

E-mail Address

Identifies the address to receive a test e-mail notification.

Click **Test** to send the test message.

Related information

For more information, see the [IBM Knowledge Center](#).

Design Forms

Use this page and the Java applet to design forms for the attributes that are displayed on the IBM Security Identity Manager interface.

Related information

For more information, see the [IBM Knowledge Center](#).



Form designer interface

Use the work areas in the form designer applet to design custom forms on form templates, tabs, and attributes.

The form designer interface has these work areas:

Menu and toolbar buttons

Use the menu bar and toolbar buttons to work on form templates, tabs, and attributes. Place the mouse cursor over a toolbar button to view its function or action. You can also select some of these actions from a menu when you right-click an attribute. The following menu items and toolbar buttons are available:

Menu bar	Menu item	Toolbar button	Action
Click Form to open, save, or reset a form template to the last saved design.	Open Form Template		Opens the form template from the form category folders.
	Save Form Template		Saves the form template that is currently open.
	Reset Form Template	None	Resets the form template to the last saved design.











<i>Table 10. Form designer applet menu and toolbar buttons (continued)</i>			
Menu bar	Menu item	Toolbar button	Action
Click Tab to add, rename, delete, or shift a tab left or right in the interface. Tabs are shown in the Template Attributes work area of the form designer applet. The tab names in the form designer correspond to the tab names in the resulting notebook forms in the IBM Security Identity Manager interface.	Add Tab		Adds a container for grouping form elements.
	Rename Tab	None	Renames an existing tab container.
	Delete Tab		Deletes an existing tab from the form template.
	Shift Tab Left		Shifts an existing tab container to the left.
	Shift Tab Right		Shifts an existing tab container to the right.
Click Attribute to edit, delete, move an attribute up or down in the interface, or change the control type of an attribute. Attributes are shown in the Template Attributes work area of the form designer applet.	Edit Attribute	None	You can edit and configure an attribute.
	Delete Attribute		Removes an attribute from a form template.
	Move Up Attribute		Repositions the attribute up 1 space in the attribute list of the form template.
	Move Down Attribute		Repositions the attribute down 1 space in the attribute list of the form template.
	Change To	None	You can change the selected attribute control type to a newly selected control type. Possible control types are: <ul style="list-style-type: none"> CheckBox Date DropDown Box Editable Text List ListBox LoginHours Password Password Popup Search Control Search Match SubForm TextArea TextField UMask

Table 10. Form designer applet menu and toolbar buttons (continued)			
Menu bar	Menu item	Toolbar button	Action
Click View to select various interface viewing options, such as floating work areas or viewing the source of the form template.	Float Attribute List		Moves the attribute list from the form designer to a floating pop-up window.
	Float Property		Moves the property list from the form designer to a floating pop-up window.
	View Source		Opens a pop-up window that shows the XML source for the form template.
Click Theme to select an interface theme for the form designer applet.	Default Theme	None	Applies the default menu theme to the form designer interface.
	High Contrast, Big Font Theme	None	Applies a large font and high contrast colors to the form designer interface.
	High Contrast Theme	None	Applies high contrast colors to the form designer interface.

Categories

Use the left pane of the form designer to select a category, such as Account, Organization, or Service. Each form category has associated object profiles that represent system entities. Each object profile is associated with a form template.

Double-click a category folder to expand the list of available form templates for that category. Loading the list of form templates might take some time. The list of form templates for some categories varies, depending on service types.

Double-click a form template to open it.

Template Attributes

Use the middle pane of the form designer to view and change the active attributes for a selected form template. Right-click the attribute to show the available actions for that attribute. Possible actions are:

- Change To
- Move To Tab
- Rename Tab
- Move Up Attribute
- Move Down Attribute
- Edit Attribute
- Delete Attribute

For example, a Service form template has a \$serviceName attribute. To change the control type that is associated with an attribute, right-click the attribute and select **Change To** from the list. Then, select the control type that you want to use.

Attribute List

Use this list to view all of the attributes for the selected object that are not currently included on the form. You can sort the list in ascending or descending order. You can also add attributes from this list to the list of active template attributes. For example, an Organization object has additional attributes, such as \$postalcode, which you might add to the list of active template attributes.

Properties

Contains **Format** and **Constraint** tabs, which specify data type and other parameters for a specific attribute. For example, the data type for a \$servicename attribute is Directory String, and it is a required attribute.

Related information

For more information, see the [IBM Knowledge Center](#).

Control types used by the form designer

Use control types in the form designer applet to specify how users enter a value for an attribute.

CheckBox



Assigns a single check box as the data gathering field. This control type is typically used for attributes that are Boolean in nature.

Date



Provides a calendar pop-up window that allows users to select the desired date. This control type has additional attributes that can be used to configure the date.

When you select this control type in the form designer applet, the Date Editor page is displayed. You can use the fields in the editor to configure the control type. The Date Editor contains the following fields:

DateInput Type

Select the type of date input for the calendar pop-up window.

Default

Provides a calendar pop-up window and a **Never** check box. If the user selects the check box, then the attribute value never expires.

Alternative Date

Provides a calendar pop-up window without a **Never** check box. Use this type if the attribute value must expire at some point in time.

Show Time

Select this check box to include a pop-up window that you can use to view and specify a time.

DropDown Box



Creates a list for an attribute. You must populate the attributes to be contained in the list by using one of the following options:

Custom Values

Limits the information that is available in the list on the resulting form. When you select this option, the **Select Editor** page is displayed. You can use the fields in the editor to configure the control type. The Select Editor contains the following fields and toolbar buttons:

Number of Rows

Type the number of rows to include in the list and press **Enter**. Use this field to specify the number of rows in the list. If the original list contains more rows than the number that you enter, then the extra rows are removed.

Data Value

Type a data value.

Display Value

Type a display value to display in the list.

Use Blank Row

Select this check box to insert a blank entry into the list.

Add Row

Click to add a row to display in the list.

Delete Row

Click to delete a row from the list.

Use Display Value as Data Value

Click to use the same value that is entered in the **Display Value** column for the **Data Value** column.

Use Index as Data Value

Click to use the same value that is in the index for the **Data Value** column.

Search Filter

Provides a broader range from which to gather information when populating the box. Using an LDAP search filter assigns a value to an attribute through the use of a search control. When you select this option, the SearchFilter Editor page is displayed. You can use the fields in the editor to configure the control type. The SearchFilter Editor contains the following fields:

Search Base

Select the scope of the search from these options:

org searches the organization of the selected container in the organization tree.

contextual searches the selected organizational unit in the organization tree.

Object Class

Type the name of the LDAP class to search for, such as `erNTGlobalGroup`. The value for the group field on the resulting form must be `erroles`.

Attribute

Type the attribute to search for, such as `erNTLocalName`.

Source Attribute

Type the attribute value to return after the search has completed, such as `erNTGlobalGroupId`.

Description Attribute

Type the attribute value that is appropriate for the service type. If there is no entry in this field, the group search page in the user interface contains no **Description** column in the search results table.

Filter

Type any additional filter that needs to be applied to the search, such as `(objectclass=erNTLocalGroup)`. The value for the group field on the resulting form must be `objectclass=erroles`.

Delimiter

Type the delimiter to use to separate attribute values in the resulting form.

Multiple Value

Select this check box to change a dropdown box to a list box in the resulting form. The list box allows users to select more than one value.

Show Query UI

Select this check box to display a search page in the resulting form. When this option is not selected, only search results are displayed in a separate page.

Paginate Results

Select this check box to display the search results across multiple pages.

Editable Text List

Enables the display of multi-value attributes on the user interface. This control type is a list box that displays user-provided information. Users can enter information into the text field and add it to the list box by clicking **Add**, and they can delete information from the list box by selecting the entry and clicking **Delete**.

ListBox



Provides a list box for an attribute. The list box contains user-selected data. Users can add one or more items to a list box, and they can delete one or more items from the list box.

Custom Values

Limits the information that is available in the list on the resulting form. When you select this option, the Select Editor page is displayed. You can use the fields in the editor to configure the control type. The Select Editor contains the following fields and toolbar buttons:

Number of Rows

Type the number of rows to include in the list and press **Enter**. Use this field to specify the number of rows in the list. If the original list contains more rows than the number that you enter, then the extra rows are removed.

Data Value

Type a data value.

Display Value

Type a display value to display in the list.

Use Blank Row

Select this check box to insert a blank entry into the list.

Add Row

Click to add a row to display in the list.

Delete Row

Click to delete a row from the list.

Use Display Value as Data Value

Use the same value that is entered in the **Display Value** column for the **Data Value** column.

Use Index as Data Value

Use the same value that is in the index for the **Data Value** column.

Search Filter

Provides a broader range from which to gather information when populating the box. Using an LDAP search filter assigns a value to an attribute through the use of a search control. When you select this option, the SearchFilter Editor page is displayed. You can use the fields in the editor to configure the control type. The SearchFilter Editor contains the following fields:

Search Base

Select the scope of the search from these options:

org searches the organization of the selected container in the organization tree.

contextual searches the selected organizational unit in the organization tree.

Object Class

Type the name of the LDAP class to search for, such as `exNTGlobalGroup`. The value for the group field on the resulting form must be `erroles`.

Attribute

Type the attribute to search for, such as `exNTLocalName`.

Source Attribute

Type the attribute value to return after the search has completed, such as `exNTGlobalGroupId`.

Filter

Type any additional filter that needs to be applied to the search, such as (objectclass=erNTLocalGroup). The value for the group field on the resulting form must be objectclass=erroles.

Delimiter

Type the delimiter to use to separate attribute values in the resulting form.

Multiple Value

Select this check box to change a dropdown box to a list box in the resulting form. The list box allows users to select more than one value.

Show Query UI

Select this check box to display a search page in the resulting form. When this option is not selected, only search results are displayed in a separate page.

Paginate Results

Select this check box to display the search results across multiple pages.

LoginHours

Defines the hours that a service is available for users to log in to it. Use this control type only on forms for services that support restricted login times, such as a Windows 2000 service.

When you select this control type in the form designer applet, the LoginHours Editor page is displayed. You can use the fields in the editor to configure the control type to default to a specific type of search. The LoginHours Editor contains the following fields:

Time Interval

Select the time interval to be displayed in the resulting form:

One Hour sets the time interval to one-hour blocks.

Mid Hour sets the time interval to half-hour blocks.

Orientation

Select the orientation for the editor that is used to define login times on the resulting form:

Portrait places the days of the week along the X-axis and the time (in half-hour or one-hour blocks) along the Y-axis.

Landscape places the time (in half-hour or one-hour blocks) along the X-axis and the days of the week along the Y-axis.

Password

Provides a text box for an attribute that does not display the information that a user provides. The information is masked on the screen for security.

Password Popup

Opens a window for the user to enter secure information. The information is masked on the screen and provides two text fields to enter the information. This control type is typically used for an individual's shared secret.

Search Control

Provides a text field search page for the selected attribute, and includes **Search** and **Clear** buttons. Users populate the text field by selecting the desired search result. In the resulting form in the user interface, the **Search** button opens a search page with the search type already selected, and the **Clear** button clears the text field.

When you select this control type in the form designer applet, the Search Control Editor page is displayed. You can use the fields in the editor to configure the control type to default to a specific type of search. The Search Control Editor contains the following fields:

Category

Select the category for the search.

Profile

Select the profile to use for the search.

Attribute

Select the attribute to use for the search.

Operator

Select the operator, such as **Contains** or **Equals**, that links the **Attribute** and **Value fields** together.

Value

Type the value for the attribute.

Type

Select the type of attributes to be returned. A single-value type provides a text field for the user to populate. A multi-value type provides a list box of attributes. In this scenario, users can identify which attributes to search by selecting the attributes that they do not wish to include in the search and clicking the **Delete** button. This removes the selected attributes from the list of searchable attributes.

Search entire organization (current container only if not checked)

Select this check box if you want the search to include the entire organization.

A related control type is the Search Match control type, which is the Search Control control type with an additional feature that allows automatic searching and populating of an attribute's list box.

Search Match

Similar to the Search Control control type, with an additional feature that allows automatic searching and populating of an attribute's list box. Users can use the automatic searching feature by typing in the first few letters of the desired value in the text field and clicking **Add**. If one result is found, the result is automatically added to the list box. If more than one result is found, a **Search Results** page is displayed. A user can then select which items to add to the list box.

Provides a text field search page for the selected attribute. Users populate the text field by selecting the desired search result. In the resulting form, the **Search** button opens a search page with the search type already selected. The **Clear** button clears the text field. The **Delete** button is used to remove a selected item from the list box.

When you select this control type in the form designer applet, the **Search Control Editor** page is displayed. You can use the fields in the editor to configure the control type to default to a specific type of search. The Search Control Editor contains the following fields:

Category

Select the category for the search.

Profile

Select the profile to use for the search.

Attribute

Select the attribute to use for the search.

Operator

Select the operator, such as **Contains** or **Equals**, that links the **Attribute** and **Value fields** together.

Value

Type the value for the attribute.

Type

Select the type of attributes to be returned. A single-value type provides a text field for the user to populate. A multi-value type provides a list box of attributes. In this scenario, users can identify which attributes to search by selecting the attributes that they do not wish to include in the search

and clicking the **Delete** button. This removes the selected attributes from the list of searchable attributes.

Search entire organization (current container only if not checked)

Select this check box if you want the search to include the entire organization.

A related control type is Search Control.

SubForm



The SubForm control type provides a means to utilize custom user interfaces for complex multi-valued attributes. Some IBM Security Identity Manager adapters use this control type infrequently.

SubForm is a special control type used to invoke a Servlet, JSP, or static HTML page from a popup window that opens from a custom IBM Security Identity Manager form. Subforms provide a means to submit an arbitrary number of parameter names and values to a custom Servlet or JSP and are used to create custom user interfaces for complex multi-valued attributes.

Parameter	Description	Value
customServletURI	The URI to the Servlet, JSP, or static HTML page to be invoked from the main form. If a Servlet is implemented and deployed in the default web application for IBM Security Identity Manager, the value for this parameter is the same as the <i>URL-pattern</i> value defined in web.xml in the <i>servlet-mapping</i> tag, without the slash (/). If a JSP is implemented, the value for this parameter is the JSP file name including the jsp file extension. This parameter is required on all subforms.	Servlet name or JSP file name, such as <code>sample.jsp</code>
<i>Parameter Name</i>	Arbitrary parameter name and value that is included in the HTTP request that invokes the resource at customServletURI.	<i>Parameter Value</i> , such as <code>racfconnectgroup servlet</code>

TextArea



Places a text area adjacent to the attribute. A text area is a multiline text field used to gather user input and display data previously gathered.

TextField



Places a text field adjacent to the attribute. A text field is a single line area used to gather user input or display data previously gathered.

UMask



Allows a user to define UNIX access rights to files and directories.

Related information

For more information, see the [IBM Knowledge Center](#).

Properties used by the form designer

Use the **Properties** page to configure attribute format and constraints.

The **Properties** page includes the following tabs:

Format

Use this tab to change the format of a form. Available fields in this tab are:

Name

Use this field to add or modify the name of an attribute. The form uses this identifier to process LDAP attributes.

Data Type

Use this field to add or modify the data type of an attribute, such as Directory String, Distinguished Name, binary code, or another data type.

Label

Use this field to add or modify a user-readable label for the attribute. For example, \$homepostaladdress, where the \$ (dollar) symbol indicates a key to look up a string in a resource bundle.

Size

Use this field to add or modify the visible width in units of pixels for the following control type: TextField, Password, Search Control, and Search Match. Size represents the number of visible items for the following control type: ListBox and Editable TextList.

Rows

Use this field to add or modify the value used by the TextArea control type to represent the number of visible text lines.

Cols

Use this field to add or modify the value used by the TextArea control type to represent the visible width in average character widths.

Width

Use this field to add or modify the value used by the SubForm control type to represent the width of a window in units of pixels.

This property is also used by the DropDownBox, EditableTextList, ListBox, SearchControl, and SearchMatch controls to represent the width of their associated combo boxes in pixels. For EditableTextList and SearchMatch controls, width also determines the width of associated text boxes in pixels.

If width is not specified, it is assumed to be a default of 300 pixels. If the width for these controls is set to 0, the associated combo boxes are not a fixed size and resize dynamically, depending upon the options added.

Height

Use this field to add or modify the value by the SubForm control type to represent the height of a pop-up window in units of pixels

Read-Only on Modify

Select this check box to set an attribute to read-only. Only the label is shown in the form; users cannot modify the attribute value.

Direction

Select the direction of text:

inherit presents text in the same direction as the form category to which the attribute belongs

ltr presents text from left to right

rtl presents text from right to left

Hide on Modify

Select this check box to hide the attribute field in the form when the form is in modify state. For example, if you select this check box for the Owner field within a service form, the Owner field is shown when users create a service. However, it is not shown when users change a service.

Autocomplete

Select this check box to enable autocomplete for the **TextField**, **Password** and **PasswordPopUp** fields. When enabled, autocomplete allows the browser to predict the value. When a user starts to type in a field, the browser displays options to fill in the field, based on earlier typed values. In some browsers you might need to activate an autocomplete function for this format to work.

Constraints

Use this tab to enter values for constraint fields to guarantee the type and syntax of data that users can enter in form fields. Custom constraints are field-level data restrictions of various types. When you select a control type of **Search Control**, **Search Match**, **ListBox**, or **DropDownBox**, all of the constraint fields are disabled except for the **Required** constraint.

Required

Select this check box to prevent the form from being submitted without some value in the field where this constraint is placed.

Validate and Update Constraints



In the field next to **Validate and Update Constraints** in the constraint type list, type a sample value for the attribute you selected from the form template layout area. Click **Validate and Update Constraints**. This action tests the value entered against the constraints activated for the attribute. If the test value you enter complies with all constraints, a message of success is shown after you click **Validate and Update Constraints**.

Constraints fall into one of these general categories:

Value constraints

Require a parameter, such as Max Length = 10, where 10 is the parameter to constrain the value by.

Invalid characters

Enter the characters that are defined as invalid.

Maximum length

Type a numeric value that constrains the length of the value entered for the field to the number of characters specified.

Minimum length

Type a numeric value that prevents the form from being submitted unless the value entered has at least as many characters specified by this constraint.

Maximum value

Type a numeric value to set a high end point on the value entered (is at most *n*).

Minimum value

Type a numeric value to set a low end point on the value entered (is at least *n*).

Maximum number of lines

Type a numeric value to guarantee that the value entered on the form does not exceed the maximum number of lines specified (in a multi-line field).

No white space

Select this check box to prevent any white space from being entered on the form.

Data type constraints

Define valid values that occur within a range of characters or numbers.

ASCII-Only

Select this check box to constrain the characters in the field to ASCII.

ASCII7

Select this check box to constrain the characters in the field to ASCII-7.

ASCII8

Select this check box to constrain the characters in the field to ASCII-8.

Integer only

Select this check box for only integers in the field.

Numeric

Select this check box for only numbers in the field.

Date range

Type a date range to force an ending date to be after a beginning date.

Syntactic constraints

Define valid values that conform to rules for sequences of characters and structured parts.

Email address

Select this check box to guarantee that the syntax of the value in the field complies with the following rules:

- Has one @ sign
- Invalid characters, such as < > () . ; " \ [] do not occur before the @ sign
- The @ sign must be followed by a valid domain name or IP address.

IP address (IPv4)

Select this check box to guarantee that the value in the field is a valid IPv4 address of the form 127.0.0.1 The four octets are separated by a dot and none of the octets exceeds 255.

IP address (IPv6)

Select this check box to guarantee that the value conforms with the text representation of IP addresses defined in RFC 2373. For example, 0:0:0:0:0:0:0:1 is the loopback IPv6 address. See RFC 2373 for more details.

Domain name

Select this check box to ensure that the value in the field is compliant with the Windows NT Domain Name syntax. The name must have two leading backslashes (\\) and can contain up to 15 characters, except for these characters: " / \ [] : ; | = , + * ? < >

The name cannot consist solely of periods or spaces.

Invalid characters

Type characters in this field to define characters that are not valid when entered for the field.

DN

Select this check box to guarantee that the value entered in this field conforms with the distinguished name structure. For example, *cn=common name, ou=organizational name, o=organization*.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Entities

Use this page to customize system entities.

Manage Entities table

Lists the system entities. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a system entity. To select one or more system entities, select the check box adjacent to the system entity. To select all system entities, select the check box at the top of the column.

Name

Indicates the name of the system entity. Click the entity name to change information for the entity.

Entity Type

Indicates the entity type of the corresponding system entity.

Custom Class

Indicates the LDAP class of the corresponding system entity.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a customized entity.

Change

Click to change the selected entity.

Delete

Click to delete the selected entity. You cannot delete an entity for which dependent data exists. You cannot delete a service or account profile.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Create an Entity

Use this wizard to create a IBM Security Identity Manager system entity.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Type

Use this page to view or select the system entity category.

Note: If you are creating an entity, you can view and select the category for the entity that you are creating. However, if you are changing an entity, you can view the category, but you cannot change it.

The table contains the available categories of system entities. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a system entity category. Click the radio button adjacent to the system entity category for the entity that you want to create. For example, you can select Business Partner Person or Person as the category.

Category

Identifies the category of the system entity.

Related information

For more information, see the [IBM Knowledge Center](#).

Entity Detail Information

Use this page to specify the entity name and associated LDAP class, name attribute, and default search attributes.

Entity name

Indicates the name of the custom system entity.

LDAP class

Indicates the corresponding LDAP class that the custom entity uses. To select an LDAP class from the LDAP server, click **Search**.

The **Search** button is not available for account profiles or service profiles.

Name attribute

Indicates the attribute of the selected LDAP class that is used as the entity instance name attribute. To select a name attribute, click **Browse name attributes**.

Valid entries for this field depend on which LDAP class is selected. If no LDAP class is selected, this field is inactive.

Default search attributes

Indicates the list of attributes from the selected LDAP class to be used for advance searching. Select the search attributes that you want to add to the entity and click **Add**. To remove attributes from the entity, select the attributes and click **Remove**.

This field is not available for service profiles.

Related information

For more information, see the [IBM Knowledge Center](#).

Attribute Mapping

Use this page to map system attributes to selected LDAP attributes.

Select an attribute from the ITIM attribute list. Then select the attribute from the Custom LDAP attribute list that you want to map to the ITIM attribute and click **Map**.

ITIM attribute

Displays the system attributes of the category to be created.

Custom LDAP attribute

Displays the custom LDAP schema attributes that are not yet mapped.

Attribute Mapping table

Lists the system attributes and the LDAP attributes to which they are mapped. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates the pair of mapped attributes to which the **Reset** button applies.

ITIM Attribute

Indicates the name of the system attribute.

Custom LDAP Attribute

Indicates the name of the custom LDAP schema attribute to which the system attribute is mapped.

Click **Reset** to return a selected pair of attributes to the default mapping.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Finish** when you are done with this task.

Related information

For more information, see the [IBM Knowledge Center](#).

Attribute Auditing

Use this page to remove attributes for Person, BPPerson, or Account entities from the audit process.

By default all attributes are included in the audit process. If an attribute value might exceed 4000 bytes, remove it from the **Audited Attributes** list.

This process applies only to Person, BPPerson (Business Partner Person), and Account entities.



Warning: The audit process fails if it encounters an attribute that exceeds 4000 bytes.

Audited attributes

List containing the attributes that are included in the auditing process. All attributes initially appear in this list.

To remove an attribute from this list and add it to the **Available attributes** list, click on it, then click **< Remove**.

Available attributes

List containing the attributes that are excluded from the auditing process.

To return an attribute in this list to the **Audited attributes** list, click on it, then click **Add >**.

Related information

For more information, see the [IBM Knowledge Center](#).

Change an Entity

Use this notebook to change a system entity.

Select type

Use this page to view the system entity category.

Entity Detail Information

Use this page to specify the entity name and associated LDAP class, name attribute, and default search attributes.

Attribute Mapping

Use this page to map system attributes to selected LDAP attributes.

“Attribute Auditing” on page 520

Use this page to exclude attributes from the audit process. This is required for attributes that have values longer than 4000 bytes.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Type

Use this page to view the system entity category.

If you are creating an entity, you can view and select the category for the entity that you are creating. However, if you are changing an entity, you can view the category, but you cannot change it.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related information

For more information, see the [IBM Knowledge Center](#).

Entity Detail Information

Use this page to specify the entity name and associated LDAP class, name attribute, and default search attributes.

Entity name

Indicates the name of the custom system entity.

LDAP class

Indicates the corresponding LDAP class that the custom entity uses. To select an LDAP class from the LDAP server, click **Search**.

Name attribute

Indicates the attribute of the selected LDAP class that is used as the entity instance name attribute. To select a name attribute, click **Browse name attributes**.

Valid entries for this field depend on which LDAP class is selected. If no LDAP class is selected, then this field is inactive.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related information

For more information, see the [IBM Knowledge Center](#).

Attribute Mapping

Use this page to map system attributes to selected LDAP attributes.

Select an attribute from the ITIM attribute list. Then select the attribute from the Custom LDAP attribute list that you want to map to the ITIM attribute and click **Map**.

ITIM attribute

Displays the system attributes of the category to be created.

Custom LDAP attribute

Displays the custom LDAP schema attributes that are not yet mapped.

Attribute Mapping table

Lists the system attributes and the LDAP attributes to which they are mapped. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates the pair of mapped attributes to which the **Reset** button applies.

ITIM attribute

Indicates the name of the system attribute.

Custom LDAP attribute

Indicates the name of the custom LDAP schema attribute to which the system attribute is mapped.

Click **Reset** to return a selected pair of attributes to the default mapping.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related information

For more information, see the [IBM Knowledge Center](#).

Attribute Auditing

Use this page to remove attributes for Person, BPPerson, or Account entities from the audit process.

By default all attributes are included in the audit process. If an attribute value might exceed 4000 bytes, remove it from the **Audited Attributes** list.

This process applies only to Person, BPPerson (Business Partner Person), and Account entities.



Warning: The audit process fails if it encounters an attribute that exceeds 4000 bytes.

Audited attributes

List containing the attributes that are included in the auditing process. All attributes initially appear in this list.

To remove an attribute from this list and add it to the **Available attributes** list, click on it, then click **< Remove**.

Available attributes

List containing the attributes that are excluded from the auditing process.

To return an attribute in this list to the **Audited attributes** list, click on it, then click **Add >**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select LDAP Class

Use this page to search for and select an LDAP class.

Object class name

Type a search string to be used as search criteria to find an LDAP class and click **Search**.

LDAP Classes table

Lists the LDAP classes that the search returns. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates which LDAP class is selected.

Object class name

Identifies the current LDAP classes in the LDAP server with a name that contains the search string you entered.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Attribute

Use this page to select a name attribute for the system entity.

Attributes table

Lists the LDAP schema attributes that are associated with the corresponding LDAP class. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates which attribute is selected.

Attribute Name

Identifies the name of the LDAP schema attribute that is associated with the corresponding LDAP class.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Operations

Use this page to add, change, or delete operations for a system entity.

Operation Level

Indicates the defined level of the operation. The list of operations depends on the operation level selected.

Global level operations apply to all entities and entity types.

Entity type level operations apply to all entities of that specific type, such as an account or person entity. For static operations, an entity type defines the namespace of the operation. For nonstatic operations, an entity type defines the type of the target entity. An operation at the entity type level does not override an operation at the global level. Select an entity type from the **Entity Type** list.

Entity level operations override the operations that are defined at the entity type level. Select an entity type from the **Entity type** list and select an entity from the **Entity** list. By default, all operations of a particular entity type are shown for the corresponding entities at the entity level. For example: by default, all the operations for the Entity type **Account** are shown for all Account Entities (such as **LDAP Account** and **Windows Local Account**).

System Entities table

Lists the operations for system entities. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an entity operation. To select one or more entity operations, select the check box next to the entity operation. To select all entity operations, select the check box at the top of the column.

Operation

Identifies the name of the workflow operation that is applied to the entity. To modify the workflow operation, click the name of the operation.

Type

Indicates whether the entity is user-defined or system-defined. At the entity type level, **System Defined** is displayed for predefined operations and **User Defined** is displayed only for new operations in the **Type** column. For inherited operations at the entity level, **System Defined** is displayed by default. If the user adds an operation or modifies an existing operation at the entity level, then **User Defined** is displayed in the **Type** column.

Level

Displays the logical level to which the operation applies. Can be one of the following levels:

Global

Operations that are defined at the Global level.

Entity type

All Entity type operations have a level of **Entity type**. All Entity operations start with a level of **Entity type** because they inherit their behavior from the Entity type operation. These operations can be modified. If an operation is modified, it overrides logically higher or more general operations.

Entity

The new operations defined at the entity level.

Entity override

Indicates that this operation was overridden and now applies to the particular entity instead of to the overall entity type.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add an operation or to override an operation defined at a higher level.

Change

Click to modify the selected operation.

Delete

Click to delete the selected operation.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Add Operation

Use this page to add a customized operational workflow using the Workflow Designer.

This page displays the level defined for the operation.

Global level operations apply to all entities and entity types.

Entity type level operations override the operations that are defined at the global level.

Entity level operations override the operations that are defined at the entity type level.

Operation Name

Type a name of the workflow operation that you want to define for the corresponding system entity and click **Continue**. To override an operation that is defined at a higher level, enter the operation name that you want to override and click **Continue**.

Related information

For more information, see the [IBM Knowledge Center](#).

Define Operation

Use this page and the Java applet to define operations for the system entities that appear on the IBM Security Identity Manager interface.

Use the designer to create a visual business process by combining design nodes into a logical operation. Operations can be as simple as requiring only one approval, or they can be as complex as requiring multiple approvals with requests for information (RFIs), loops, and so on. Manual activities that are defined in the operation populate an individual participant's To Do list as each process in the operation is completed. At any point, the system administrator can view any user's To Do list and act as the Participant, overriding the approval authority.

To define an operation, drag and drop the design nodes from the node palette onto the operation design space and connect them with transition lines.

After you place a design node on the operation design space, double-click the node to configure its properties.

Operation designer interface

The operation designer has these areas:

Operation Name

Displays the name of the operation.

Target

Displays the name of the target, such as an account, person, or business partner person.

Node palette

Displays all available nodes in the left pane of the interface.

Design space

Displays the nodes that you are working with in the large pane of the interface.

High Contrast

Select this check box to display the operation design interface without color representing the design nodes.

Properties

Click this button to view configurable properties of the operation node.

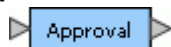
Update

Click this button to refresh the view of the operation design space.

Design nodes

The following design nodes are available:

Approval



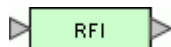
Use this node to define the person who must approve a request or activity before operation processes can continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Mail



Use this node to configure e-mail notification.

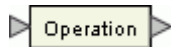
RFI



Use this node to request information from a person. For example, you might need a manager to provide contact information for a new employee before the process of issuing the employee an e-mail account can complete. The person must respond with the information before operation processes can

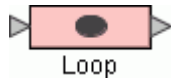
continue. You can also define an interval of time in which the person must respond to the request before it is escalated.

Operation



Use this node to initiate an operation that has been defined previously. This operation can be initiated at any point during the primary operation.

Loop



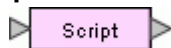
Use this node to repeat a specified activity while or until a specified condition is met.

Extension



Use this node to specify an operation extension to manage people and accounts.

Script



Use this node to specify a JavaScript script that runs when processing the operation activities.

Work Order



Use this node to e-mail a request notification for a manual activity. For example, you might use this node in an operation to request an ID badge for a new employee. Work order participants are not required to have an IBM Security Identity Manager account. They must, however, have an e-mail address that is stored in the IBM Security Identity Manager directory server.

Manage Life Cycle Rules

Use this page to create, change, delete, or run a life cycle rule.

Life Cycle Rule Level

Indicates the defined level of the life cycle rule. The list of life cycle rules depends on which life cycle rule level is selected.

Global level rules apply to all entities and entity types.

Entity type level rules override the life cycle rules that are defined at the global level. Select an entity type from the **Entity Type** list.

Entity level rules override the life cycle rules that are defined at the entity type level. Select an entity type from the **Entity Type** list and select an entity from the **Entity** list.

Life Cycle Rules table

Lists the life cycle rules defined for entities. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a life cycle rule. To select one or more life cycle rules, select the check box adjacent to the life cycle rule. To select all life cycle rules, select the check box at the top of the column.

Name

Identifies the name of the life cycle rule of the specified system entity. Click the name of the life cycle rule to modify the life cycle rule.

Description

Provides additional information about the life cycle rule.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to create a life cycle rule.

Change

Click to modify the selected life cycle rule.

Delete

Click to delete the selected life cycle rule.

Run

Click to run the selected life cycle rule.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Life Cycle Rules

Use this notebook to define a life cycle rule that determines the operations to use when automatically handling commonly occurring events. Such an event might be suspending an account that has been inactive for a period of time.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to specify the life cycle name, description, and operation.

Name

Type a name to identify the life cycle rule of the entity.

Description

Type information about the life cycle rule.

Operation

Indicates the operation defined for the entity. The life cycle rule can only run operations without input parameters.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related information

For more information, see the [IBM Knowledge Center](#).

Event

Use this page to specify the LDAP search filter and schedule for the life cycle rule.

Search filter

Specify a valid LDAP search filter statement that selects the users or accounts to which the life cycle rule applies.

Event table

Lists the schedules that are defined for the life cycle rule. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a schedule. To select one or more schedules, select the check box adjacent to the schedule. To select all schedules, select the check box at the top of the column.

Schedule

Indicates the life cycle rule schedule, which is the interval of time and time of day to run the life cycle rule.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add a schedule entry for the life cycle rule.

Change

Click to modify the selected schedule entry.

Delete

Click to delete the selected schedule entry from the table.

Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

Related information

For more information, see the [IBM Knowledge Center](#).

Define Schedule

Use this page to define a schedule for the life cycle rule.

The fields displayed depend on the scheduling option that is selected. Select one of these schedule intervals to reconcile accounts for this service:

Daily

Reconciles accounts every day. After you select this option, click the clock icon to specify a time in the **At this time** field.

Weekly

Reconciles accounts once a week. After you select this option, select a day from the **On this day of the week** list and click the clock icon to specify a time in the **At this time** field.

Monthly

Reconciles accounts once a month. After you select this option, select a date from the **On this day of the month** list and click the clock icon to specify a time in the **At this time** field.

Hourly

Reconciles accounts once an hour. After you select this option, select a time from the **At this minute** list.

Annually

Reconciles accounts on a specific date and time of the year. After you select this option, select a month from the **Month** list. Then select a date from the **On this day of the month** list and click the clock icon to specify a time in the **At this time** field.

During a specific month

Reconciles accounts on a specific month, day, and time. After you select this option, select a month from the **Month** list. Then select a day from the **On this day of the week** list and click the clock icon to specify a time in the **At this time** field.

Quarterly

Reconciles accounts four times per year on a specific day and time of the quarter. The reconciliation occurs on the specified day past January 1, April 1, July 1, and October 1. After you select this option, select a day from the **On this day** list and click the clock icon to specify a time in the **At this time** field.

Semi-Annually

Reconciles accounts two times per year on a specific day and time of the half-year. The reconciliation occurs on the specified day past January 1 and July 1. After you select this option, select a day from the **On this day** list and click the clock icon to specify a time in the **At this time** field.

Related information

For more information, see the [IBM Knowledge Center](#).

Configure Policy Join Behavior

Use this page to view or change the join directives for a specific attribute in a provisioning policy. A join directive defines how to process an attribute when a conflict occurs between provisioning policies.

Note: This page is a Java applet that does not automatically close and clear from memory after starting. If you encounter performance problems, close and reopen the page.

Click **Service Type** to select from a list of available services, such as NotesProfile. You can view or modify the list attributes.

The user interface for configuring provisioning policy join directives is divided into two panes.

Left pane

The left pane contains a list of attributes, their corresponding label, and their current join directive. It is used to determine precedence sequence. Attributes that are higher in the list take precedence over attributes that are lower in the list.

Attribute Name

Displays an attribute name such as `ernotesdepartment`.

Click an attribute in the list to display the attribute name, the available join directives, and a window to enter any customized Java code in the right pane.

Label

Displays additional information about the attribute, such as `Department`.

Join Directive

Displays the existing join directive for the attribute before you make changes. Only join directives that are applicable to the selected attribute are displayed.

Right pane

The right pane displays the selected attribute's name, description, and applicable join directives. Use the **Join Directive** tab to configure provisioning policy precedence by selecting one of the join directives listed.

Attribute Name

Indicates the name of the attribute that is selected in the left pane.

Description

Optionally, specify information about the policy join directive.

Union

Specifies the attribute values and removes the redundancies. If no other join directive is specified, this is the default join directive.

Intersection

Retrieves the common attribute values.

Priority

Uses the priority of the policy to determine which attribute value to use. If the conflicting policies have the same priority, the first policy found by the system is used.

OR

Indicates a mathematical OR used on a boolean string. `TRUE || TRUE = TRUE` `TRUE || FALSE = TRUE` `FALSE || FALSE = FALSE`

AND

Indicates a mathematical AND used on a boolean string. `TRUE & TRUE = TRUE` `TRUE & FALSE = FALSE` `FALSE & FALSE = FALSE`

Append

Adds the attribute value defined in one policy to the attribute value defined in another policy.

The APPEND join type was designed to be used on single-valued text attributes (such as **comment on WinNT service**).

When joining provisioning parameters using the APPEND join type, all individual values are concatenated into a single string value with a user defined delimiter between them. The delimiter can be defined or changed in **enrolepolicies.properties** file, where the current line reads:

```
provisioning.policy.join.Textual.AppendSeparator=<<<>>>
```

Bitwise OR

Indicates a mathematical Bitwise OR used on a bitstring.

Bitwise AND

Indicates a mathematical Bitwise AND used on a bitstring.

Highest

Uses the highest attribute value from the conflicting policies.

Lowest

Uses the lowest attribute value from the conflicting policies.

Average

Averages the attribute values from the conflicting policies and uses the average value.

Precedence sequence

Uses a user-defined ordering precedence to determine which attribute value to use.

Custom

Defines a custom join directive using Java code. Custom join directives provide administrators with the ability to completely change the built-in join logic. Enter the fully qualified Java class name of the custom join directive class you created for the attribute.

Compliance Alert Rule

Configure a compliance alert rule to specify when to send compliance alerts. To configure a compliance alert rule, select one of the following options:

Numeric Order (higher value generates alert)

Select this option if you want to generate a compliance alert before sending a higher attribute value to the managed resource if the attribute value was increased as a result of a provisioning policy evaluation. If the attribute value was decreased as a result of the evaluation, the attribute value is automatically sent to the managed resource and no alert is generated.

Numeric Order (lower value generates alert)

Select this option if you want to generate a compliance alert before sending a lower attribute value to the managed node if the attribute value was decreased as a result of a provisioning policy evaluation. If the attribute value was increased as a result of the evaluation, the attribute value is automatically sent to the managed resource and no alert is generated.

Never generate alert

Select this option if you do not want to generate a compliance alert when a provisioning policy evaluation leads to a new value for an attribute. The new attribute value is automatically sent to the managed resource.

Always generate alert

Select this option if you want to generate a compliance alert when a provisioning policy evaluation leads to a new value for an attribute. The participant must accept the new attribute value before it is sent to the managed resource. This is the default value for attributes that have a single value.

Precedence sequence

Select this option if you want higher values in the list to be considered more privileged than lower values. When a provisioning policy evaluation leads to assignment of a higher attribute value, the attribute value is sent to the managed resource and no compliance alert is generated. If the attribute value is decreased as a result of the evaluation, a compliance alert is generated before the attribute value is sent to the managed resource.

The following table shows each type of service attribute, the corresponding join directive, and the default join directive.

Service Attribute Type	Applicable Join Directives	Default Join Directive
Multi-valued string or number attribute	UNION INTERSECTION PRIORITY (undefined) CUSTOM	UNION
Single-valued string	PRECEDENCE_SEQUENCE PRIORITY AND OR APPEND BITWISE_AND BITWISE_OR HIGHEST LOWEST AVERAGE CUSTOM	PRIORITY
Single-valued boolean string	AND OR PRIORITY CUSTOM	AND
Single-valued integer	HIGHEST LOWEST AVERAGE PRIORITY PRECEDENCE_SEQUENCE CUSTOM	HIGHEST
Singled-valued bitstring	BITWISE_AND BITWISE_OR PRIORITY CUSTOM	BITWISE_OR

Use these buttons to update the Attributes table:

Move Up

Click to move an attribute value up a row in the table.

Move Down

Click to move an attribute value down a row in the table.

Delete

Click to remove an attribute value from the table.

Add

Click to add a new attribute value to the precedence sequence. You must first type the new value into the adjacent text field before you click **Add**.

Save

Click to save the compliance alert rule in the IBM Security Identity Manager data store.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Action

Use this page to specify the policy enforcement action that occurs for an account that has a noncompliant attribute.

Mark

Sets a mark on an account that has a noncompliant attribute.

Suspend

Suspends an account that has a noncompliant attribute.

Correct

Replaces a noncompliant attribute on an account with the correct attribute.

Alert

Issues an alert for an account that has a noncompliant attribute.

Use these buttons:

Submit

Click to save the selection and continue to the next page. This button is displayed when **Mark**, **Suspend**, or **Correct** is selected as the enforcement action.

Continue

Click to save the selection and continue to the next page. This button is displayed only when **Alert** is selected as the enforcement action.

Related information

For more information, see the [IBM Knowledge Center](#).

Configure Policy Enforcement

Use this notebook to configure policy enforcement for a service.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this page to specify an alert, including participants, escalation intervals, and process types.

Alert name

Indicates the name that identifies the alert.

Send compliance alert to

Identifies which participants receive the compliance alert.

Number of days to wait before escalating compliance alert

Indicates the number of days before an alert is escalated.

Escalate compliance alert to

Identifies which participants receive an escalated compliance alert.

Number of days after which the system will take corrective action

Specifies the number of days the system waits before taking corrective action.

Process Types table

Specifies the processes that generate a compliance alert.

Generate Alert

Indicates the process type that generates an alert. Select the check box of the process type that you want to generate alerts. If the check box is cleared, the system automatically corrects a noncompliant account for that process type.

Process Type

Indicates the type of workflow process that generates a compliance alert.

Click other tabs to specify additional information. Click **Submit** to submit your request.

Related information

For more information, see the [IBM Knowledge Center](#).

E-mail

Use this page to specify an alert e-mail.

Use default template

Indicates whether to use the default e-mail template instead of the custom fields for the alert.

Subject

Type the subject line of the e-mail notification.

Plain text body

Type the main content of the e-mail notification.

XHTML body

Specify the XHTML dynamic content of the e-mail notification.

Click other tabs to specify additional information. Then, click **Submit** to submit your request.

Related information

For more information, see the [IBM Knowledge Center](#).

Import Data

Use this page to import data or delete an import operation record.

The **Import Data** table contains the records of previous data imports. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a import item. To select one or more import items, select the check box adjacent to the import item. To select all import items, select the check box at the top of the column.

Import Name

Identifies the name of the import operation.

File Name

Identifies a file name that the import operation assigns.

Start Time

Indicates the corresponding start time of the import operation.

End Time

Indicates the corresponding end time of the import operation. If the import is in progress, **In Progress** is displayed in this field.

Processed Count

Indicates the number of objects that have been imported for an import currently in progress.

Status

Indicates the current state of the import operation.

- **Failed** indicates that the import was unsuccessful.
- **Failed (Conflicts Not Resolved)** indicates that the import was unsuccessful because the user logged out of the console before resolving import conflicts.
- **Canceled** indicates that the import operation is canceled.
- **Canceling** indicates that a cancel operation has been initiated by user.
- **Completed Success** indicates that the import operation is complete.
- **Conflict Detected** indicates that the file you want to import conflicts with existing system data. The import operation might require manual conflict resolution. Click the **Conflict Detected** link to open the conflict resolution page.
- **Processing** indicates that the import operation is in progress.
- **Submitted** indicates that the import has been submitted and is waiting for processing.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Upload File

Click to start the import process.

Delete

Click to delete the selected import operation record.

Cancel

Click to cancel the selected import.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Upload File

Use this page to specify the name and directory of the file to import.

Import name

Optional. Identifies the name for each import task.

File to upload (.jar)

The name of the Java Archive (JAR) file that contains previously exported data. Click **Browse** to locate the file.

Related information

For more information, see the [IBM Knowledge Center](#).

Evaluate Import File

Use this page to determine whether objects in an import file conflict with existing system data, before you import the file.

The **Import File** table lists the objects evaluated in a file that you might import. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Indicates the objects to be imported into the system repository and to override the existing objects with an imported object.

Name

Identifies the name of the object.

Object Type

Identifies the object type.

Description

Provides additional identification of the object.

Conflict

Indicates whether the object in the import file has a conflict with existing system data.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Import** to import the file.

Related information

For more information, see the [IBM Knowledge Center](#).

Export Data

Use this page to create a new export file, or to delete or export all files.

The **Export Data** table lists the export files. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the export that you want to delete or cancel.

Export Name

Identifies the name of the export file.

File Name

Identifies the file name of the export file.

Type

Identifies whether the export operations is a partial or a full system export.

Start Time

Indicates the corresponding start time of the export operation.

End Time

Indicates the corresponding end time of the export operation. If the export is in progress, **In Progress** is displayed in this field.

Processed Count

Indicates the number of objects that have been exported for an export currently in progress.

Status

Indicates the current state of the export operation.

- **Canceled** indicates that the export operation is canceled.
- **Canceling** indicates that a cancel operation has been initiated by user.
- **Completed Success** indicates that the export operation is complete.
- **Failed** indicates that the export failed.
- **Processing** indicates that the export operation is in progress.
- **Submitted** indicates that the export has been submitted and is waiting for processing.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create a new export file.

Export All

Click to start an export of all files.

Delete

Click to delete the selected export operation record.

Cancel

Click to cancel the selected export operation.

Refresh

Click to update the list of items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Create a Partial Export

Use this page to add or remove system objects to export.

The **Export Data** table lists the system objects. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an object. To select one or more objects, select the check box adjacent to the object. To select all objects, select the check box at the top of the column. You cannot select and remove dependent objects.

Name

Identifies the name of the system object.

Object Type

Identifies the object type.

Dependent

Indicates whether the object is dependent on an object specified for export.

Description

Provides the attribute description of the object.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add an object to the export list.

Remove

Click to remove the selected object from the export list.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Objects

Use this page to select system objects to export.

Name

Type the name of an object. If you do not know the name of the object that you want to find, type a portion of the name to display a list of objects and click **Search**.

Object type

Select the type of the object that you want to export.

Search

Displays a list of all objects matching the specified search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

The table lists the system objects available for export. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an object. To select one or more objects, select the check box adjacent to the object. To select all objects, select the check box at the top of the column.

Name

Identifies the name of the system object.

Description

Provides the description attribute of the object.

Business Unit

Identifies the business unit in which the object is specified.

Related information

For more information, see the [IBM Knowledge Center](#).

Partial Export

Use this page to specify the name and directory of the file to export.

Export name

Optional. Type the name of the export operation.

Export to file (.jar)

Type the name of the file for the data export. The default file type is .jar. Ensure that you type the file name and its extension.

Click **Submit** to add the export operation to the list of exports.

Related information

For more information, see the [IBM Knowledge Center](#).

Export All

Use this page to specify the name and directory of the file to export.

Export name

Optional. Type the name of the export operation.

Export to file (.jar)

Type the name of the file for the data export. The default file type is .jar. Ensure that you type the file name and its extension.

Click **Submit** to add the export operation to the list of exports.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Access Types

Use the **Manage Access Types** page to create, change, or delete an access type in the access types tree.

Click the expand (+) icon to expand any subordinate access types in the **Access Types** tree. Click the icon (▸) next to each access type to see tasks that are available. Alternatively, click an access type in the tree to view or change its details. You must be authorized to view or change details of an access type. For example, the tree contains these types:

Access Types

Identifies an access type, which contains system-defined and custom-defined access types. System defined access types are:

- Application
- E-mail group
- Role
- Shared folder

You can use these choices:

Create Type

Click to create an access type node in the tree.

Change

Click to change the specifications for a selected access type node in the tree.

Delete

Click to delete a selected access type node in the tree. You cannot delete an access type node that has child items or a group or role association.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Type Details

Use this page to specify or view the key and description of an access type.

Access type key

A unique name that you provide for the access type.

Description

The description of the corresponding access type.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Ownership Types

Use this page to create or delete an ownership type or account category.

Select

Specifies an ownership type or account category. To select one or more ownership types or account categories, select the check box next to the ownership type or account category. To select all, select the check box at the top of the column.

Ownership Type Key

Enter a key name for the ownership type or account category.

Label

Enter a custom label for the ownership type or account category.

Description

Enter additional information about the ownership type or account category, such as its purpose.

Account Category Key

Enter a key name for the account category. **n/a** indicates that the row is an ownership type.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Create

Click to create an ownership type or account category.

Delete

Click to delete one or more selected ownership types or account categories.

Related information

For more information, see the [IBM Knowledge Center](#).

Create Ownership Type

Use this page to specify the key and description of an ownership type or an account category.

Individual

Select this check box to create an account category.

Ownership type key

A unique name that you provide for the ownership type.

Account Category Key

A unique name that you provide for the account category.

Description

The description of the corresponding ownership type or account category.

Related information

For more information, see the [IBM Knowledge Center](#).

View Requests

View Pending Requests by User

Use this page to view the requests for a user that have been submitted, but not completed. The current date is the default value for both the start date and end date.

User ID

Displays the user ID of the user whose pending requests you want to view. Click **Search** to find the user.

Start date

Click the calendar icon to select the date that the delegation starts. The default date is the current date.

End date

Click the calendar icon to select the date that the delegation ends. The default date is the current date.

Requests table

Lists the requests matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a pending request. To select one or more pending requests, select the check box adjacent to the pending request. To select all pending requests, select the check box at the top of the column.

Request Type

Identifies the type of request. Click the type of request to view the request details.

Service Name

Identifies the name of the service. If there is more than one service associated with the request, Multiple Services is displayed.

Date Submitted

Identifies the date and time that the request was submitted.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Cancel Request

Click to cancel a pending request.

Refresh

Click to update items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this notebook page to review general information about the request.

One or more of the following fields might not be displayed, depending on the type of request that you are viewing.

Request type

Displays the type of request. **Account add** and **User data change** are example request types.

Service name

Displays the service for which the request is associated.

Completion status

Displays the status of the request.

Date submitted

Displays the date and time when the request was submitted.

Date completed

Displays the date and time when the request was completed. If the request has not been completed, this field is blank.

Result details

Displays information about the results of the completion of the request.

Service information

Displays information about the service for which the request was made.

View All Requests by User

Use this page to view all the requests that a user submitted within a specified time period. The current date is the default value for both the start date and end date.

User ID

Displays the user ID of the user whose requests you want to view. Click **Search** to find the user.

Start date

Click the calendar icon to select the date that the delegation starts. The default date is the current date.

End date

Click the calendar icon to select the date that the delegation ends. The default date is the current date.

Status

Click one or more check boxes to allow for additional filtering of the requests presented.

Errors

Returns only those requests that have errors.

Failed

Indicates that a user request failed.

Canceled

Indicates that a user request is canceled.

Rejected

Indicates that a user request is rejected.

Warnings

Returns only those requests that have warnings.

Timeout

Indicates that a user request timed out.

Terminated

Indicates that a user request is terminated.

Success

Returns only those requests that are successful.

Submitted

Indicates that a user request is submitted for completion of RFI activity.

Approved

Indicates that a user request is approved.

Pending

Returns only those requests that are pending.

Escalated

Indicates that a user request is escalated.

Requests table

Lists the requests that match the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a pending request. To select one or more pending requests, select the check box next to the pending request. To select all pending requests, select the check box at the top of the column.

Status

Identifies the status of the request.

Request type

Identifies the type of request. Click the type of request to view the request details.

Date Submitted

Identifies the date and time that the request was submitted.

Request ID

Identifies the unique identifier for your request.

Requestor

Identifies the user who submitted the request. Click the name to view the details of the requestor.

Requested for

Identifies the user for whom the request was made. Click the name to view the details of the requestor.

Service Name

Identifies the name of the service. If there is more than one service associated with the request, multiple services are displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Cancel Request

Click to cancel a pending request.

Refresh

Click to update items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this notebook page to review general information about the request.

One or more of the following fields might not be displayed, depending on the type of request that you are viewing.

Request type

Displays the type of request. **Account add** and **User data change** are example request types.

Service name

Displays the service for which the request is associated.

Completion status

Displays the status of the request.

Date submitted

Displays the date and time when the request was submitted.

Date completed

Displays the date and time when the request was completed. If the request has not been completed, this field is blank.

Result details

Displays information about the results of the completion of the request.

Service information

Displays information about the service for which the request was made.

View Pending Requests by Service

Use this page to view the requests for a user that have been submitted, but not completed. The current date is the default value for both the start date and end date.

Service name

Displays the name of the service on which you want to review pending requests. Click **Search** to find the name of the service.

Start date

Click the calendar icon to select the date that the delegation starts. The default date is the current date.

End date

Click the calendar icon to select the date that the delegation ends. The default date is the current date.

Requests table

Lists the requests matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a pending request. To select one or more pending requests, select the check box adjacent to the pending request. To select all pending requests, select the check box at the top of the column.

Status

Identifies the status of the request.

Request Type

Identifies the type of request. Click the type of request to view the request details.

Requestor

Identifies the user who submitted the request. Click the name of the user who the request is for to view the user details.

Requested for

Identifies the user for whom the request was made. Click the name of the user who the request is for to view the user details.

Date Submitted

Identifies the date and time that the request was submitted.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Cancel Request

Click to cancel a pending request.

Refresh

Click to update items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this notebook page to review general information about the request.

One or more of the following fields might not be displayed, depending on the type of request that you are viewing.

Request type

Displays the type of request. **Account add** and **User data change** are example request types.

Service name

Displays the service for which the request is associated.

Completion status

Displays the status of the request.

Date submitted

Displays the date and time when the request was submitted.

Date completed

Displays the date and time when the request was completed. If the request has not been completed, this field is blank.

Result details

Displays information about the results of the completion of the request.

Service information

Displays information about the service for which the request was made.

View All Requests by Service

Use this page to display all requests that were submitted for a service, within a specified time period. The current date is the default value for both the start date and end date.

Service name

Displays the name of the service whose requests you want to view. Click **Search** to find the name of the service.

Start date

Click the calendar icon to select the date that the delegation starts. The default date is the current date.

End date

Click the calendar icon to select the date that the delegation ends. The default date is the current date.

Status

Click one or more check boxes to allow for additional filtering of the requests presented.

Errors

Returns only those requests that have errors.

Failed

Indicates that a user request failed.

Canceled

Indicates that a user request is canceled.

Rejected

Indicates that a user request is rejected.

Warnings

Returns only those requests that have warnings.

Timeout

Indicates that a user request timed out.

Terminated

Indicates that a user request is terminated.

Success

Returns only those requests that are successful.

Submitted

Indicates that a user request is submitted for completion of RFI activity.

Approved

Indicates that a user request is approved.

Pending

Returns only those requests that are pending.

Escalated

Indicates that a user request is escalated.

Requests table

Lists the requests that match the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a pending request. To select one or more pending requests, select the check box next to the pending request. To select all pending requests, select the check box at the top of the column.

Status

Identifies the status of the request.

Request Type

Identifies the type of request. Click the type of request to view the request details.

Date Submitted

Identifies the date and time that the request was submitted.

Requestor

Identifies the user who submitted the request. Click the name to view the details of the requestor.

Requested for

Identifies the user for whom the request was made. Click the name to view the details of the requestor.

Service Name

Identifies the name of the service. If there is more than one service associated with the request, multiple services are displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Cancel Request

Click to cancel a pending request.

Refresh

Click to update items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this notebook page to review general information about the request.

One or more of the following fields might not be displayed, depending on the type of request that you are viewing.

Request type

Displays the type of request. **Account add** and **User data change** are example request types.

Service name

Displays the service for which the request is associated.

Completion status

Displays the status of the request.

Date submitted

Displays the date and time when the request was submitted.

Date completed

Displays the date and time when the request was completed. If the request has not been completed, this field is blank.

Result details

Displays information about the results of the completion of the request.

Service information

Displays information about the service for which the request was made.

View All Requests

Use this page to view all requests that users submitted within a specified time period. The current date is the default value for both the start date and end date.

Request type

Identifies the type of request, such as adding or deleting an account or user. Select an option from the menu to filter by request type.

Time interval

Identifies the range of time you want to search between. To search between specific dates, click **Specific Date Range**.

Start date

This option is displayed if you select **Specific Date Range** from the time interval list. Click the calendar icon to select a date from a calendar for the start of the period of time that you want to view requests. The default date is the current date.

End date

This option is displayed if you select **Specific Date Range** from the time interval list. Click the calendar icon to select a date from a calendar for the end of the period of time that you want to view requests. The default date is the current date.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

More Search Criteria

Click to search by a more advanced set of criteria.

Status

Click one or more check boxes to allow for additional filtering of the requests presented.

Errors

Returns only those requests that have errors.

Failed

Indicates that a user request failed.

Canceled

Indicates that a user request is canceled.

Rejected

Indicates that a user request is rejected.

Warnings

Returns only those requests that have warnings.

Timeout

Indicates that a user request timed out.

Terminated

Indicates that a user request is terminated.

Success

Returns only those requests that are successful.

Submitted

Indicates that a user request is submitted for completion of RFI activity.

Approved

Indicates that a user request is approved.

Pending

Returns only those requests that are pending.

Escalated

Indicates that a user request is escalated.

Search by

Search by **Date request was submitted** or **Date request was completed**. By default, the system searches by **Date request was submitted**.

Service associated with request

Search by the service on which the request was submitted. By default, the system searches on all services. Select **Filter By Service** from the menu, and click **Search** to search for a request associated with a specific service.

User request

Search by the user for which the request was submitted. To search for a request associated with a specific user, select **Requested by user** from the menu, and click **Search**.

Request ID

Search by the unique identifier associated with the request.

Requests table

Lists the requests that match the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a pending request. To select one or more pending requests, select the check box next to the pending request. To select all pending requests, select the check box at the top of the column.

Status

Identifies the status of the request.

Request Type

Identifies the type of request. Click the type of request to view the request details.

Date Submitted

Identifies the date and time that the request was submitted.

Requestor

Identifies the user who submitted the request. Click the name to view the user details of the requestor.

Requested For

Identifies the user for whom the request was made. Click the name to view the details of the requestor.

Service Name

Identifies the name of the service. If there is more than one service associated with the request, multiple services are displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Cancel Request

Click to cancel a pending request.

Refresh

Click to update items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

General

Use this notebook page to review general information about the request.

One or more of the following fields might not be displayed, depending on the type of request that you are viewing.

Request type

Displays the type of request. **Account add** and **User data change** are example request types.

Service name

Displays the service for which the request is associated.

Completion status

Displays the status of the request.

Date submitted

Displays the date and time when the request was submitted.

Date completed

Displays the date and time when the request was completed. If the request has not been completed, this field is blank.

Result details

Displays information about the results of the completion of the request.

Service information

Displays information about the service for which the request was made.

Activity Details

Use this page to review the activity details that are associated with the request.

One or more of the following fields might not be displayed, depending on the type of request that you are viewing.

Activity name

Displays a short description of the activity.

Owner

Displays the owner of the activity.

Due Date

Displays the date and time that the activity is to be completed.

Date completed

Displays the date and time when the request was completed. If the request has not been completed, this field is blank.

Activity status

Displays the current status of the activity.

User ID

Displays the user that submitted the request.

Related information

For more information, see the [IBM Knowledge Center](#).

Request Details

Use this page to review detailed information about the request.

This page contains detailed information about the request. The request consists of one or more request types, depending on the workflow set up for the request. These request types are displayed as links under a root structure. Click the request type in the root structure to view additional details about the request.

One or more of the following fields might not be displayed, depending on the type of request that you are viewing.

Request type

Displays the type of request. **Account add** and **User data change** are example request types.

Request ID

Identifies the unique identifier for the request.

Completion status

Displays the status of the request.

Service name

Displays the service for which the request is associated.

Date submitted

Displays the date and time when the request was submitted.

Date scheduled

Displays the date and time when the request was scheduled.

Date started

Displays the date and time when the request started.

Last modified

Displays the date and time when the request was last modified.

Date completed

Displays the date and time when the request was completed. If the request has not been completed, this field is blank.

Access name

Displays the access for which the request is associated, if one exists.

Requested for

Displays the user for which the request was made.

Justification

Displays the reason that the request was made.

Canceled by

Displays the user that canceled the request.

Date canceled

Displays the date and time when the request was canceled.

Canceled justification

Displays the reason that the request was canceled.

Result details

Displays information about the results of the completion of the request.

Process data

Displays information about the current data or changes to current data. Multiple tables can be displayed, depending on how the system administrator has set up workflows for the request type. Click the ► icon to display supporting data or requested changes to data. The following table columns might be displayed:

Attribute

Provides the name of the attribute.

Original Value

Provides the original value of the attribute.

Requested Value

Provides the requested value of the attribute.

Related information

For more information, see the [IBM Knowledge Center](#).

Error and Warning Messages

Use this page to view the details about error and warning messages.

Error and Warning Messages table

Lists the error and warning messages that occurred on a request. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Name

Identifies the type of activity that was processing when the error or warning occurred.

Type

Identifies the access or service type that is associated with the request.

Subject

Identifies the subject of the request.

Summary

Identifies the state of the request.

Result Detail

Provides a description of the error or warning that occurred.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

View Personal Profile

Use this page to view the personal profile information for the user that you have selected.

The profile contains personal, business, and contact information about who the user is, how to contact the user, and so on. Your ability to change and view profile information is determined by the authority your system administrator has granted to you.

Related information

For more information, see the [IBM Knowledge Center](#).

Personal Information

Use this notebook page to review the user's personal information.

The following fields are the default fields:

Last name

Specifies the user's last name, or family name.

Full name

Displays a value for distinguishing users, such as the user's full name.

Preferred user ID

Displays the default user ID that new accounts and access use when they are created.

First name

Specifies the user's first name, or given name.

Initials

Specifies the user's initial.

Home address

Specifies the user's postal address at home.

Shared secret

Specifies a value that is used to retrieve a new password when a password is reset.

Organizational roles

Specifies the organizational roles to which the user belongs.

Related information

For more information, see the [IBM Knowledge Center](#).

Business Information

Use this notebook page to review the user's business information.

The following fields are the default fields:

Office number

Specifies the office number.

Employee number

Specifies the employee number. This information is a numeric or alphanumeric identifier assigned to a user by the business/organization.

Title

Specifies the user's job title.

Manager

Specifies the user's manager.

Postal address

Specifies the user's postal address at work.

Administrative assistant

Specifies the personal or departmental administrative assistant.

Related information

For more information, see the [IBM Knowledge Center](#).

Contact Information

Use this page to review the user's contact information.

The following fields are the default fields:

E-mail address

Specifies the e-mail address.

Telephone number

Specifies the work telephone number.

Mobile telephone number

Specifies the mobile telephone number.

Pager

Specifies the pager number.

Home telephone number

Specifies the home telephone number.

Aliases

Specifies any aliases that are associated with the user ID.

Related information

For more information, see the [IBM Knowledge Center](#).

User Details

Use this page to review personal information about the user as an individual.

The following fields are the default fields:

Full name

A value for distinguishing users, such as the user's full name.

Last name

Specifies the user's last name, or family name.

E-mail address

Specifies the user's e-mail address.

Sponsor

Specifies the user's sponsor.

Organizational roles

Specifies the organizational roles to which the user belongs.

Aliases

Specifies any aliases that are associated with the user ID.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a Service

Use this page to find the service that you want.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Service searches for service names that contain the text that is entered in the **Search information** field.

Business unit searches for business units in which the business unit name contains the text that is entered in the **Search information** field.

Service type

Select a service type from the list.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Services table

Lists the services that match the search criteria that you specified. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box next to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view the service details.

Description

Identifies a brief description of the service.

Service Type

Identifies the type of service.

Business Unit

Identifies the business unit associated with the service.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a User

Use this page to search for a user.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select an attribute from the list. All searchable attributes and the personal profile are included in this list. If you select an attribute, the search is based on that attribute. If you select **Entire profile**, the search is based on all attributes associated with the user.

Last Name searches for the user's last name.

Full Name searches for the user's full name.

E-mail Address searches for the user's e-mail address.

Entire Profile searches all attributes associated with the user.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Users table

Lists the users matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

Name

Identifies a value for distinguishing a user, such as the user's full name. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the user's e-mail address.

Custom Display

Identifies a custom display attribute.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

Status

Identifies the user's status.

Users are either active or inactive. A user must be active to log in to the system. Users become inactive when they are suspended. The suspended users still exist, but they cannot access the system. System administrators can restore inactive users.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Activity Details

Use this notebook page to view the details associated with the selected activity.

Fields on this page vary, depending on whether the activity is an approval, a request for information, or a work order for a manual service.

Activity name

Displays the name of the activity.

Owner

Displays the owner of the activity.

Due date

Displays the date the activity is to be completed.

Date completed

Displays the date and time when the request was completed. If the request has not been completed, this field is blank.

Activity status

Displays the status of the activity.

User ID

Displays the user ID for the account requested.

Owner comments

Displays comments about the request that the owner specified, if this is an approval activity.

If this activity is for a request for information, an additional **Information table** contains these fields:

Attribute

Names the account attribute.

Start value

Specifies the initial value of the attribute.

Submitted value

Indicates a change in the value of an attribute. For example, a change might be a comment that an approver entered in a comment field.

Related information

For more information, see the [IBM Knowledge Center](#).

View Approval Details

Use this page to review the details of a request.

Activity name

Displays the name of the activity.

Due date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Activity status

Displays the status of the activity.

Owner's comments

Displays the comments made by the user who is responsible for completing the activity.

Owner

Displays the name of the user who is responsible for completing the activity.

Date completed

Displays the date that the activity was completed. If this field is blank, the activity has not yet been completed.

User ID

Displays the user for whom the activity is being completed.

Related information

For more information, see the [IBM Knowledge Center](#).

Compliance Alert Details

Use this page to view the details associated with the selected compliance alert.

Fields in this page vary, depending the type of activity.

Activity name

Displays the name of the activity.

Activity due on

Displays the date the activity is to be completed.

Activity status

Displays the status of the activity.

Owner's comments

Displays comments about the request that the owner specified.

Participant

Displays the owner of the activity.

Activity completed on

Displays the date and time when the request was completed. If the request has not been completed, this field is blank.

User ID

Displays the user ID for the account requested.

Related information

For more information, see the [IBM Knowledge Center](#).

Service Details

Use this page to view the details that are related to the selected service. Each service has its own unique set of information. Refer to the documentation provided with the adapter for details about the displayed fields.

The following fields are common for most services. All fields are read-only, so you cannot change any information related to the service. These fields might or might not be displayed on the service form by default. Except for the **Service name** field, these fields can be added or removed.

Service name

Displays the name of the service.

Description

Displays the description of the service that was provided by the service owner.

URL

For remote services, displays the URL used to connect to the resource hosting the service. The *address* value is displayed in brackets for IPv6 addresses.

User ID

Displays the user ID used to log into the remote resource.

Owner

Displays the name of the service provider.

Service prerequisite

Displays the prerequisite that must be met before the service can be used, for example, at least one service account must exist.

Related information

For more information, see the [IBM Knowledge Center](#).

Activity Owners

Use this page to view the details about the owners of an activity.

Owners table

Lists the owners of an activity. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Full Name

A value for distinguishing users, such as the user's full name. Click the name of the user to view the user's personal profile.

Telephone Number

Identifies the user's telephone number.

E-mail Address

Identifies the user's e-mail address.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Manage Activities

View Activities

Use this page to manage your to-do list. You can also view the details of your activities that have been grouped.



Activities table

Lists the activities that you can manage. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an activity. To select one or more activities, select the check box adjacent to the activity. To select all activities, select the check box at the top of the column.

State

Identifies the status of the activity. It is either locked by you () , locked by another user () , or unlocked.

Activity

Identifies the type of activity. Click the name of the activity to view details about it.

If the subject of an activity has more than one item listed, the activities have been grouped. Activities are grouped automatically by the system and allow you to process the activities individually or collectively. For example, you can approve a group of five account activities at the same time. Or, you can approve two of the requests and then reject the remaining three requests.

Due Date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested For

Displays the user for whom the request was submitted. Click the name of the user (if a link is available to you) to view the personal profile for the user.

Subject

Identifies the user-specified purpose of the request. If two or more items are listed for an activity, the activities have been automatically grouped.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Lock

Click to lock the selected item. When an activity is assigned to a group of users, it can be locked by the user who plans to complete the activity. While the other users in the group can view the activity, they cannot process it.

Unlock

Click to unlock a selected item. The user that locked the item must unlock it.

Assign

Click to assign the selected activity to someone else in the group to complete. This button is displayed only when the activity is assigned to a group of users.

Refresh

Click to update items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

View Activities by User

Use this page to manage your to-do list. You can also view the details of your activities that have been grouped.



Activities table

Lists the activities that you can manage. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an activity. To select one or more activities, select the check box adjacent to the activity. To select all activities, select the check box at the top of the column.

State

Identifies the status of the activity. It is either locked by you () , locked by another user () , or unlocked.

Activity

Identifies the type of activity. Click the name of the activity to view details about it.

If the subject of an activity has more than one item listed, the activities have been grouped. Activities are grouped automatically by the system and allow you to process the activities individually or collectively. For example, you can approve a group of five account activities at the same time. Or, you can approve two of the requests and then reject the remaining three requests.

Due Date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested For

Displays the user for whom the request was submitted. Click the name of the user to view the user's personal profile.

Subject

Identifies the user-specified purpose of the request. If two or more items are listed for an activity, the activities have been automatically grouped.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Lock

Click to lock the selected item. When an activity is assigned to a group of users, it can be locked by the user who plans to complete the activity. While the other users in the group can view the activity, they cannot process it.

Unlock

Click to unlock a selected item. The user that locked the item must unlock it.

Assign

Click to assign the selected activity to someone else in the group to complete. This button is displayed only when the activity is assigned to a group of users.

Refresh

Click to update items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

View Activities by User

Use this page to manage the to-do list of a specified user.



Activities table

Lists the activities that you can manage. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an activity. To select one or more activities, select the check box adjacent to the activity. To select all activities, select the check box at the top of the column.

State

Identifies the status of the activity. It is either locked by you () , locked by another user () , or unlocked.

Activity

Identifies the type of activity. Click the name of the activity to view details about it.

If the subject of an activity has more than one item listed, the activities have been grouped. The system automatically groups the activities, allowing you to process the activities individually or collectively. For example, you can approve a group of five account activities at the same time. Or, you can approve two of the requests and then reject the remaining three requests.

Due date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested for

Displays the user for whom the request was submitted. Click the name of the user to view the user's personal profile.

Subject

Identifies the user-specified purpose of the request. If two or more items are listed for an activity, the activities have been automatically grouped.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Lock

Click to lock the selected item. When an activity is assigned to a group of users, the user who plans to complete the activity can also lock it. While the other users in the group can view the activity, they cannot process it.

Unlock

Click to unlock a selected item. The user that locked the item must unlock it.

Assign

Click to assign the selected activity to someone else in the group to complete. This button is displayed only when the activity is assigned to a group of users.

Refresh

Click to update items in the table.

Change User

Click to search for and view activities for a different user.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a User

Use this page to select a user ID to view the activities of another user.

User ID

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

ITIM Accounts table

Lists the users matching the specified criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a user.

User ID

Identifies the user ID for the activity owner.

Owner

Identifies the activity owner.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Request Details

Use this page to recertify the roles, accounts, and groups of a user. When the activity is locked by another user, some fields on this page are disabled or are not displayed.

Request type

Displays the type of the request.

Submission date

Displays the date and time when the request was submitted.

Due date

Displays the date and time by which the activity needs to be completed. An activity that passes this date either forwards to a defined escalation participant if one exists, terminates automatically, or remains available as an overdue activity item.

Requested for

Displays the user for whom the request was submitted. Click the name of the user to view the user's personal profile.

Requested by

Displays the user who submitted the request.

Activity status

Displays the status of the activity.

Instructions

Displays detailed instructions for the activity. To view the instructions, click the  icon.

Reviewer Action tables

Use these tables to recertify roles, accounts, and groups (which include access items). The tables contain a list of roles and a list of account and group items associated with the user.

Roles table

Lists the roles.

This table might or might not be displayed, depending on the configuration of the user recertification policy, and whether the user has any roles. The table contains these columns:

Roles

Identifies the name of the role.

Description

Provides additional information about the role.

Still Required

Select whether the user needs one or more roles.

If the user still requires the role, select **Yes** to recertify the role. If the user no longer requires the role, select **No** to reject the role.

Select **All** to recertify all roles.

Select **None** to reject all roles.

Accounts and Groups table

Lists the accounts and groups. A group that is defined as an access is displayed with the access name and description rather than with the group name and description. Only accounts and groups that require a recertification decision are displayed.



This table might not be displayed, depending on:

- The configuration of the user recertification policy.
- The accounts and groups, if any, that are owned by the user.

The table contains these columns:

Accounts and Groups

Identifies the accounts and any groups associated with each account. Accounts are identified using the user ID and the name of the service on which they reside.

Click the  icon to collapse the table and list accounts only. Click the  icon to expand the table and list all accounts and the groups associated with each account. You can also expand or collapse by account. These options are displayed only if there are one or more groups associated with an account.

Ownership Type

Displays the ownership type specified for the account. Ownership types are governed by the provisioning policy of the service.

Description

Provides additional information about the account or group.

Still Required

Select whether the user needs one or more accounts and groups.

If the user still requires the account or group, select **Yes** to recertify the account or group. If the user no longer requires the account or group, select **No** to reject the account or group.

Because of the relationship that exists between accounts and groups, an account recertification selection of **No** applies to all groups associated with the account.

Select **All** to recertify all accounts and groups. You can also select **All** for each account to select the account and all groups associated with the account.

Select **None** to reject all accounts and groups. You can also select **None** for each account to reject recertification on the account and all groups associated with the account.

Note: Some accounts might be displayed in the table for information purposes if groups on the accounts require recertification, but the accounts themselves are required by the user and are not subject to recertification. In other words, the account is included on the page, but you cannot act on it.

Preview the impact of your selections

Click to view the impact that your selections have on the roles, accounts, and groups of the user being recertified. Impacted items can include roles, accounts, and groups that are not included in the recertification activity. For example, when you select a role as not required, it might affect accounts and groups owned by the user. It might also affect accounts and groups owned by the user that are not part of the recertification activity.

Comments

Provide additional comments and justification for your actions.

To complete the activity, click **Submit**.

To save your current selections and return to the **Approve and Review Requests** page without submitting the activity, click **Save as Draft**. When you or another user returns to complete the activity, the activity displays the selections that were previously made. However, if the activity passes its due date before the activity is completed, an automatic timeout action treats the activity as if no selections were made.

To return to the list of activities and cancel your action, click **Close**.


Related information

For more information, see the [IBM Knowledge Center](#).

Success

Use this page to confirm that you have successfully completed recertification of the user's roles, accounts, and groups.

Choices submitted

Click the  icon to view the recertification choices you submitted. The choices are divided into two tables, which include a list of roles and a list of account and group items associated with the user.

Roles table

Lists the roles. This table might or might not be displayed, depending on the configuration of the user recertification policy, and whether or not the user has any roles. The table contains these columns:

Roles

Identifies the name of the role.

Description

Provides additional information about the role.

Still Required



Indicates your choice for whether the user still requires the role.

Accounts and Groups table

Lists the accounts and groups. A group that is defined as an access is displayed with the access name and description rather than with the group name and description. Only accounts and groups that require a recertification decision are displayed. This table might or might not be displayed, depending on the configuration of the user recertification policy and the accounts and groups, if any, that are owned by the user. The table contains these columns:

Accounts and Groups

Identifies the accounts and any groups associated with each account. Accounts are identified using the user ID and the name of the service on which they reside.

Click the  icon to collapse the table and list accounts only. Click on the  icon to expand the table and list all accounts and the groups associated with each account. You can also expand or collapse by account. These options are displayed only if there are one or more groups associated with an account.

Description

Provides additional information about the account or group.

Still Required

Indicates whether or not you specified that the user still requires the account or group.

Note: Some accounts might be displayed in the table for information purposes if groups on the accounts require recertification, but the accounts themselves are required by the user and are not subject to recertification. In other words, the account is included on the page, but you cannot act on it.

Related information

For more information, see the [IBM Knowledge Center](#).

Approval Details

Use this page to approve or reject an access or account activity.

Depending on the activity, some of these fields might not be displayed.

Request type

Displays the type of request that was submitted. Click the name of the request type to view the request details.

Service name

Displays the name of the service associated with the account.

Submission date

Displays the date and time when the request was submitted.

Due date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested for

Displays the user for whom the request was submitted. Click the name of the user to view the user's personal profile.

Requested by

Displays the user who submitted the request. Click the name of the user to view the user's personal profile.

Instructions

Displays detailed instructions for the activity as specified by the activity notification.

Comments

Type a justification for whether you approve or reject the access or account activity.

You can use these buttons:

:

Approve

Click to approve the activity. Depending on how the workflow is configured, either the access or account is created, or the workflow proceeds to the next step.

Reject

Click to reject the access or account activity. The activity is complete.

Related information

For more information, see the [IBM Knowledge Center](#).

Grouped Approval Details

Use this page to view details about a group approval activity.

Request type

Displays the type of request that was submitted. Click the name of the request type to view the request details.

Service name

Displays the name of the service associated with the account.

Submission date

Displays the date and time when the request was submitted.

Due date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested for

Displays the user for whom the request was submitted. Click the name of the user to view the user's personal profile.

Requested by

Displays the user who submitted the request. Click the name of the user to view the user's personal profile.

Related information

For more information, see the [IBM Knowledge Center](#).

Complete a Grouped Approval

Use this page to approve or reject a collection of account activities. Approvals are grouped automatically by the system and allow you to process the activities individually or collectively.



Activities table

Lists the grouped approvals. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an activity. To select one or more activities, select the check box adjacent to the activity. To select all activities, select the check box at the top of the column.

State

Identifies the state of the approval. It is either locked by you () , locked by another user () , or unlocked.

Due date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested for

Identifies the user who requires an account. Click the name of the user to view the user's personal profile.

Subject

Identifies the name of the account or service that the activity was created for. Click to specify additional information about the activity.

Request type

Identifies the type of request associated with the activity.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Comments

Type a justification for whether you approve or reject the account activity.

Use these buttons:

Approve

Click to approve the activity. Depending on how the workflow is configured, the access or account is created, or the workflow proceeds to the next step.

Reject

Click to reject the access or account activity. The activity is complete.

Lock

Click to lock the selected item. While the other users can view the activity, they cannot process it.

Unlock

Click to unlock a selected item. The user that locked the item must unlock it.

Assign

Click to assign the selected activity to someone else to complete.

Related information

For more information, see the [IBM Knowledge Center](#).



Provide Information for a Grouped RFI

Use this page to provide information for a collection of request for information (RFI) activities. The system automatically groups RFI activities, allowing you to process the activities individually or collectively.

Activities table

Lists the grouped activities. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

State

Identifies the state of the activity. It is either locked by you () , locked by another user () , or unlocked.

Due date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested for

Displays the user for whom the request was submitted. Click the name of the user to view the user's personal profile.

Subject

Identifies the name of the account or service that the activity was created for. Click to provide information for the activity.

Request type

Identifies the type of request associated with the activity.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

RFI Details

Use this page to review additional details about the request for information (RFI) activity and to provide information about the activity.

Request type

Displays the type of request that was submitted. Click the name of the request type to view the request details.

Service name

Displays the name of the service associated with the account.

Submission date

Displays the date and time when the request was submitted.

Due date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested for

Displays the user for whom the request was submitted. Click the name of the user to view the user's personal profile.

Requested by

Displays the user who submitted the request. Click the name of the user to view the user's personal profile.

Instructions

Displays detailed information about the request.

Click **Provide Information** to specify the information that is required by the activity.

Related information

For more information, see the [IBM Knowledge Center](#).

Provide Information

Use this notebook to provide information for an account.

The pages that are displayed in the notebook vary, depending on the type of service that you selected and by the authority that the system administrator has granted you. For example, for the AIX service, the Account information, Access information, and Administration choices pages might be displayed.

The fields that are displayed on these pages also vary, depending on the type of service that you selected and by the authority that the system administrator has granted you.

Type the appropriate values in the fields that are displayed and click **Submit**.

The following topics define the default service attributes for the default services. For information about other service attributes, see your system administrator.

Related information

For more information, see the [IBM Knowledge Center](#).

AIX Default Attributes

For the AIX service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Access information page**UNIX Shell**

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the read, write, and execute permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the access used by the account as a default change file mode value for the user home directory.

Administration choices(1) page**Force a password change?**

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as the secondary group of the user.

Groups that can use the su command on this user

Specify the name of the group that can use the UNIX **su** command on the user.

Groups to be administered

Specify the groups to administer.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before the date that a password expires that a warning is issued to the user.

Administrative roles

Specify the administrative roles for the user.

Additional mandatory methods for authenticating the user

Specify other mandatory authentication methods.

Additional optional methods for authenticating the user

Specify other optional authentication methods.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices(2) page

Audit class

Specify the list of audit classes for the user.

Allow user to execute daemon process?

Select this check box to enable the user to run daemon processes on the system.

Allow user to log in to the system?

Select this check box to enable the user to log directly into the system.

Allow user to remotely login to the system?

Select this check box to enable the user to log into the system remotely.

Can another user switch user to this user?

Select this check box to enable another user to use the UNIX **su** command on this user.

Is this user an administrator?

Select this check box to designate the user as an administrator of the system.

Trusted path status

Select the default trusted path status for the account.

always

Specifies that the user that is confined to the trusted path.

/notsh

Specifies that the user session ends if the secure attention key (SAK) signal is detected.

nosak

Specifies that the SAK key is disabled.

on

Specifies that the standard trusted path management is used.

Soft limit for largest core size

Specify the soft limit for the largest core file that the user's process can create.

Soft limit for maximum amount of CPU utilization

Specify the soft limit for the largest amount of system unit time (in seconds) that the user's process can use.

Soft limit for largest data segment

Specify the soft limit for the largest process data segment for the user's process.

Soft limit for largest file size

Specify the soft limit for the largest file that the user's process can create or extend.

Soft limit for largest stack segment

Specify the soft limit for the largest process stack segment for the user's process.

Largest core size

Specify the largest core file that the user's process can create.

Maximum CPU utilization

Specify the largest amount of system unit time (in seconds) that the user's process can use.

Largest data segment

Specify the largest process data segment for the user's process.

Largest file size

Specify the largest file that the user's process can create or extend.

Largest stack segment

Specify the largest amount of physical memory that the user's process can allocate.

Allowed login time

Specify the days and times that the user is allowed to access the system.

Allowed number of login retries before locking the account

Specify the number of failed login attempts before the account is locked.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in weeks) that the account can remain active after the password for the account has expired.

Minimum alphabetic characters in password

Specify the minimum number of alphabetic characters that must be included in the password for the account.

Minimum difference between the current and last password

Specify the minimum number of characters that are required in a new password that were not in the old password.

Maximum number of characters that can be repeated in a password

Specify the maximum number of characters in a password that can be repeated.

Minimum length of the password

Specify the minimum length of the password.

Password restriction methods

Specify password restriction methods to the account.

Password dictionaries used to restrict passwords

Specify the password dictionary files that are used to restrict which passwords can be used by the account.

Number of previous passwords that cannot be reused

Specify the number of passwords to be kept in the password history.

Account last accessed on

Specify a value for the last access date and time.

Valid terminals allowed to access the account

Specify which terminals can log in using this account.

System authentication mechanism for the user

Specify the authentication mechanism the system uses to authenticate the user.

Authentication registry where the user is administered

Specify the registry that is used for authenticating the user.

Related information

For more information, see the [IBM Knowledge Center](#).

HP-UX Default Attributes

For the HP-UX service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page

UNIX Shell

Specify a default command shell for the account.

Force a password change?

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the names of the groups to use as secondary groups of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Allow at jobs?

Select this check box to enable this account to run an *at* job.

Allow cron jobs?

Select this check box to enable this account to run a *cron* job.

Administration choices page

Password warning age

Specify the number of days before the date that a password expires that a warning is sent to the user.

Maximum number of days (weeks for AIX) the account can remain valid after the password expires

Specify the maximum time that the account can remain active after the password for the account has expired.

Number of days the account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allowed number of login retries before locking the account

Specify the number of login attempts that can occur before the account is locked.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Although you can specify a time, this feature is disabled and you can only set an account expiration date. Alternatively, select **Never** to set the account to never expire.

Related information

For more information, see the [IBM Knowledge Center](#).

LDAP Default Attributes

For the LDAP service type, IBM Security Identity Manager provides a set of default attributes.

User page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

User Container

Click **Search** to search for the location in the LDAP tree where you want to add the user.

Full name

Type a value for distinguishing users, for example, the full name of the user.

Preferred user ID

Type the user ID. This determines the default user ID that new accounts and access use when they are created.

Last name

Type the last name of the user.

First name

Type the first name of the user.

Initials

Type the initials of the user.

E-mail address

Type the e-mail address of the user.

Display name

Type the name of the user that you want to be displayed in the IBM Security Identity Manager interface.

Description

Type information about the intended purpose of the account.

Home telephone number

Type the home telephone number of the user.

Mobile telephone number

Type the mobile telephone number of the user.

Pager

Type the pager number of the user.

Business page**Title**

Type the business title of the user.

Employee number

Type the employee number of the user.

Employee type

Type the employment specification of the user, such as regular, contractor, or business partner.

Manager

Type the name of the manager of the user.

Administrative assistant

Type the name of the assistant of the user.

Business category

Type the business category type of the user.

Department number

Type the department number of the user.

Telephone number

Type the business telephone number of the user.

Fax number

Type the business fax number of the user.

Postal address

Type the business postal address of the user.

Office number

Type the office location of the user.

Location name

Type the locale of the user.

Address page**Registered address**

Type the registered address of the user.

Street

Type the street name of the registered address.

State

Type the state in which the user resides.

Destination indicator

Type an applicable destination indicator.

Physical delivery office name

Type the name of the physical address.

Home address

Type the home address of the user.

Postal code

Type the postal code of the user.

Post office box

Type the post office box number of the user.

Preferred delivery method

Type the preferred method of delivery of the user.

Other page**Driver license**

Type the driver's license number of the user.

Preferred language

Type the preferred language of the user.

Teletex terminal ID

Type the teletex terminal ID of the user.

Telex number

Type the teletex number of the user.

Related information

[For more information, see the IBM Knowledge Center.](#)

Linux Default Attributes

For the Linux service type, IBM Security Identity Manager provides a set of default attributes.

Employee information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX shell**

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

This field is not supported for Linux operating systems.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices pages**Force a password change?**

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Specify the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Specify the maximum number of days that the password for the account is valid.

Password minimum age

Specify the minimum number of days that the password for the account is valid.

Password warning age

Specify the number of days before expiration that a password expiration warning is issued to the user.

Maximum number of days the account can remain valid after the password expires

Specify the maximum time (in days) that the account can remain active after the password for the account has expired.

Related information

For more information, see the [IBM Knowledge Center](#).

Solaris Default Attributes

For the Solaris service type, IBM Security Identity Manager provides a set of default attributes.

Account information page

The following list contains the default attributes. The administrator can remove attributes from or add attributes to the list.

For more information about other attributes, refer to your specific adapter installation and configuration guide.

User ID

Type the login user ID for the user.

Gecos (comments)

Type general descriptive information about the user.

UID number

Type the user ID number for the user.

Allow duplicate UIDs?

Select this check box to allow the group ID to be duplicated (non-unique).

Access information page**UNIX Shell**

Specify a default command shell for the account.

Account expiration date : Date

Specify a date for when the account expires.

Account expiration date : Time

Specify a time that the account expires on the date specified in the **Account expiration date : Date** field. Alternatively, select **Never** to set the account to never expire.

UNIX umask

Specify the permissions to be used by the account for a default file creation mask.

Home directory permissions

Specify the permissions to be used by the account as a default change file mode value for the user home directory. Set these permissions to enable deleting the home directory when the user account is deleted, if you also select **Delete home directory when the account is deleted** for the service.

Administration choices page**Force a password change?**

Select this check box to force the user to change the password for this account when logging in for the first time.

Primary group

Specify the name of the group to use as the primary group of the user.

Secondary group

Specify the name of the group to use as a secondary group of the user.

Home directory

Type the fully qualified UNIX path for the home directory of the user account.

Password maximum age

Type the maximum number of weeks that the password for the account is valid.

Password minimum age

Type the minimum number of weeks that the password for the account is valid.

Password warning age

Type the number of days before expiration that a password expiration warning is issued to the user.

Number of days account can remain idle

Specify the maximum time (in days) that the account can remain idle.

Allow at jobs?

Select this check box to allow this account to run an *at* job.

Allow cron jobs?

Select this check box to allow this account to run a *cron* job.

Related information

For more information, see the [IBM Knowledge Center](#).

Local Groups

Use this page to select local groups.

Lists the groups based on the search you requested. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box adjacent to the group. To select all groups, select the check box at the top of the column.

Name

Identifies the name of the local group.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

[For more information, see the IBM Knowledge Center.](#)

Work Order Details

Use this page to view details about a work order and to complete the work order.

Request type

Displays the type of request that was submitted. Click the name of the request type to view the request details.

Service name

Displays the name of the service associated with the account.

Submission date

Displays the date and time when the request was submitted.

Due date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested for

Displays the user for whom the request was submitted. Click the name of the user to view the user's personal profile.

Requested by

Displays the user who submitted the request. Click the name of the user to view the user's personal profile.

Instructions

Displays instructions for completing this work order.

Comments

Optional. Type information in this field describing why you failed the work order. A user can view this information and submit the work order again.

You can use these buttons:

Successful

Click if you completed the work order. Depending on how the workflow is configured, the work order either completes or proceeds to the next step.

Warning

Click if the work order is only partially complete.

Failure

Click if you cannot complete the work order.

Related information

For more information, see the [IBM Knowledge Center](#).

Complete a Grouped Work Order

Use this page to complete a collection of work order activities. The system automatically groups the work orders, allowing you to process the activities individually or collectively.



Activities table

Lists the grouped work orders. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a work order. To select one or more work orders, select the check box adjacent to the work order. To select all work orders, select the check box at the top of the column.

State

Identifies the state of the work order. It is either locked by you () , locked by another user () , or unlocked.

Due date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested for

Identifies the user who submitted the request. Click the name of the user to view the user's personal profile.

Subject

Identifies the name of the account or service that the work order was created for. Click to review the work order details.

Request type

Identifies the type of request associated with the activity.

Comments

Specify information about these work orders.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Successful

Click if you completed the work orders. Depending on how the workflows are configured, the work orders either complete or proceed to the next step.

Warning

Click if you partially completed the work orders. If there are additional steps in the workflows, the work orders do not proceed.

Failure

Click if you cannot complete the work orders. The work orders are complete.

Related information

For more information, see the [IBM Knowledge Center](#).

Grouped Compliance Alerts

Use this page to correct or defer compliance alerts.

Activities table

Lists the activities that are associated with a compliance alert. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an activity. To select one or more activities, select the check box adjacent to the activity. To select all activities, select the check box at the top of the column.

State

Identifies the state of the compliance. It is either locked by you (🔒), locked by another user (🔒👤), or unlocked.

Due Date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested For

Identifies the user whose account is noncompliant. Click the name of the user to view the user's personal profile.

Subject

Displays the user ID for the noncompliant account. Click the name of the user to view the user's personal profile.

Request Type

Identifies the type of request associated with the activity.

Service Name

Identifies the name of the service on which the noncompliance was found.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Comments

Provides an optional field for information about correcting the noncompliance alert.

You can use these buttons:

Click **Correct** to correct a noncompliant account.

Click **Defer** to take action on a noncompliant account at a later time.

Related information

For more information, see the [IBM Knowledge Center](#).

Compliance Alert Details

Use this page to view details about a compliance alert and correct or defer the compliance violation.

Request type

Identifies the type of request associated with the activity. Click the name of the request type to view more information.

Service name

Identifies the name of the service on which the noncompliance was found.

Submission date

Identifies the date and time when the compliance alert was submitted.

Due Date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested for

Identifies the user whose account is noncompliant. Click the name of the user to view the user's personal profile.

Requested by

Identifies the user who made the request. Click the name of the user to view the user's personal profile.

Instructions

Provides information on why the account is noncompliant, and information on correcting the compliance.

Comments

Provides an optional field for information about correcting the noncompliance alert.

Compliance details

Provides detailed information on the compliance.

You can use these buttons:

Click **Correct** to correct a noncompliant account.

Click **Defer** to take action on a noncompliant account at a later time.

Related information

For more information, see the [IBM Knowledge Center](#).

Compliance Correction

Use this page to correct account attributes.

Noncompliant Attributes table

Lists the account attributes that are associated with a compliance alert. You can choose to correct only a subset of attributes. If you correct only a subset of attributes, a new activity is displayed with any attributes you have not corrected. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an attribute. To select one or more attributes, select the check box adjacent to the attribute. To select all attributes, select the check box at the top of the column.

Attribute

Identifies a noncompliant attribute.

Old Value

Identifies the existing, noncompliant value of the attribute.

New Value

Identifies the value the attribute should have, based on a provisioning policy.

Access Violation

Indicates that a noncompliant value also caused an access entitlement violation. If this field is blank, the noncompliant value has no relation to any access definition for the service. This column is not displayed if no values are present in the table.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Defer Compliance Alert

Use this page to defer compliance alerts for a specified period of time.

Explanation

Optional. Provide a reason for deferring correction.

Defer for (days)

The number of days you can defer a correction. The maximum value is determined by the policy enforcement setting that is set by your system administrator.

Related information

For more information, see the [IBM Knowledge Center](#).

Recertification Details

Use this page to perform a recertification activity.

Request type

Displays the type of request that was submitted. Click the name of the request type to view the request details.

Service name

Displays the name of the service associated with the account.

Submission date

Displays the date and time when the recertification request was submitted.

Due date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested for

Identifies the user who requires recertification. Click the name of the user to view the user's personal profile.

Requested by

Displays the user who submitted the request. Click the name of the user to view the user's personal profile.

Instructions

Displays detailed instructions for the activity as specified by the activity notification.

Comments

Type a justification for the recertification activity.

You can use these buttons:

Select **Approve** to approve recertification.

Select **Reject** to reject recertification.

Related information

For more information, see the [IBM Knowledge Center](#).

Complete a Grouped Recertification

Use this page to perform a collection of recertification activities. Recertifications are grouped automatically by the system and allow you to process the activities individually or collectively.



Activities table

Lists the grouped recertifications. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an activity. To select one or more activities, select the check box adjacent to the activity. To select all activities, select the check box at the top of the column.

State

Identifies the state of the recertification. It is either locked by you () , locked by another user () , or unlocked.

Due date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested for

Identifies the user who requires recertification. Click the name of the user to view the user's personal profile.

Subject

Identifies the name of the account or service that the recertification was created for.

Request type

Identifies the type of request associated with the activity.

Comments

Type a justification for your recertification action.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Select **This access/account is still required** to approve recertification.

Select **This access/account is no longer required** to reject recertification.

Related information

For more information, see the [IBM Knowledge Center](#).



Grouped User Recertification Activities

Use this page to complete a collection of user recertification activities. The system automatically groups activities.

Activities table

Lists the grouped user recertification activities. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

State

Identifies the state of the activity. It is either locked by you () , locked by another user () , or unlocked.

Due Date

Identifies the date and time by which you must complete the activity. An activity that passes this date either forwards to a defined escalation participant, ends automatically, or remains available as an overdue activity.

Requested For

Identifies the user requiring recertification. Click the name of the user to view the user's personal profile.

Subject

Identifies the user requiring recertification. Click to open and complete the user recertification activity.

Request Type

Identifies the type of request associated with the activity.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Preview Impact

Use this page to preview the impact your user recertification approval choices have on roles, accounts, and groups.

This page displays only those roles, accounts, and groups that are no longer required as a result of your recertification decisions. Some accounts and groups might be impacted and listed on this page even if they are not displayed in the recertification activity. For example, if you specify that the user no longer requires a role, the user might own accounts and groups that depend on the role.

Roles No Longer Required table

Lists the roles that you specified that the user no longer requires. The table contains these columns:

Roles

Identifies the name of the role.

Description



Provides additional information about the role.

Accounts and Groups No Longer Required table

Lists the accounts and groups that the user no longer requires. The table contains these columns:

Accounts and Groups

Identifies the accounts and any groups associated with each account. Accounts are identified using the user ID and the name of the service on which they reside. All impacted groups and accounts are displayed here, even if they are not displayed in the recertification activity.

Click the  icon to collapse the table and list accounts only. Click the  icon to expand the table and list all accounts and the groups associated with each account. You can also expand or collapse by account. These options are displayed only if there are one or more groups associated with an account.

Impact

Displays the impact to the account or group that is listed. The impact is *specified as not required* (✖) if you specified the account or group as not required in the recertification activity. The impact is *implied as not required* (☒✖) if the account or group is dependent on one or more roles or accounts that you specified as not required in the recertification activity.

Ownership Type

Displays the ownership type specified for the account. Ownership types are governed by the provisioning policy of the service.

Description

Provides additional information about the account or group.

Impacted By

Identifies the roles or the account that is impacting the account or group and causing it to be *implied as not required*. This column can contain either one account or one or more roles. To prevent the account or group from being impacted, go back to the **Review Request** page. Try recertifying an account or role that is listed in the **Impacted By** column. Then, preview the impact again to ensure that the account or group is no longer impacted.

Manage Delegation Schedules

Use this page to delegate your activities to other authorized users. When delegating your activities, specify schedules that do not overlap.

Delegation table

Lists the schedules that you have created to delegate your activities to other authorized users.

Select

Specifies a delegation schedule. To select one or more delegation schedules, select the check box adjacent to the schedule. To select all delegation schedules, select the check box at the top of the column.

Login ID

Identifies the ID of the IBM Security Identity Manager user account to which you are delegating your activities. Click the login ID to change the delegation time period.

Name

Specifies the name of the user to whom you have delegated your activities for the period of time selected.

Status

Specifies the status of the IBM Security Identity Manager user account to which you are delegating your activities.

Start Date

Specifies the date and time when delegation begins.

End Date

Specifies the date and time when delegation ends.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

You can use these buttons:

Add

Click to add another delegation schedule.

Change

Click to change a delegation schedule. This button is disabled if there are no items in the table.

Delete

Click to delete a delegation schedule. This button is disabled if there are no items in the table.

Related information

For more information, see the [IBM Knowledge Center](#).

Set Up Delegation

Use this page to delegate approvals and other activities, and to select dates and times for the delegation interval. Ensure that the user you select as a participant for workflow activities is able to access the activities list.

Delegate to

Select the name of the user to which you want to delegate your activities. Click **Search** to choose from a list of available users.

You can delegate activities only to users having the same authority as you and who belong to the same group. For example, as a manager, you can delegate your activities to other managers.

Your activities can be delegated only to one user. If your activities are delegated to one user, and then you delegate them to another user without stopping the first delegation, the second delegation replaces the first one.

Start date

Click the calendar icon to select the date that the delegation starts. The default date is the current date.

Start time

Click the clock icon to select the time of day that the delegation starts. The default time is the current time.

End date

Click the calendar icon to select the date that the delegation ends. The default date is the current date.

End time

Click the clock icon to select the time of day that the delegation ends. The default time is the current time.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Login Account

Use this page to select a login account to which you want to delegate activities.

Accounts table

The **Accounts** table displays the accounts that you can select. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Select the radio button in this column to select a login account to which you want to delegate activities.

User ID

Identifies the user ID associated with the account.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Assign Activities

Use this page to assign an activity to another authorized user to complete. The activities must be assigned to a group of users.

Users table

Lists the users who can complete the activities. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Click the radio button in this column to select an activity.

User Name

Identifies the user's full name. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the user's e-mail address.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click **Assign** to assign the activities to another authorized user. The activity is locked for the person that you assigned it to.

Related information

For more information, see the [IBM Knowledge Center](#).

View Request Details

Use this page to view the details of an account activity.

Request type

Displays the type of request that was submitted.

Service name

Displays the name of the service associated with the request.

Date submitted

Displays the date and time when the request was submitted.

Service information

Displays the description of the service for which the request was made.

Requested changes table

Lists the details of the selected request. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Attribute

The attribute associated with the request.

Requested value

The value of the attribute.

Submitted value

The submitted value of the attribute.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Delegate Account

Use this page to search for and select an account for delegation. Ensure that the selected user has permission to process the activities that are delegated.

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search Results table

Lists the users matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Click the radio button in this column to select a user.

User ID

Identifies the user ID of the user to whom you want to delegate.

Owner

Identifies the owner of the IBM Security Identity Manager account to whom you want to delegate.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Success

This page confirms that you have successfully completed your task.

Click a related task you might want to perform.

Related information

For more information, see the [IBM Knowledge Center](#).

Message

Use this page to view a message about an action you attempted. Click the message ID for additional information.

Related Tasks

Identifies other related tasks you can perform upon receiving this message.

Related information

For more information, see the [IBM Knowledge Center](#).

About

Use this page to view information about the system.

Server name

Displays the server name. In a cluster configuration, this is the server name for the user's current session.

Version

Displays the version of IBM Security Identity Manager software that you are using.

Build number

Displays the current build number for the version of IBM Security Identity Manager that you are using.

Maintenance level

Displays the last fixpack level that was installed for the version of IBM Security Identity Manager that you are using.

Build date

Displays the date on which the last build occurred.

Build time

Displays the exact time and the time zone in which the last build occurred.

Related information

For more information, see the [IBM Knowledge Center](#).

Common Helps

Advanced Search

Enter Search Filter

Use this page to specify an LDAP filter to use in your search.

Type the LDAP filter statements that select your search targets and click **Search**.

Related information

For more information, see the [IBM Knowledge Center](#).

Add User

Use this page to locate users.

Search information

Type a string (or a portion of the string) for the attribute value for the user that you want to find. If you do not type a value in this field or if you type an asterisk (*), and then click **Search**, the entire list of users is displayed as long as the number of users does not exceed the search limit.

Attribute

Click **User name** or **User ID** to search by the user's name or ID.

Users table

Lists the users matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

User Name

Identifies the user's full name. Click the name of the user to view the user's personal profile.

User ID

Identifies the user's last name.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select People

Use this page to locate a person that you want to select.

Attribute

Select an attribute on which to search.

Operator

Select an operator for the search argument, such as Contains.

Value

Type a value that the attribute might have, such as all or part of a person's full name.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

User table

Lists the users matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box adjacent to the role. To select all roles, select the check box at the top of the column.

Person Name

Identifies the name of the person. Click the name for more information about the person.

E-mail Address

Provides additional information about the role.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Advanced Search

Use this page to specify the criteria used to search for a user.

User type

Select either a person or a business partner person. Click **Change** to change the user type.

Full name

Type all or part of the name of the user you want to locate.

Business unit

Click **Search** to specify the business unit that contains the user.

Click **Clear** to remove the selected business unit.

Select the **Include subunits** check box to include any subunits for the specified business unit.

Status

Select whether the search returns a user with active, inactive, or with any status.

Add a search field

Click to add additional search objects, such as an employee number.

You can use these buttons:

Search

Click to search for the user.

Search filter

Click to specify an LDAP filter for the search.

Related information

For more information, see the [IBM Knowledge Center](#).

Select User Type

Use this page to specify the type of users to search for.

Select

Click a radio button to select a specific user type.

User type

Displays the user type, such as a person or a business partner person.

Related information

For more information, see the [IBM Knowledge Center](#).

Advanced Search

Use this page to specify the criteria to search for an account.

These fields represent preset and customized advanced search fields. The actual fields might vary depending on the customized filters your system administrator has chosen.

Account type

Displays the account type for the service on which the account exists. You can change the account type, if you are using advanced search from Manage Users. The account type is pre-filled if you are using advanced search from Manage Services and cannot be changed.

User ID

Type the user ID.

Full name

Type the full name of the user.

Description

Type a description of the account.

User comment

Type a comment about the account.

Local groups

Specify a group that is entitled to the account. Click **Add** to add a group.

E-mail address

Specify an e-mail address that is associated with the account.

Telephone number

Specify a telephone number that is associated with the account.

Status

Select whether to search all accounts, or only active or inactive accounts.

Compliance Status

Select whether to search all accounts, or only compliant or noncompliant accounts.

Owner

Click **Browse** to select an account owner.

Add another search field

Select additional attributes to qualify your search.

You can use these buttons:

Search

Click to search for an account.

Search filter

Click to specify an LDAP filter for your search criteria.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Accounts

Use this page to select accounts.

Attribute

Select the name or description of the account.

Operator

Select an operator for the search argument, such as Contains.

Value

Type a value, which is all or part of the account name or description.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Accounts table

Lists the accounts matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account. To select one or more accounts, select the check box adjacent to the account. To select all accounts, select the check box at the top of the column.

Account Name

Identifies the name of the account. Click the name of the account for more information about the account.

Description

Provides additional information about the account.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Admin Domains

Use this page to select admin domains.

Attribute

Select the name or description of the admin domain.

Operator

Select an operator for the search argument, such as Contains.

Value

Type a value, which is all or part of the admin domain name or description.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Admin domains table

Lists the admin domains matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an admin domain. To select one or more admin domains, select the check box adjacent to the admin domain. To select all admin domains, select the check box at the top of the column.

Admin Domain Name

Identifies the name of the admin domain. Click the name of the admin domain for more information about the admin domain.

Description

Provides additional information about the admin domain.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Business Partner Unit

Use this page to select business partner units.

Attribute

Select the name or description of the business partner unit.

Operator

Select an operator for the search argument, such as Contains.

Value

Type a value, which is all or part of the business partner unit name or description.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Business Partner Unit table

Lists the business partner units matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a business partner unit. To select one or more business partner units, select the check box adjacent to the business partner unit. To select all business partner units, select the check box at the top of the column.

Business Partner Unit Name

Identifies the name of the business partner unit. Click the name of the business partner unit for more information about the business partner unit.

Description

Provides additional information about the business partner unit.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Directories

Use this page to select directories.

Attribute

Select the name or description of the directory.

Operator

Select an operator for the search argument, such as Contains.

Value

Type a value, which is all or part of the directory name or description.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Directories table

Lists the directories matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a directory. To select one or more directories, select the check box adjacent to the directory. To select all directories, select the check box at the top of the column.

Directory Name

Identifies the name of the directory. Click the name of the directory for more information about the directory.

Description

Provides additional information about the directory.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Groups

Use this page to select groups.

Attribute

Select the name, description or category of the group.

Operator

Select an operator for the search argument, such as Contains.

Value

Type a value, which is all or part of the group name, description, or category.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Groups table

Lists the groups matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box next to the group. To select all groups, select the check box at the top of the column.

Group Name

Identifies the name of the group. Click the name of the group for more information about the group.

Description

Displays information about the intended purpose of the group.

View

Identifies the view of tasks that users have in this group.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Locations

Use this page to select locations.

Attribute

Select the name or description of the location.

Operator

Select an operator for the search argument, such as Contains.

Value

Type a value, which is all or part of the location name or description.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Locations table

Lists the locations matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a location. To select one or more locations, select the check box adjacent to the location. To select all locations, select the check box at the top of the column.

Location Name

Identifies the name of the location. Click the name of the location for more information about the location.

Description

Provides additional information about the location.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Organizations

Use this page to select organizations.

Attribute

Select the name or description of the organization.

Operator

Select an operator for the search argument, such as Contains.

Value

Type a value, which is all or part of the organization name or description.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Organizations table

Lists the organizations matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an organization. To select one or more organizations, select the check box adjacent to the organization. To select all organizations, select the check box at the top of the column.

Organization Name

Identifies the name of the organization. Click the name of the organization for more information about the organization.

Description

Provides additional information about the organization.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Organizational Units

Use this page to select organizational units.

Attribute

Select the name or description of the organizational unit.

Operator

Select an operator for the search argument, such as Contains.

Value

Type a value, which is all or part of the organizational unit name or description.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Organizational Units table

Lists the organizational units matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an organizational unit. To select one or more organizational units, select the check box adjacent to the organizational unit. To select all organizational units, select the check box at the top of the column.

Organizational Unit Name

Identifies the name of the organizational unit. Click the name of the organizational unit for more information about the organizational unit.

Description

Provides additional information about the organizational unit.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select ITIM Users

Use this page to select users who have a system account on the ITIM service.

Attribute

Select a system attribute to search by, such as User ID.

Operator

Select an operator to apply to the search, such as Contains.

Value

Type information about the system account, such as the user ID.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

ITIM Users table

Lists the system accounts matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a system account. To select one or more system accounts, select the check box adjacent to the system account. To select all system accounts, select the check box at the top of the column.

User Name

Indicates the name of the owner of the system account that fits the search criteria.

User ID

Identifies the ID of the system account.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Business Unit

Use this page to select a business unit.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Organization

Organizations that have the organization name or description in the search information field.

Organizational Unit

Organizational units that have the organizational unit name or description in the search information field.

Location

Locations that have the location name or description in the search information field.

Admin Domain

Admin domains that have the admin domain name or description in the search information field.

Business Partner Organization Unit

Business partner units that have the business partner name or description in the search information field.

Business Units Found table

Lists the business units matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a business unit. To select one or more business units, select the check box adjacent to the business unit. To select all business units, select the check box at the top of the column.

Name

Identifies the name of the business unit. Click the link for more information about the business unit.

Parent

Identifies the parent business unit name of the business unit.

Description

Provides additional information about the business unit.

Type

Identifies the type of business unit, such as organization, organizational unit, or location.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Organizational Roles

Use this page to select organizational roles.

Attribute

Select the description or name of the role.

Operator

Select a Boolean operator for the search argument, such as Contains.

Value

Type a value, which is all or part of the role name or description.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Roles table

Lists the roles matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a role. To select one or more roles, select the check box next to the role. To select all roles, select the check box at the top of the column.

Name

Identifies the name of the role.

Description

Provides additional information about the role.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

Role Type

Indicates whether the role is static or dynamic.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.

- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Access Entitlement Search

Use this page to find the access entitlement that you want.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Access Entitlements table

Lists the users matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an access entitlement. To select one or more access entitlements, select the check box adjacent to the access entitlement. To select all access entitlements, select the check box at the top of the column.

Access Name

Identifies the name of the access entitlement.

Access Type

Identifies the type of access entitlement, such as an application or shared folder.

Access Description

Provides a brief description of the access entitlement.

Service Name

Identifies the name of the service associated with the access entitlement.

Access Owner

Identifies the owner of the access entitlement.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Miscellaneous Common Helps

Success

This page confirms that you have successfully completed your task.

Click a related task you might want to perform.

Related information

For more information, see the [IBM Knowledge Center](#).

Confirm

Use this page to verify that you want to complete the requested action. The **Confirm** page is displayed for requests that can have a detrimental effect on your system.

Verify that the action specified in the message displayed is what you want to be done and click the appropriate button.

Related information

For more information, see the [IBM Knowledge Center](#).

Confirm

Use this page to verify that you want to complete the requested action.

Verify that the action specified in the message displayed is what you want done.

Immediate

Runs the request immediately, after you click a button for your requested action.

Effective date

Runs the request at a date and time that you set. After you select this option, click the calendar and clock icons to specify the scheduled date and time.

Related information

For more information, see the [IBM Knowledge Center](#).

Message

Use this page to view a message about an action you attempted. Click the message ID for additional information.

Related Tasks

Identifies other related tasks you can perform upon receiving this message.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a User

Use this page to search for a user.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select an attribute from the list. All searchable attributes and the personal profile are included in this list. If you select an attribute, the search is based on that attribute. If you select **Entire profile**, the search is based on all attributes associated with the user.

Last Name searches for the user's last name.

Full Name searches for the user's full name.

E-mail Address searches for the user's e-mail address.

Entire Profile searches all attributes associated with the user.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Users table

Lists the users matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

Name

Identifies a value for distinguishing a user, such as the user's full name. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the user's e-mail address.

Custom Display

Identifies a custom display attribute.

Business Unit

Identifies the business unit to which the role applies. Click the link for more information about the business unit.

Status

Identifies the user's status.

Users are either active or inactive. A user must be active to log in to the system. Users become inactive when they are suspended. The suspended users still exist, but they cannot access the system. System administrators can restore inactive users.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a User

Use this page to search for and select a user whose password you want to change.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select an attribute from the list. All searchable attributes and the personal profile are included in this list. If you select an attribute, the search is based on that attribute. If you select **Entire profile**, the search is based on all attributes associated with the user.

Last Name searches for the user's last name.

Full Name searches for the user's full name.

E-mail Address searches for the user's e-mail address.

Entire Profile searches all attributes associated with the user.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Advanced

Click to search using additional filter criteria.

Users table

Lists the users matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a user. To select one or more users, select the check box adjacent to the user. To select all users, select the check box at the top of the column.

Name

Identifies a value for distinguishing a user, such as the user's full name. Click the name of the user to view the user's personal profile.

E-mail Address

Identifies the user's e-mail address.

Last Name

Identifies the user's last name.

Business Unit

Identifies the business unit. Click to view details about the organization.

Status

Identifies the user's status.

Users are either active or inactive. A user must be active to log in to the system. Users become inactive when they are suspended. The suspended users still exist, but they cannot access the system. System administrators can restore inactive users.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Select a Service

Use this page to find the service that you want.

Search information

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Search by

Select the search category.

Service searches for service names that contain the text that is entered in the **Search information** field.

Business unit searches for business units in which the business unit name contains the text that is entered in the **Search information** field.

Service type

Select a service type from the list.

Search

Click to display a list of items whose information matches the search criteria. If the search results exceed the search limit, a warning message is displayed, and the defined number of results are listed.

Services table

Lists the services that match the search criteria that you specified. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a service. To select one or more services, select the check box next to the service. To select all services, select the check box at the top of the column.

Service Name

Identifies the name of the service. Click the name of the service to view the service details.

Description

Identifies a brief description of the service.

Service Type

Identifies the type of service.

Business Unit

Identifies the business unit associated with the service.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).

Password

Use this page to specify a password for the account that you are working with.

Generate a password for me

Select this radio button to have the system generate a password for the account.

Allow me to type a password

Select this radio button to specify a password for the account.

Password

Type a new password for the account in this field. The password is encrypted when it is saved.

Confirm password

Type the new password again.

Password Strength Rules table

Lists the rules that the new password must conform to for this account. If the password does not conform to these password strength rules, an error message is displayed, and you must specify a new password. This table might not be displayed if no password policy has been set.

Password Rule

Displays the password rules.

Setting

Displays the value that is required for the password rule.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Creating passwords during account restore

The account **Restore** feature can use this page to restore multiple accounts at one time. There are two categories of accounts. Each category is handled differently.

Accounts of the first category are listed on the Create a New Password page. The menu selection of **Generate a password for me** or **Allow me to type a password** is applied to them, as described on this page.

Accounts of the second category are listed in an *information message* window that pops up on the page. For these accounts, the system automatically generates a password that is *different* from any password (typed or generated) for accounts in the first category.

For example, some accounts are kept in the credential vault. If the credentials for these accounts are configured to require check out and check in, then these accounts belong to the second category. In this case, the system generates a password that is not displayed during the **Restore** process. Instead, you must check out the credentials from the vault, in order to view the generated password.

Schedule request

Schedule request

Select one of these schedule intervals for this request:

Immediate

Runs the request immediately after you click the button to complete the task.

Effective date

Runs the request at a day and hour that you specify. After you select this option, click the calendar icon to specify the scheduled day, and click the clock icon to specify the scheduled hour.

Click **Submit** to perform or schedule the request.

Related information

For more information, see the [IBM Knowledge Center](#).

Change an Expired Password

Use this page to change an expired password.

When your IBM Security Identity Manager password expires, you can no longer use it to log in to your account. If you try to log in with an expired password, you are prompted to change your password.

New password

Type a new password for the account in this field. The password is encrypted when it is saved. Asterisks (*) are displayed as you type.

Confirm password

Type the new password again. Asterisks (*) are displayed.

Click **OK** to change the password.

Related information

For more information, see the [IBM Knowledge Center](#).

Select Group

Use this page to search for a group.

Group name or description

Type information about the search. If you do not type a value in this field, or if you type an asterisk (*) and click **Search**, the entire list of search results is displayed if the number of results does not exceed the search limit.

Groups table

Lists the groups matching the specified search criteria. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies a group. To select one or more groups, select the check box next to the group. To select all groups, select the check box at the top of the column.

Group Name

Displays the name of the group.

View

Identifies the view of tasks that users have in this group.

Description

Displays information about the intended purpose of the group.

Business Unit

Identifies the business unit in which the group is specified.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Related information

For more information, see the [IBM Knowledge Center](#).


Home

Use this page to directly access the tasks that you can perform.

The **Home** page is displayed after you log in to the system. It includes status information and links to tasks that you can perform.

After you have clicked on a task link, you can exit the task and navigate back to the **Home** page by closing the task or selecting the **Home** link that displays in the upper left corner of the task page.

Service Connection Status table

Lists the current status of services you own. The table is displayed only when the login user is a service owner. Click the  icon to toggle the table open or closed. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Status

Displays the current status of the service.



Indicates that the connection to the service was successful.



Indicates the status of the connection is unknown.



Indicates that the connection to the service failed.

Refresh

Click this button to obtain the updated status of the services. However, perform a **Test Connection** before refreshing the service status.

Service Name

Identifies the name of the service. Click the service name to view and make changes to the service.


Service Description

Provides a description of the service.

Last Status Date

Identifies the last time that IBM Security Identity Manager attempted to contact the service and query the connection status.

Common Tasks

Provides a list of common administrative tasks you can perform. Click the  icon to toggle the task list open or closed.

To perform a task, click the task link within the task panel.

Related information

For more information, see the [IBM Knowledge Center](#).

Business Unit Details

Use this page to view business unit details for an organization. The business unit fields available on this page vary according to the business unit type. All text fields are read-only.

Context within the organization

Provides a root structure below a Root Organization showing the organization structure, including organizations, organizational units, business partner organizational units, locations, and admin domains.

Related information

For more information, see the [IBM Knowledge Center](#).

Account Information

Use this page to review the details related to the selected account. All fields are read-only.

The fields that are displayed on this page vary based on the type of service that you selected and by the authority the system administrator has granted you.

User ID

The user ID associated with the account. This field is common for all accounts.

If additional tabs are available, click the tabs to continue reviewing information.

Related information

For more information, see the [IBM Knowledge Center](#).

Logon

Login

Use this page to log in to the system. You must provide a valid user ID and password.

User ID

Type your user ID for the IBM Security Identity Manager account that you want to access.

Password

Type the case-sensitive password that is associated with the user ID. Each letter that you type is replaced by an asterisk (*).

Click **Forgot your password?** if you cannot remember your password and need to reset your password. If forgotten password authentication is turned off, this option is not available.

Note: An error message is displayed when you click this link if:

- The user ID is not in the system.
- The forgotten password questions have not yet been answered.
- The administrator has changed the forgotten password questions since you last logged in to the system.

Contact your help desk or system administrator for help with logging in.

Click **Log In** to log in to the system.

If you are logged out of the system because of inactivity or because the server was reset, you are prompted to log in to the system again.

Do not start two browser sessions from the same client computer. The two sessions are regarded as one session, which can affect data integrity.

Related information

For more information, see the [IBM Knowledge Center](#).

Forgot Your Password

Use this page to submit a request to reset your password, when you do not remember it.

Answer the forgotten password questions correctly to reset your password. The answers must match those specified when you configured your forgotten password information.

After answering the questions, click **OK**. If you answered the questions correctly, your password is either automatically reset or an additional page allows you to set the password, depending on the system configuration. A success message is displayed. If you are unable to remember your password or the exact answers to the questions, contact your help desk or system administrator to have your password reset.

Related information

For more information, see the [IBM Knowledge Center](#).

Change Forgotten Password Information

Use this page to specify information so that you can later reset your password by clicking **Forgot your password?** on the **Login** page.

The kinds of questions and the number of required fields are determined by your system administrator. Some configurations require that you provide your own set of questions and answers, or answer only a limited number of questions. Required fields are marked with an asterisk (*).

If you have already saved an answer and need to change your answer, you click **Clear** to clear the answer and retype it. The **Clear** button is available only if a previously answered question has not already been cleared.

If you are changing a question or its corresponding answer, click **Edit** to update the question field and clear the contents of the answer field. The **Edit** button is available only when the previously specified question and answer fields have not already been edited.

Click **OK** to save the information. You must answer all required fields before clicking **OK**.

Related information

For more information, see the [IBM Knowledge Center](#).

Your Password Expired


Use this page to reset an expired password.

When your IBM Security Identity Manager password expires, you can no longer use it to log in to your account. If you try to log in with an expired password, you are prompted to change your password.

If password synchronization is enabled, the password change applies to all of your accounts. If password synchronization is disabled, the password change applies only to your IBM Security Identity Manager account.

Current IBM Security Identity Manager password

Supply the current password for your IBM Security Identity Manager account in this field.

Click the  icon next to **Review the criteria for my new password** to display a list of password strength rules that must be applied for this account. The new password must conform to the password strength rules for the account, or the password is not changed. The password strength rules vary for an account, depending on your organization guidelines. If the table that displays the password strength rules is empty, no rules have been defined.

New password

Type a new password for the account in this field. The password is encrypted when it is saved. Only asterisks (*) are displayed as you type.

New password (confirm)

Type the new password again. Only asterisks (*) are displayed.

Click **OK** to change the passwords of the selected accounts. Your password must conform to the password strength rules, or an error message occurs.

Related information

For more information, see the [IBM Knowledge Center](#).

Specify Forgotten Password Information

Use this page to enter forgotten password information for your account.

The number of challenge question and answer pairs that are displayed on this page vary based on the number of questions the administrator has defined for users.

Question

This option is available only if user-defined challenge response has been enabled. Type the question that you want to ask, such as **What is the name of the town in which I was born?**

Answer

Type the answer to the question.

If multiple fields are available, continue entering question and answer information.

Related information

For more information, see the [IBM Knowledge Center](#).

Specify New Password

Use this page to change your password for one or more accounts. Each account is represented by the account type that hosts the account and the user ID for the account.

For sponsored accounts, the password change applies only to the current account.

For individual accounts:

If password synchronization is enabled

The password change applies to all your individual accounts. Click the ▶ icon next to **View my accounts that will be affected by this password change** to view the list of individual accounts up to the maximum search limit number. The password change applies to any individual accounts not listed because of the search limitation.

If password synchronization is not enabled

The password change applies only to the current account.

Accounts table

Lists the accounts, including your IBM Security Identity Manager login account. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

User ID

Displays the user ID of the account.

Account Type

Identifies the managed resource.

Description

Provides additional information about the account type.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

Click the ▶ icon next to **Review the criteria for my new password** to display a list of password strength rules that must be applied for this account. The new password must conform to the password strength rules for the account, or the password is not changed. The password strength rules vary for an account, depending on your organization guidelines. If the table that displays the password strength rules is empty, no rules have been defined.

New password

Type a new password for the selected accounts in this field. Asterisks (*) are displayed as you type.

New password (confirm)

Type the new password again. Asterisks (*) are displayed.

Click **OK** to change the passwords of the selected accounts.

Change Forgotten Passwords

Use this page to change the password for one or more accounts that belong to another user. You can change the password only when password editing is enabled.

Generate a password for me

Select this option to allow the system to generate a new password for you.

Allow me to type a password


Select this option to specify a password for the account.

Password

Type a new password for the account in this field. Asterisks (*) are displayed as you type. To edit this field, select the **Allow me to type a password** option.

Confirm password

Type the new password again. Asterisks (*) are displayed as you type. To edit this field, select the **Allow me to type a password** option.

Click the  icon next to **View password strength rules** to display a list of password strength rules that must be applied for this account. The new password must conform to the password strength rules for the account, or the password is not changed. The password strength rules vary for an account, based on your organization guidelines.

Password Rule table

Lists the rules that the password policy has defined.

Password Rule

Identifies the password rule.

Setting

Identifies the value for password rule.

If no password policy has been set, the **Password Rule** table might not be displayed.

Accounts table

Lists the accounts, including your IBM Security Identity Manager login account. Each account is represented by the service that hosts the account and the user ID for the account. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select

Specifies an account.

If password synchronization is not enabled, the check box next to the account is preselected. The password change applies only to that current account. If you cannot change the password for an account, the check box is disabled.

If password synchronization is enabled and you are changing the password for an individual account, a list of individual accounts is displayed. This list displays the number of accounts up to the maximum search limit. These accounts are not selectable. The password change applies to all individual accounts. The individual accounts not listed are also changed. If you are changing the password for a sponsored account, the password change applies only to the current account. The Select column is not displayed when password synchronization is enabled.

Service Name

Identifies the name of the service that hosts the account. Click the name of the service to view information about the service.

User ID

Identifies the user ID for the account. Click the user ID to view the details about the account.

Ownership Type

Identifies the ownership type for an account. This column is displayed when password synchronization is disabled.

Click **Submit** to submit your request. If password synchronization is not enabled, you must select an account before clicking **Submit**.

Related information

For more information, see the [IBM Knowledge Center](#).

Password

Use this page to provide a shared secret to retrieve password information for the account that you are working with.

Shared secret

Type the shared secret for the account in the field. The shared secret value is defined in personal information of the account.

Related information

For more information, see the [IBM Knowledge Center](#).

Password

Use this page to retrieve your password for the account that you are working with.

Service name

Provides the name of the service from which you are retrieving your password.

Service description

Provides information about the service.

User ID

Provides the user ID for the account.

Password

Provides the password for the account.

Click **Done** when you have finished retrieving your password.

Related information

For more information, see the [IBM Knowledge Center](#).

About

Use this page to view information about the system.

Server name

Displays the server name. In a cluster configuration, this is the server name for the user's current session.

Version

Displays the version of IBM Security Identity Manager software that you are using.

Build number

Displays the current build number for the version of IBM Security Identity Manager that you are using.

Maintenance level

Displays the last fixpack level that was installed for the version of IBM Security Identity Manager that you are using.

Build date

Displays the date on which the last build occurred.

Build time

Displays the exact time and the time zone in which the last build occurred.

Related information

For more information, see the [IBM Knowledge Center](#).

Message

Use this page to view a message about an action you attempted. Click the message ID for additional information.

Related Tasks

Identifies other related tasks you can perform upon receiving this message.

Related information

For more information, see the [IBM Knowledge Center](#).

Page help does not display

In some browsers, the page helps for the IBM Security Identity Manager administration console might generate a Java 404 error.

The page help file is loaded after the console page load is completed. This loading might take a second or more depending on your computer. If you open the page help before it is loaded, the 404 error is generated. If you click the help icon again after the file is loaded, the help file opens.

Chapter 3. User administration

You can manage people and their user accounts and access in IBM Security Identity Manager.

A *person* is an individual in the system that has a person record in one or more corporate directories. Because information about a person can exist in the system without a user account, the term *user* is often used to describe a person that has profile information in Security Identity Manager.

A user who has an Security Identity Manager service account is called a Security Identity Manager user. Some people might not require an Security Identity Manager service account. For example, external customers or business partners who require access to a specific managed resource might not require an Security Identity Manager account. However, they might be populated into the system as persons.

Use the **Manage Users** page for the following tasks:

- Create and delete profiles that define a person in the system
- Change a user's personal profile
- Suspend or restore a person
- Transfer a person to another business unit
- Request an access or account for a person
- Change or delete an access/account for a person
- Change or reset user account passwords
- Delegate activities to a Security Identity Manager user
- Recertify a user (Only system administrators can perform this task.)

User management

A *user* is an individual who uses IBM Security Identity Manager to manage their accounts. A person who has an Security Identity Manager account is a resource user. Users need different degrees of access to resources for their work. Some users must use a specific application, while other users must administer the system that links users to the resources that their work requires.

Person profiles

A *profile* is a set of attributes that describe a person within the system, such as the user name and contact information.

The specific information contained in the profile is defined by the system administrator.

Attributes

An *attribute* is a characteristic that describes an entity, such as a user, an account, or an account type.

For example, a user is an entity. Some of the attributes that make up a user entity are full name, home address, aliases, and telephone number. These attributes are presented in the user personal profile. Attribute values can be modified, added, and deleted.

An attribute can be specified in an attribute field, as a filter, during a search for an account or user. Several attributes for accounts and account types can be customized by your system administrator.

Aliases

An *alias* is an identity name for a user. A user can have multiple aliases to map to the various user IDs that the user has for accounts.

A user can have several aliases; for example, GSmith, GWSmith, and SmithG.

Roles

Organizational roles are a method of providing users with entitlements to managed resources. These roles determine which resources are provisioned for a user or set of users who share similar responsibilities.

If users are assigned to an organizational role, the managed resources available to that role then become available to those users. Those resources must be properly assigned to that role.

A role might be a child role of another organizational role, which then becomes a parent role. The child role inherits the permissions of the parent role. In addition, a role might be a child role of another organizational role in a provisioning policy. The child role also inherits the permissions of provisioning policy.

Security Identity Manager groups

A *group* is a collection of Security Identity Manager users. Security Identity Manager users can belong to one or more groups. Groups are used to control user access to functions and data in Security Identity Manager.

Some users might belong to default groups that Security Identity Manager provides. Your site might also create additional, customized groups. Each group references a user category, which has a related set of default permissions and operations, and views that the user can access.

Groups grant specific access to certain applications or other functions. For example, one group might have members that work directly with data in an accounting application. Another group might have members that provide help desk assistance.

Creating user profiles

You can create an IBM Security Identity Manager user profile for an individual who requires one.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

If a new user requires a new business unit, create the business unit first. A business unit might be necessary.

Procedure

To create an Security Identity Manager user, complete these steps:

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, click **Create**.
3. On the **Select User Type** page, select the user type. To place the user under a different business unit than the default, click **Search** to search for and select a business unit. Then, click **Continue**.
4. On the **Create User** page, click each tab and specify the required information for the user. The number of tabs that are displayed and the information in each tab is determined by your system administrator.
 - a) On the **Personal Information** tab, type information about the user in the fields. To assign a role for this user, click **Search** to search and select an organizational role. Then, click **Business Information**.
 - b) On the **Business Information** tab, type information about the user in the fields. Then, click **Contact Information**.
 - c) On the **Contact Information** tab, type information about the user in the fields. Then, click **Assignment Attributes**.
 - d) On the **Assignment Attributes** tab, specify values for the role assignment attributes for the user that you are creating.

You can specify values for attributes only if you assigned a role to this user, and the role or its parent role contains assignment attributes.

Note: You cannot specify values in the following cases:

- You did not assign a role.
- You assigned a role, but either the role or its parent role does not have assignment attributes.

e) Click **Continue**.

5. On the **Create a New Password** page, provide a password for the user.

6. Choose a time and date to schedule this operation.

You can select **Immediate**, or you can specify an effective date and time.

7. Click **Submit**.

The user is provisioned an Security Identity Manager account with the password that you provide.

8. On the **Success** page, click **Close**.

9. On the **Select a User** page, click **Refresh**.

The new user is displayed in the **Users** table.

What to do next

You can now do other activities for the new user, such as requesting accounts and access.

[“Defining assignment attributes when creating a role” on page 677](#)

When creating a role, you can optionally define assignment attributes to be associated with the role.

[“Defining assignment attributes for an existing role” on page 678](#)

When modifying an existing role, you can optionally define assignment attributes to be associated with the role.

[“Setting assignment attribute values to the user members of a role” on page 679](#)

You can set assignment attribute values to the user members of a static organizational role if you defined assignment attributes in the role definition.

Changing user profiles


You can change information that is associated with a IBM Security Identity Manager user by updating the user profile.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

To change a user profile, complete these steps:

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, click the icon () next to the name of the user whose personal profile you want to change, and click **Change**.
3. On the **Change User** page, click each tab and specify the required information for the user. The tabs that are displayed and the information in each tab is determined by your system administrator.
 - a) On the **Personal Information** tab, type information about the user in the fields. To assign a role for this user, click **Search** to search for and select an organizational role. Then, click **Business Information**.

- b) On the **Business Information** tab, type information about the user in the fields. Then, click **Contact Information**.
- c) On the **Contact Information** tab, type information about the user in the fields. Then, click **Assignment Attributes**.
- d) On the **Assignment Attributes** tab, specify values for the role assignment attributes for the user that you are creating.
You can specify values for attributes only if you assigned a role to this user, and the role or its parent role contains assignment attributes.

Note: You cannot specify values in the following cases:

- You did not assign a role.
- You assigned a role, but either the role or its parent role does not have assignment attributes.

e) Click **Continue**.

4. When your changes are done, click **Submit Now** to save the changes, or click **Schedule Submission** to select a date and time to schedule the change.
5. On the **Success** page, click **Close**.
6. On the **Select a User** page, click **Close**.

[“Defining assignment attributes when creating a role” on page 677](#)

When creating a role, you can optionally define assignment attributes to be associated with the role.

[“Defining assignment attributes for an existing role” on page 678](#)

When modifying an existing role, you can optionally define assignment attributes to be associated with the role.

[“Setting assignment attribute values to the user members of a role” on page 679](#)

You can set assignment attribute values to the user members of a static organizational role if you defined assignment attributes in the role definition.

Deleting user profiles

You can delete an IBM Security Identity Manager user profile. This action affects all the accounts that are associated with the user.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

When you delete a user, all the accounts that are associated with the user become orphan accounts. You can optionally choose to delete the individual accounts that are associated with the user.

To delete a user:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, select the check mark next to the name of the user you want to delete. You can select one or more users to delete.

- c) You might want to delete all of the individual accounts that are associated with the user that you select. Select the **Include individual accounts when suspending, restoring, or deleting users** check box.

Note: Only the individual accounts that are associated with the user are deleted. Sponsored accounts associated with the user are orphaned. For the ITIM Service, both individual accounts and sponsored accounts associated with this user are deleted.

- d) Click **Delete**.
3. On the **Confirm** page, review the users and their accounts to be deleted. Optionally, select a date and time to do the request.
4. Click **Delete** to submit your request.
5. On the **Success** page, click **Close**.
6. On the **Select a User** page, click **Close**.

What to do next

Assign owners to orphaned accounts. See [“Assigning an account to a user” on page 728](#). If an account is no longer needed, delete the account. See [“Deleting accounts from a service” on page 725](#).

Transferring users

When a user moves to a different business unit within the company, you can transfer the user to another business unit.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, select the check mark next to the full name of the user you want to transfer. You can select one or more users to transfer.
 - c) Click **Transfer**.
3. On the **Business Unit** page, complete the following steps:
 - a) Type information about the business unit in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Business Units** table, click the radio button next to the business unit to which you want to transfer the user. Click **OK**.
4. On the **Confirm** page, review the users and their accounts. Optionally, select a date and time to do the request, and then click **Transfer** to submit your request.
5. On the **Success** page, click **Close**.
6. On the **Select a User** page, click **Close**.

Suspending users

When a user leaves the company and no longer needs access to IBM Security Identity Manager, you can suspend the system access that the user has.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To suspend a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, select the check mark next to the full name of the user you want to suspend. You can select one or more users to suspend.
 - c) To suspend all of the individual accounts that belong to the user that you selected, select the **Include individual accounts when suspending, restoring, or deleting users** check box.
Note: Sponsored accounts are not affected. You might want to customize the suspend user operation to handle sponsored accounts. For example, have the operation transfer the sponsored accounts to the service owner or the manager of the user who is suspended.
 - d) Click **Suspend**.
3. On the **Confirm** page, review the users and their accounts to be suspended. Optionally select a date and time to do the request, and then click **Suspend** to submit your request.
4. On the **Success** page, click **Close**.
5. On the **Select a User** page, click **Close**.

Restoring users

When a user is suspended, all the associated user accounts become inactive. Restoring an inactive user returns the user accounts to an active state.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) To restore all of the individual accounts that belong to the user that you selected, select the **Include individual accounts when suspending, restoring, or deleting users** check box.
Note: Sponsored accounts associated with the user are not affected. A suspended sponsored account must be restored through the account table.

Note: If the check box is selected, you cannot restore more than one user at a time. If multiple users are selected, **Restore** is disabled.

- c) In the **Users** table, click the icon () next to the name of the user you want to restore.
- d) Click **Restore**.

If a password is required to restore the individual accounts of the user, you are prompted to change the password.

If password synchronization is enabled

- Individual accounts use the existing synchronized password. You are not prompted to change the password for individual accounts.
- If no synchronized password exists, you are prompted to change the password. The passwords for all the individual accounts associated with the user are changed to the new password.

If password synchronization is disabled

You are prompted to change the password. The passwords for all the listed individual accounts are changed to the new password. Individual accounts on services that do not require password change on user restore are not affected by the password change.

3. If you want to schedule your change request for a later date and time, select **Effective Date**.
 - a) Click the calendar and clock icons to select a date and time.
 - b) Click **Submit**.
4. On the **Success** page, click **Close**.
5. Click **Refresh** to verify that the user is returned to active status.

What to do next

View the accounts for the restored user to ensure that the account status is active. Perform additional user administration tasks on the **Select a User** page, or click **Close** to exit the page.

Recertifying users

You can select a recertification policy and run that policy for a specific user. Only user recertification policies that are enabled can be located and run.

Before you begin

Only system administrators can perform this task.

About this task

You might need to run a recertification policy for a specific user for one of the following reasons:

- The recertification status is erroneous or needs to be changed.
- It might be necessary to override the results of one particular recertification policy with another.

To recertify a user, complete these steps:


Procedure

1. From the navigation tree, click **Manage Users**.

The **Manage Users** page is displayed.
2. On the **Manage Users** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.

A list of users that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
- b) In the **Users** table, click the icon () next to the user that you want to recertify, and then click **Recertify**.
- The **Select a Recertification Policy** page is displayed.
3. On the **Select a Recertification Policy** page, complete these steps:
- a) Type information about the policy in the **Search information** field.
 - b) In the **Search by** field, specify whether to search for policy names or descriptions, and then click **Search**.
- A list of policies that match the search criteria is displayed.
- If the table contains multiple pages, you can:
- Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
- c) In the **Recertification Policies** table, select the policy that you want to run, and then click **Run**.
- A confirmation page is displayed.
4. On the **Confirm** page, click **Run**.

Results

A **Success** page is displayed, indicating that you successfully submitted a request to recertify the user.

What to do next

On the **Success** page, click **Close**.

Account management

You can manage accounts for users in IBM Security Identity Manager.

Accounts

An *account* is the set of parameters for a managed resource that defines an identity, user profile, and credentials.

An account defines login information (your user ID and password, for example) and access to the specific resource with which it is associated.

In IBM Security Identity Manager, accounts are created on services, which represent the managed resources such as operating systems (UNIX), applications (Lotus Notes®), or other resources.

Accounts, when owned, are either individual or sponsored. Individual accounts are for use by a single owner and have an ownership type of Individual. Sponsored accounts are assigned to owners who are responsible for the accounts, but might not actually use them to access resources. Sponsored accounts can have various types of non-Individual ownership types. IBM Security Identity Manager supplies three ownership types for sponsored accounts Device, System, and Vendor. You can create additional ownership types for sponsored accounts by using the Configure System utility.

Accounts are either active or inactive. Accounts must be active to log in to the system. An account becomes inactive when it is suspended. For example, a request to recertify your account usage might be declined and the recertification action is *suspend*. Suspended accounts still exist, but they cannot be used to access the system. System administrators can restore and reactivate a suspended account if the account is not deleted.

Account types

An *account type* represents a managed resource, such as an operating system, a database application, or another application that IBM Security Identity Manager manages. For example, an account type might be a Lotus Notes application.

Users access these account types by receiving an account on the managed resource. Contact your system administrator for additional information about the account types that are available in your environment.

Requesting an account for a user

You can request an account for a user.

Before you begin


Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can request an account on a service, you must create that service. You must also define appropriate Service ACIs to enable the non-administrative users to search the services on the **Request an Account** > **Select a Service** page.

About this task

To request an account for a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, click the icon () next to the name of the user who you want to request an account for.
 - c) Click **Request accounts**.
The **Select a Service** page is displayed.
3. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field, select an option in the **Search by** field, select an attribute from the **Service type** list, and then click **Search**.
Note: Service ACIs must be defined to enable the non-administrative users to search the services.
 - b) In the **Services** table, select the service on which you want to request an account.
 - c) Click **Continue**.
The **Select an Ownership Type** page is displayed.
4. Select the ownership type for the account, and then click **Continue**.
The number of ownership types is determined by the provisioning policy entitlements for the service. The default provisioning policy entitles accounts to the Individual ownership type. Any additional ownership types must be added to the provisioning policy for the service.
Note: If only one ownership type is entitled, this page is not displayed. All accounts are created with that ownership type. For example, if the default provisioning policy is used, all accounts are created as individual accounts.
The **User** page is displayed.
5. On the **User** page, complete these steps:

- a) Click each tab and specify the required information for that account. The tabs that are displayed vary based on the type of service that you selected.
For example, for the AIX service, account information, access information, and administration information pages is displayed.
 - b) If password editing is disabled, click **Submit Now** to complete the request, or click **Schedule Submission** to select a date and time to schedule the request.
 - c) If password editing is enabled, click **Continue** to proceed to the **Password** page. Create a password for the account you are requesting. To specify a password for the account, select whether you want to have the system generate the password or to specify the password now. Click **Submit Now** to complete the request, or click **Schedule Submission** to select a date and time to schedule the request. If you specify a password, the password must conform to the password strength rules for the account.
6. On the **Success** page, click **Close**.
 7. On the **Manage Accounts** page, click **Close**.

Viewing accounts for a user

You can view a list of accounts for users in IBM Security Identity Manager.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To view a list of accounts for a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, click the icon () next to the name of the user whose accounts you want to view, and click **Accounts**.
3. On the **Accounts** page, complete these steps:
 - a) Type information about the account in the **Account information** field.
 - b) In the **Search by** field, specify whether the search is to be done against user IDs or owners.
 - c) In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do.
The advanced search option opens a new page where you can specify additional search criteria.
4. On the **Accounts** page, when you are done viewing accounts, click **Close**.

Viewing or changing account details

You can view or change account details for user accounts in IBM Security Identity Manager.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To view or change account details for a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, click the icon () next to the name of the user whose accounts you want to view or change, and click **Accounts**.
3. On the **Accounts** page, complete these steps:
 - a) Type information about the account in the **Account information** field.
 - b) In the **Search by** field, specify whether the search is to be done against user IDs or owners.
 - c) In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do.

The advanced search option opens a new page where you can specify additional search criteria.
4. On the **Accounts** page, click the user ID to view or change account details.
5. On the **Account Information** page, view account details, or if you want to change account details, specify the required information for the user. The tabs that are displayed and the information in each tab is determined by your system administrator. When your changes are done, click **Submit Now** to save the changes, or click **Schedule Submission** to select a date and time to schedule the change.

Note: When you change account information for the administrator account, such as ITIM Manager, there might be limitations on which information you can change. If the administrator account is configured to use an authentication repository other than ITIM service, you cannot force the account to change password at the next login. When the authentication repository is not ITIM Service, IBM Security Identity Manager does not manage the password.
6. On the **Success** page, click **Close**.
7. On the **Accounts** page, when you are done viewing accounts, click **Close**.

Deleting user accounts

You can delete accounts for users in IBM Security Identity Manager.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To delete user accounts, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, click the icon () next to the name of the user whose accounts you want to delete, and click **Accounts**.
3. On the **Accounts** page, complete these steps:

- a) Type information about the account in the **Account information** field.
- b) In the **Search by** field, specify whether the search is to be done against user IDs or owners.
- c) In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do.
The advanced search option opens a new page where you can specify additional search criteria.
4. On the **Accounts** page, select the check mark next to any accounts you want to delete that are associated with a specific user ID and service name. You can select one or more user accounts to delete. Click **Delete**.
5. On the **Confirm** page, verify that you want to delete the listed accounts, optionally select a date and time to do the request, and then click **Delete**.
6. On the **Success** page, click **Close**.
7. On the **Manage Accounts** page, click **Close**.

Suspending user accounts

You can suspend user accounts in IBM Security Identity Manager. When you suspend an account, it becomes inactive.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To suspend user accounts, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, click the icon () next to the name of the user whose account you want to suspend, and click **Accounts**.
3. On the **Accounts** page, complete these steps:
 - a) Type information about the account in the **Account information** field.
 - b) In the **Search by** field, specify whether the search is to be done against user IDs or owners.
 - c) In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do.
The advanced search option opens a new page where you can specify additional search criteria.
4. On the **Accounts** page, select the accounts you want to suspend that are associated with a specific user ID and service name. You can select one or more user accounts to suspend. Click **Suspend**.
5. On the **Suspend Accounts** page, verify that you want to suspend the listed accounts. Optionally, select a date and time to do the request, and then click **Suspend**.
6. On the **Success** page, click **Close**.
7. On the **Manage Accounts** page, click **Close**.

Restoring user accounts

You can restore inactive user accounts that were suspended in IBM Security Identity Manager. When you restore an account, it becomes active again.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To restore a user account, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, click the icon () next to the name of the user whose account you want to restore, and click **Accounts**.
3. On the **Accounts** page, complete these steps:
 - a) Type information about the account in the **Account information** field.
 - b) In the **Search by** field, specify whether the search is to be done against user IDs or owners.
 - c) In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do.

The advanced search option opens a new page where you can specify additional search criteria.
4. On the **Accounts** page, select the check marks next to the accounts that you want to restore. The account is associated with a specific user ID and service name. Click **Restore**.

Note: If a password is required to restore the selected accounts, you are prompted to change the password for those accounts.

If password synchronization is enabled

- Individual accounts use the existing synchronized password. You are not prompted to change the password for individual accounts. If you are restoring sponsored accounts, you are prompted to change the password for those listed accounts. The passwords for all listed sponsored accounts are changed to the new password.
- If no synchronized password exists, you are prompted to change the passwords for all listed accounts regardless of ownership type. The passwords for all the listed accounts are changed to the new password. If you change the password of an individual account, the password change applies to all individual accounts. The passwords for individual accounts not listed are synchronized to the new password.

If password synchronization is disabled

You are prompted to change the password. The passwords for all listed accounts regardless of ownership type are changed to the new password.

5. On the **Restore Accounts** page, verify that you want to restore the listed account. Optionally select a date and time to do the request. Click **Submit**.
6. On the **Success** page, click **Close**.
7. On the **Manage Accounts** page, click **Close**.

What to do next

View the accounts of the user to ensure that the account is active.

Access management

You can manage access to resources for users in IBM Security Identity Manager. *Access* is your ability to use a specific resource, such as a shared folder or an application.

Access

In IBM Security Identity Manager, access can be created to represent access to access types such as shared folders, applications (such as Lotus Notes), email groups, or other managed resources.

An access differs from an account in that an account is a form of access; an account is access to the resource itself.

Access is the permission to use the resource. *Access entitlement* defines the condition that grants access to a user with a set of attribute values of a user's account on the managed resource. In IBM Security Identity Manager, an access is defined on an existing group on the managed service. In this case, the access is granted to a user by creating an account on the service and assigning the user to the group. Access entitlement can also be defined as a set of parameters on a service account that uses a provisioning policy.

When a user requests new access, by default an account is created on that service. If an account exists, the account is modified to fulfill the access entitlement. For example, you can assign the account to the group that grants access to an access type. If one account exists, the account is associated with the access. If multiple accounts exist, you must select the user ID of the account to which you want to associate your access.

An access is often described in terms that can be easily understood by business users.

Requesting access for users

You can request access for a user. Access gives the user the ability to use a specific resource.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.


Before you can request access, you must create an access entitlement for a service.

About this task

Only access associated with entitlements of the ownership type Individual can be granted (request by users). If you request access for a user with a sponsored account, an individual account is automatically created. For example, you request access for a user whose preferred user ID is `jdoe`. The user account is a sponsored account with the ownership type Vendor. A user ID `jdoe1` is created with an individual account for the requested access.

To request access for a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, click the icon () next to the name of the user who you want to request access for.
 - c) Click **Request access** to display the **Select Access** page.
3. On the **Select Access** page, complete these steps:

- a) Type information about the service in the **Access information** field, select an access type from the **Access type** tree, and then click **Search**.
- b) In the **Access** table, select the access that you want to request.
- c) Click **Continue**.
4. On the **Select Accounts** page, select one or more accounts that you are requesting the access for. This page is displayed only if more than one individual account exists.
5. Click **Submit** to complete the request, or click **Schedule Submission** to select a date and time to schedule the request.
6. On the **Success** page, click **Close**.
7. On the **Select Access** page, click **Close**.

Viewing access for users

You can view access for a user.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To view access for a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, click the icon () next to the name of the user for which you want to view access.
 - c) Click **Access**.
3. When you are finished viewing access entitlements, on the **Manage Access** page, click **Close**.

Deleting user access

You can delete access for users in IBM Security Identity Manager.

Before you begin


Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To delete access for a user, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.

- b) In the **Users** table, click the icon () next to the name of the user whose accounts you want to delete, and click **Access**.
3. On the **Access** page, select the check mark next to the access you want to delete that is associated with a specified access name. Click **Delete**.
4. On the **Confirm** page, verify that you want to delete the listed access, optionally select a date and time to do the request, and then click **Delete**.
5. On the **Success** page, click **Close**.
6. On the **Access** page, click **Close**.

Password management

There are two ways to manage passwords in IBM Security Identity Manager.

When password editing is enabled, you can supply user passwords with the **Change Passwords** task. When password editing is disabled, you can reset user passwords with the **Reset Passwords** task.

Changing user passwords

When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

If password editing is disabled, you must use the **Reset Passwords** option to modify passwords because you do not have access to the **Change Passwords** task.


If password synchronization is enabled, the password is changed for all of the individual accounts automatically.

If password synchronization is not enabled, you can choose which accounts you want to change the password for.

Password synchronization applies only to individual accounts. Sponsored accounts are not affected by password synchronization. A user can specify different passwords for sponsored accounts.


To change passwords for other users, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user for whom you are changing passwords in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, click the icon () next to the name of the user whose passwords you want to change, and click **Change Passwords**.
3. On the **Change Passwords** page, complete these steps:
 - a) Select how you want the password to be generated.
If you select to type a new password, type and confirm the password.
 - b) Select the accounts that you want to change the password for.

Note: If password synchronization is enabled and you are changing the password for individual accounts, a list of individual accounts is displayed. This list displays the number of accounts up to

the maximum search limit. These accounts are not selectable. The password change applies to all individual accounts. The individual accounts that are not listed are also changed.

- c) If you want to schedule your change request for a later date and time, click the icon () next to **Schedule**. Select **Effective Date**, and click the calendar and clock icons to select a date and time.
- d) Click **Submit**.

4. On the **Success** page, click **Close**.

[“Resetting user passwords” on page 623](#)

When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

[“Changing user passwords for sponsored accounts” on page 624](#)

When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

[“Resetting user passwords for sponsored accounts” on page 625](#)

When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

Resetting user passwords

When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

If password editing is enabled, you must use the **Change Passwords** option to modify passwords because you do not have access to the **Reset Passwords** task.


If password synchronization is enabled, the password is changed for all of the individual accounts automatically.

If password synchronization is not enabled, you can choose which accounts you want to change the password for.

Password synchronization applies only to individual accounts. Sponsored accounts are not affected by password synchronization. A user can specify different passwords for sponsored accounts.


To reset passwords for other users, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user for whom you are resetting passwords in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, click the icon () next to the name of the user whose passwords you want to reset, and click **Change Passwords**.
3. On the **Reset Passwords** page, complete these steps:
 - a) Select the accounts that you want to reset the password for.

Note: If password synchronization is enabled and you are resetting the password for individual accounts, a list of individual accounts is displayed. This list displays the number of accounts up to

the maximum search limit. These accounts are not selectable. The password reset applies to all individual accounts. The individual accounts not listed are also changed.

- b) If you want to schedule your change request for a later date and time, click the icon () next to **Schedule**. Select **Effective Date**, and click the calendar and clock icons to select a date and time.
- c) Click **Submit**.

4. On the **Success** page, click **Close**.

[“Changing user passwords” on page 622](#)

When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

[“Changing user passwords for sponsored accounts” on page 624](#)

When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

[“Resetting user passwords for sponsored accounts” on page 625](#)

When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

Changing user passwords for sponsored accounts

When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.



About this task

If password editing is disabled, you must use the **Reset Passwords** option to modify passwords because you do not have access to the **Change Passwords** task.


Password synchronization applies only to individual accounts. Sponsored accounts are not affected by password synchronization. A user can specify different passwords for sponsored accounts.

To change passwords for other users, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user for whom you are changing passwords in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, click () next to the name of the user whose passwords you want to change, and click **Accounts**.
 - c) On the **Accounts** page, type information about the account that you are changing password for in the **Search information** field. Select an attribute from the **Search by** list, and select an ownership type. Click **Search**.
 - d) Click () next to the name of the account, and click **Change Password**.
3. On the **Change Passwords** page, complete these steps:
 - a) Select how you want the password to be generated.
If you select to type a new password, type and confirm the password.
 - b) Select the accounts that you want to change the password for.

Note: If password synchronization is enabled and you are changing the password for individual accounts, a list of individual accounts is displayed. This list displays the number of accounts up to the maximum search limit. These accounts are not selectable. The password change applies to all individual accounts. The individual accounts not listed are also changed.

- c) If you want to schedule your change request for a later date and time, click the icon () next to **Schedule**. Select **Effective Date**, and click the calendar and clock icons to select a date and time.
- d) Click **Submit**.

4. On the **Success** page, click **Close**.

[“Resetting user passwords for sponsored accounts” on page 625](#)

When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

[“Changing user passwords” on page 622](#)

When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

[“Resetting user passwords” on page 623](#)

When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

Resetting user passwords for sponsored accounts

When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

Before you begin



Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

If password editing is enabled, you must use the **Change Passwords** option to modify passwords because you do not have access to the **Reset Passwords** task.


Password synchronization applies only to individual accounts. Sponsored accounts are not affected by password synchronization. A user can specify different passwords for sponsored accounts.

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user for whom you are resetting passwords in the **Search information** field. Select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, click () next to the name of the user whose passwords you want to change, and click **Accounts**.
 - c) On the **Accounts** page, type information about the account that you are changing password for in the **Search information** field. Select an attribute from the **Search by** list, and select an ownership type. Click **Search**.
 - d) Click () next to the name of the account, and click **Reset Password**.
3. On the **Reset Passwords** page, complete these steps:
 - a) Select the accounts that you want to reset the password for.

Note: If password synchronization is enabled and you are resetting the password for individual accounts, a list of individual accounts is displayed. This list displays the number of accounts up to

the maximum search limit. These accounts are not selectable. The password reset applies to all individual accounts. The individual accounts that are not listed are also changed.

- b) If you want to schedule your change request for a later date and time, click the icon () next to **Schedule**. Select **Effective Date**, and click the calendar and clock icons to select a date and time.
- c) Click **Submit**.

4. On the **Success** page, click **Close**.

[“Changing user passwords for sponsored accounts” on page 624](#)

When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

[“Changing user passwords” on page 622](#)

When you have the appropriate authority, you can change the password for one or more, or all, of the accounts of other users.

[“Resetting user passwords” on page 623](#)

When you have the appropriate authority, you can reset the password for one or more, or all, of the accounts of other users.

Delegating activities

You can delegate activities for completion.

To delegate activities from one user to another user, the user you are delegating to must have authorization from the system administrator to manage activities. If you are delegating activities for yourself, you must have both read and write Delegate access control item attribute permissions set to Grant. The logged-in user must have the access control item permission to write the deLegate attribute of the user who is delegated.

You can add or delete delegation schedules for the user whose activities you are delegating. Adding a delegation schedule requires you to select a user who can manage activities and specify a time period in which to delegate activities. You can set up multiple delegation schedules for multiple delegates, but time periods cannot overlap. If you already delegated activities and want to turn off delegation, delete the delegation schedule.

Delegation does not affect the escalation period for an activity. That is, it does not restart the escalation period.

Delegating activities for another user

When a user is unavailable to manage activities, you can create a delegation schedule to delegate the to-do items of that user to another user.

Before you begin


Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To delegate activities, complete these steps:

Procedure

1. From the navigation tree, select **Manage Users**.
2. On the **Select a User** page, complete these steps:
 - a) Type information about the user for whom you are delegating activities in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.

- b) In the **Users** table, click the icon () next to the name of the user whose accounts you want to delegate, and click **Delegate Activities**.
3. On the **Manage Delegation Schedules** page, click **Add** to create a delegation schedule.
4. On the **Setup Delegation** page, click **Search** to find a delegate.
5. On the **Select Delegate Account** page, complete these steps:
 - a) Type information about the delegate in the **User ID** field and click **Search**.
 - b) In the **Accounts** table, select the user whose account you want to delegate your activities to, and click **OK**.
6. On the **Setup Delegation** page, click the calendar and clock icons to choose a date and time for starting and ending the delegation, and click **OK**.
7. On the **Success** page, click **Close**.

Chapter 4. Login administration

You can configure system login settings to control the interval at which the password of an account expires. You can configure the number of times that a user can attempt to log in before the account is suspended.

Enabling password expiration

You can configure password settings to force users to regularly change their IBM Security Identity Manager passwords within a specified time period.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Note: If you configured IBM Security Identity Manager to use the default custom registry, you can enable password expiration. If you configured IBM Security Identity Manager to use an external user registry for authentication, you cannot enable password expiration.

Users who are forced to change their password because of an expired password period are taken to the **Expired Password** page immediately after login. The user cannot access any features in the system until the password is changed.

About this task

To enable password expiration, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Set Security Properties**.
2. In the **Identity account password expiration period in days** field, type a time period, and then click **OK**. The default value of 0 indicates that the account password never expires.
3. On the **Success** page, click **Close**.

Setting a maximum number of login attempts

You can set a limit on the number of unsuccessful login attempts that a user can make. You can also suspend accounts that exceed a specified maximum number of login attempts. After the user account is suspended, the user must contact you (the system administrator) or a help desk representative. You can then restore the account and generate or provide a new temporary password for the user.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

This task is available only for administrators and cannot be customized.

About this task

This task applies only if the ITIM Service user registry is used. If another user registry is specified, the number of login attempts is managed by the external repository.

The login attempts setting also applies to incorrect challenge response answers.

To set a maximum number of login attempts, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Set Security Properties**.
2. In the **Maximum number of incorrect login attempts**, type the number of login attempts you want to allow, and then click **OK**. The default value of 0 indicates that there is no limit to the number of entries that can be attempted.
3. On the **Success** page, click **Close**.

Chapter 5. Password administration

IBM Security Identity Manager controls how passwords can be changed, generated, synchronized, and set throughout the system.

Tasks for managing system-wide password settings include:

- Enabling password resetting, including:
 - Hiding generated passwords from the administrators who generate them
 - Showing generated passwords to the administrators who generate them
- Enabling editing and changing passwords
- Synchronizing password changes for all of the individual accounts that are associated with a user
- Setting passwords when the user is created
- Setting an interval in which a user must retrieve a password before it expires
- Creating a password strength rule
- Enabling forgotten password authentication
- Excluding specific passwords

Password expiration settings are part of the login account settings.

Depending on the adapters that are used in your site environment, you might optionally set reverse password synchronization. The synchronization originates from a master password store other than IBM Security Identity Manager.

A help desk assistant can also request IBM Security Identity Manager to generate a password. The password is sent in an email to the user.

For information about managing user passwords, including the passwords of system users, see [“User management”](#) on page 607.

Enabling password resetting

Users or administrators with the correct permissions can *reset* users' passwords to new passwords that are generated by IBM Security Identity Manager. Alternatively, depending on the password settings of Security Identity Manager, users or administrators might be able to *change* users' passwords to new passwords. The new passwords must be manually specified within the limits of the password policy.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To reset another user's passwords, you must have the correct access control item permissions.

You must configure your system to use either the **Reset Passwords** function or the **Change Passwords** function. The options are not available at the same time.

If you choose to enable the **Reset Passwords** function, you also have the option of showing or hiding the generated password.

To enable password resetting:

Procedure

1. From the navigation tree, select **Set System Security > Set Security Properties**.
2. Clear the **Enable password editing** check box, and click **OK**.
3. On the **Success** page, click **Close**.

Hiding generated reset passwords

You might want to prevent every user or administrator who can reset passwords from seeing the new password that is generated. You can disable password editing and hide generated passwords.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

If you do not hide generated passwords, the users or administrators who are resetting a user's password see the password that was generated.

To enable **Reset Passwords** and hide the generated password from the user or administrator who requested that the password be reset, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Set Security Properties**.
2. Select the **Hide generated passwords for others** check box, and click **OK**.

Note: If the **Enable password editing** check box is selected, you cannot select the **Hide generated passwords for others** check box. Clear the **Enable password editing** check box if you want to hide generated passwords.

3. On the **Success** page, click **Close**.

Results

A group member who can create accounts, such as a member of the help desk assistant group, can reset a password. However, the group member cannot see the new password. IBM Security Identity Manager generates the password.

Showing generated reset passwords

You might want to enable every user or administrator who can reset passwords to see the new password that is generated. You can disable password editing and clear the hide generated passwords check box.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

If you do not hide generated passwords, the users or administrators who are resetting a user's password see the password that was generated.

To enable the **Reset Passwords** and show the generated password to the user or administrator who requested that the password be reset, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Set Security Properties**.
2. Ensure that the following conditions are true:
 - The **Enable password editing** check box is not selected.
 - The **Hide generated passwords for others** check box is not selected.
3. Click **OK**.
4. On the **Success** page, click **Close**.

Results

A group member who can create accounts, such as a member of the help desk assistant group, can reset a password. The group member can also see the new password.

Enabling password editing and changing

Users or administrators with the correct permissions can *reset* users' passwords to new passwords that are generated by IBM Security Identity Manager. Alternatively, depending on the password settings of Security Identity Manager, users or administrators might be able to *change* users' passwords to new passwords. The new passwords are manually specified within the limits of the password policy.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To change another user's passwords, a user or administrator must have the correct access control item permissions. When you enable password editing, the user or administrator with the correct access control permissions can manually specify the password.

You must configure your system to use either the **Reset Passwords** function or the **Change Passwords** function. The options are not available at the same time.

To enable password editing, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Set Security Properties**.
2. Select the **Enable password editing** check box, and click **OK**.
3. On the **Success** page, click **Close**.

Results

Enabling password editing has these results:

- Disables the ability to hide generated passwords for others.
- Enables users with the correct authority to select the **Change Passwords** option in the navigation tree and then change their own passwords.
- Enables a group member who can create accounts to create and set a value for a password for an account of another user. For example, the group member might belong to the help desk assistant group. Because the newly created password is visible, the help desk assistant can provide the information by telephone to the user.

What to do next

Note: You must log out and log back in to see the changes that are made to the navigation tree after you enable password editing.

Enabling password synchronization

Password synchronization is the process of assigning and maintaining one password for all individual accounts that a user owns. Password synchronization reduces the number of passwords that a user must remember. Password synchronization does not affect sponsored accounts.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must be a system administrator on the to enable password synchronization.

About this task

You can configure the system to automatically synchronize passwords for all individual accounts that are owned by a user. Then, the user must remember only one password. For example, a user might have two individual accounts: a IBM Security Identity Manager account and a Lotus Notes account. If the user changes or resets the password for the Security Identity Manager account, the Lotus Notes password is automatically changed to the same password as the Security Identity Manager password.

Note: When password synchronization is enabled, Security Identity Manager does the ACI evaluation for changing password on the person entity. (Before Tivoli Identity Manager version 5.0, the ACI evaluation was done on the account entity.) If the person ACI grants the user the change password operation, the user can change the password for all associated individual accounts. For sponsored accounts or if password synchronization is not enabled, the ACI evaluation is done against the account entity instead.

If password synchronization is enabled, users cannot specify different passwords for their individual accounts. Password synchronization does not affect sponsored accounts. A user can specify different passwords for sponsored accounts.

Note: When password synchronization is initially enabled, individual accounts of users are not automatically synchronized immediately. Accounts are synchronized when users change passwords or create an account.

To enable password synchronization, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Set Security Properties**.
2. Select the **Enable password synchronization** check box, and click **OK**.
3. On the **Success** page, click **Close**.

What to do next

You can change and synchronize the passwords for the individual accounts that are associated with a user.

Setting a password when a user is created

You can enable a password to be generated and set for a user automatically at the time the user is created.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

For the collected password to be set to auto-provisioned accounts, the following criteria must be met:

- An automatic entitlement that entitles the user to the account must exist.
- An account default for `expassword` must exist at the service or service type level.

About this task

This option is intended to enable prompting for a password when creating users through the user interface. By default, IBM Security Identity Manager satisfies these criteria for IBM Security Identity Manager Server login accounts. A user that is created through the user interface is automatically provisioned an Security Identity Manager Server account with a known password. The password is entered at the time of user creation.

The system property for setting the password on a user during the user creation is configured for use during auto-provisioning of Security Identity Manager accounts only. When enabled, the "Set password on user..." system property gathers a password during user creation and stores it in the user record.

Also provided is an account default for the ITIM Service service type that sets `expassword` during auto-provisioning to the value stored in the person record. You can configure another service to use this property by enabling the service for auto-provisioning and adding the necessary account default. Use the following account default script:

```
subject.getAndDecryptPersonPassword();
```

Note: If auto-provisioning is disabled, or if the account default is removed, disable the **Set password on user during user creation** property.

Procedure

To enable a password to be generated and set for a user at the time the user is created, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Set Security Properties**.
2. Select the **Set password on user during user creation** check box, and click **OK**.
3. On the **Success** page, click **Close**.

Setting a password retrieval expiration

You can set a time by which a user must retrieve a password before it expires.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Password retrieval expiration specifies the time in which a user must retrieve a password. After the new account is created, the user receives an email with the URL link that provides the password. The user must get the password before this password retrieval period expires.

This password retrieval expiration property is in effect only when password retrieval is enabled.

Note: The shared secret attribute of Person and the notifyPassword property from enRole.properties file can be used for secured password retrieval.

To set a password retrieval expiration interval, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Set Security Properties**.
2. Specify an expiration period in hours in the **Password retrieval expiration period in hours** field, and click **OK**.
3. On the **Success** page, click **Close**.

Setting password notification

As an administrator you can choose how to send password notifications to users for their accounts.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

After creating an account, changing or resetting a password, you can specify how the password notification is sent to the user.

Procedure

1. Obtain the email address of the owner.
2. Set the value of the **enrole.workflow.notifypassword** property in the enRole.properties file for the notification delivery method.

true

The default is true. Send the recipient an email with the password.

false

Send the recipient a link to a website. The recipient must have an email address and a shared secret specified in the personal profile. On the website, the user is asked for the shared secret. If the value that the user enters for the shared secret is correct, the user is taken to a Web site that shows the new password.

If the user does not specify a shared secret in their personal profile, the user must leave the field on the website blank when it asks for the shared secret.

If the request is for a manual service, the process sends a work order to the service owner. You can modify the manual work order, including the manual email notification activity.

Creating password strength rules

You can create a password policy that defines the rules to which passwords must conform. For example, password strength rules might specify that the minimum number of characters of a password must be five. The rules might specify that the maximum number of characters must be 10.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

By default, the Service owner persona can view this task and create password policies for the services the owner persona owns. Furthermore, users who can view this task and have appropriate ACI permissions can create password strength rules.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Password Policies**.
2. Create a password policy or change an existing one. Ensure that you selected a service on the **Targets** tab to which you apply the password policy.
3. Using the **Rules** tab for the password policy that you select, specify the rules that determine whether a password entry is valid.
See [“Password strength rules” on page 637](#).

Password strength rules

You can set password strength rules that a password policy uses to determine whether a password is valid.

The following table describes each password strength rule.

Attribute	Description
Maximum length	Enter the maximum number of characters that a password can contain. For example: if value of this rule set to 6, then password should have at least 6 characters.
Minimum length	Enter the minimum number of characters that a password can contain. For example: if value of this rule set to 12, then user is allowed to set password up to 12 characters.
Maximum repeated characters	Enter the maximum number of duplicate characters that a password can contain. For example, if value of this rule is 2, then user can not add PPP as part of the password.
Minimum unique characters	Enter the minimum number of unique characters that a password must contain. For example: if value of this rule is 3, then password should have at least 3 unique characters such as abcdcba.
Minimum alphabetic characters	Enter the minimum number of alphabetic characters that a password must contain. For example: if value of this rule is 3, then password should have at least 3 alphabets, such as a1b2c3d.

Table 12. Descriptions of the password attributes (continued)

Attribute	Description
Minimum numeric characters	<p>Enter the minimum number of numeric characters that a password must contain.</p> <p>For example: if value of this rule is 3, then password should have at least 3 numbers, such as a1b2c3d.</p>
Characters not allowed	<p>Enter characters that are not allowed in the password. Do not separate any characters with a space or another delimiter, unless a space or the delimiter is a disallowed character.</p> <p>For example: if you want to specify <code>_ - { } & *</code> as disallowed characters, then a correct value for this field is:</p> <pre data-bbox="618 598 1474 653">_ - { } & *</pre> <p>An incorrect value for this field is:</p> <pre data-bbox="618 724 1474 779">_ - { } & *</pre> <p>or:</p> <pre data-bbox="618 840 1474 894">_, -, , {, }, &, *</pre>
Required characters	<p>Enter character that must be in the password. Do not use a comma or a space or another delimiter.</p> <p>For example: if password value must contain a, b and c characters then a correct value for this field is:</p> <pre data-bbox="618 1071 1474 1125">abc</pre> <p>An incorrect value for this field is:</p> <pre data-bbox="618 1197 1474 1251">a b c</pre> <p>or:</p> <pre data-bbox="618 1312 1474 1367">a, b, c</pre>
Restricted to characters	<p>Enter the set of characters to which the password is restricted. That is, the password must contain only these characters. Do not separate any characters with a space or another delimiter, unless a space or the delimiter is a character that must be specified.</p> <p>For example: If you want to specify all lowercase letters then a correct value for this field is:</p> <pre data-bbox="618 1617 1474 1671">abcdefghijklmnopqrstuvwxyz</pre> <p>An incorrect value for this field is:</p> <pre data-bbox="618 1732 1474 1787">a b c d e f g h i j k l m n o p q r s t u v w x y z</pre> <p>or:</p> <pre data-bbox="618 1848 1474 1902">a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z</pre>

Table 12. Descriptions of the password attributes (continued)

Attribute	Description
Starts with characters	<p>Enter the sequence of characters that the password must start with. Do not separate any characters with a space or another delimiter, unless a space or the delimiter is a character that must be specified.</p> <p>For example, if you want to specify that a password should start with 1234 then a correct value for this field is:</p> <div style="background-color: #e0e0e0; padding: 2px; margin: 5px 0;">1234</div> <p>An incorrect value for this field is:</p> <div style="background-color: #e0e0e0; padding: 2px; margin: 5px 0;">1 2 3 4</div> <p>or:</p> <div style="background-color: #e0e0e0; padding: 2px; margin: 5px 0;">1,2,3,4</div>
Repeated history length	<p>Enter the number of passwords that are retained. This value specifies how many unique passwords must be used before a previous password can be re-used. Passwords that match any password in the history list cannot be reused. The history is updated every time the password is changed.</p> <p>For example, if this value is 7, then the password must be changed 7 times to different passwords before the old password can be reused.</p>
Reversed history length	<p>Enter the numeric value that specifies how many passwords, spelled backwards are kept in history. Passwords that match any password in the history list cannot be reused. The history is updated every time the password is changed.</p> <p>For example, if the value for this rule is 7, then the password must be changed 7 times to different passwords before the old password (spelled backwards) can be reused.</p>
Disallow user name	<p>Select the check box to disallow the use of the user name as a password. The comparison is case sensitive.</p> <p>For example, if username is John, then user is not allowed to set a password containing the word John.</p>
Disallow user name (case-insensitive)	<p>Select the check box to disallow the use of the user name as a password. The comparison is case insensitive.</p> <p>For example, if username is John, then user is not allowed to set a password containing the word John, john, johN, or any variation of John as part of the password.</p>
Disallow user ID	<p>Select the check box to disallow the use of the user ID as a password. The comparison is case sensitive.</p> <p>For example, if user ID is JSmith, then user is not allowed to set password containing word JSmith. Since the comparison is case-sensitive, the user can have Jsmith, jsmith, or other variations as part of the password.</p>

Table 12. Descriptions of the password attributes (continued)

Attribute	Description
Disallow user ID (case-insensitive)	<p>Select the check box to disallow the use of the user ID as a password. The comparison is case insensitive.</p> <p>For example, if user ID is JSmith, then user is not allowed to set password containing the word JSmith, Jsmith, jsmith, or other variations as part of the password.</p>
Do not allow in dictionary	<p>Select the check box to reject the password if its value matches a term in a dictionary that you configure, containing a list of unwanted terms.</p> <p>Note: This option is only available when a dictionary is configured.</p>
Passwords must contain characters from three of the four categories	<p>Select the check box to enable a "three of four categories" rule. This rule is compatible with the same rule in Microsoft Active Directory. The categories are as follows:</p> <ol style="list-style-type: none"> 1. Uppercase letter A through Z 2. Lowercase letter a through z 3. Number 0 through 9 4. Special character (nonalphanumeric): <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p>~!@#\$\$%^&* _ - += ` \ () { } [] ; : " ' < > , . ? /</p> </div> <p>There is no category available for Unicode characters. They are not currently supported.</p>

Enabling forgotten password authentication

When a user forgets the IBM Security Identity Manager password and must reset it, the user must verify credentials with the system.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

An administrator typically defines the forgotten password challenges for a user to attempt a forgotten password recovery.

Note: This task is effective only if a WebSphere account repository is specified. This field is on the ITIM Service **Manage Services > Change a Service > Service Information** page. This repository can be ITIM Service or a service managed by the Security Identity Manager server. If no registry is specified, the forgotten password option is not available on the **Login** page.

Respond to a set of forgotten password challenges with answers that you previously specified. Responses are not case-sensitive by default, because the `enrole.challengeresponse.responseConvertCase` property from the `enRole.properties` file has a default value that is lower. The answers are stored in lowercase in the directory server. An answer that you entered is converted to lowercase while it is compared with the stored answers. If you want answers to be case-sensitive, change the value for `enrole.challengeresponse.responseConvertCase` from `lower` to `none`.

Note: The requirement that a user must answer the challenge questions is configurable. By default, the user can bypass the challenge questions. You can force the user to respond to the challenge questions by modifying the property `ui.challengeResponse.bypassChallengeResponse` in the `ui.properties` file. To

force user response, set the value to `false`. For more information, see the `ui.properties` topic in the **Reference > Supplemental property files** section.

Configuring user-defined forgotten password questions

You can enable and configure forgotten password settings to allow users to supply their own questions for challenge response authentication.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To enable and configure user-defined forgotten password settings, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Configure Forgotten Password Settings**.
2. On the **Configure Forgotten Password Settings** page, complete these steps:
 - a) Select the **Enable forgotten password authentication** check box.
 - b) Under the **Login Behavior** field, select one of the following login options:
 - Click **Enforce password change and log in to system** if you want users to change the password and log in to the system after they successfully answer the challenge response questions. Optionally type in a message the user receives if the user fails to enter the correct answers. Type an email address to which the message is sent.
 - Click **Reset and e-mail password** if you want the system to reset the password and email the password to the user after they successfully answer the challenge response questions. Optionally type in a message the user receives if the user fails to enter the correct answers. Type an email address to which the message is sent.
 - Click **Email user a link to change password** if you want the system to send an email to the user with the link to change the password. A user can click the link in an email that prompts the user to change the password.
 - c) In the **Challenge Behavior** field, click the radio button next to **Users define their own questions**.
 - d) Type in the number of questions the user must set up and answer correctly to successfully authenticate, and click **OK**.
3. On the **Success** page, click **Close**.

Configuring administrator-defined forgotten password questions

You can enable forgotten password settings for challenge response authentication.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

An administrator sets up password challenges for users, which the users must complete before recovering their lost password. When a user answers the administrator-defined challenges successfully, different options are available to receive the new password. To set the right configuration of password recovery, you must complete these steps.

Procedure

1. From the navigation tree, select **Set System Security > Configure Forgotten Password Settings**.
2. On the **Configure Forgotten Password Settings** page, complete these steps:
 - a) Select the **Enable forgotten password authentication** check box.
 - b) Under the **Login Behavior** field, select one of the following login options.
 - Click **Reset and e-mail password** if you want the system to reset the password and email the password to the user after they successfully answer the challenge response questions. Optionally type in a message the user receives if the user fails to enter the correct answers. Type an email address to which the message is sent.
 - Click **Email user a link to change password** if you want the system to send an email to the user with the link to change the password. A user can click the link in an email that prompts the user to change the password. This option is set to default in the Identity Service Center when you access it through the virtual appliance.
 - c) Click **OK** to save your changes.
3. On the **Success** page, click **Close**.

Note:

- The **Email user a link to change password** configuration option is effective only when a user initiates the forgot password flow through the Identity Service Center.
- If a user initiates the forgot password flow through the Self-service user interface, the system prompts the user to change the password and then logs in the user to the system.

Excluding specific passwords

You can configure the system to prevent users from using specific words as passwords for their accounts.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Specified words are stored in a password dictionary in the LDAP Directory Server. This password dictionary contains a list of words that cannot be used as passwords.

This dictionary can be modified through an LDAP browser by creating `erDictionaryItem` entries under the `erDictionaryName=password` entry. Alternatively, you can import an LDIF file with the entries listed into the Directory Server.

The following is an example of an LDIF file with various words to exclude as passwords listed:

```
dn: erword=apple, erdictionaryname=password, ou=itim, dc=com
objectClass: top
objectClass: erdictionaryitem
erWord: apple

dn: erword=orange, erdictionaryname=password, ou=itim, dc=com
objectClass: top
```

```
objectClass: erdictionaryitem
erWord: orange
```

The only value that must be modified is the `erword` value. The `erword` value specifies the word that is *not* allowed to be used as a password.

After the password dictionary is populated with the wanted words, the password policies must be modified to use the dictionary. After importing the LDIF file, select the **Do not allow in dictionary** check box on the **Rules** page of password policies.

Passwords for system users

After you install IBM Security Identity Manager, three system users are defined. These system users enable IBM Security Identity Manager to communicate with the database and the directory server.

By default, the following systems users are defined:

itimuser

This user is the IBM Security Identity Manager system user. The system user is created manually before the IBM Security Identity Manager installation program was run.

db2admin or db2inst1

These users are the DB2 system users that are created by the DB2 installation program. If you installed DB2 on a Windows system, the user name is `db2admin`. If you installed DB2 on a Linux system, the user name is `db2inst1`.

ldapdb2

This user is the LDAP system user.

Initially, the `db2admin` or `db2inst1` user is created by the DB2 installation process with a password that is set to never expire. However, the password for the `ldapdb2` user and `itimuser` users can expire, based on the password policy of your system. If the passwords for these users expire, or are changed, you must reconfigure IBM Security Identity Manager and its associated middleware to use the new password values.

Changing the itimuser user password

You might need to configure IBM Security Identity Manager to use a new password for the `itimuser` user.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must be a system administrator on the IBM Security Identity Manager Server to have access to this task.

About this task

To change the password of the `itimuser` user on the system, complete these steps:

Procedure

1. From the `ISIM_HOME/bin` directory, run the `runConfig` tool.
2. From the **System Configuration** page in the `runConfig` tool, select the **Database** tab.
3. On the **Database** page, in the **User Password** field, type the new password, and then click **OK**.

Changing the db2admin user password for Windows

When you change the system user password for db2admin in Windows, you must also change the password for any service instances that use db2admin as a service account. You must change the password for both the DB2 Universal Database service instance and the DB2Admin service instance.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must be a system administrator on the IBM Security Identity Manager Server to have access to this task.

About this task

To change the password for the db2admin user on the Windows system, complete these steps:

Procedure

1. Click **Start > Settings > Control Panel > Administrative Tools > Services**.
2. From the **Services** page, double-click the DB2 Universal Database instance that IBM Security Identity Manager uses.
3. From the **Properties** page, click the **Log On** tab.
4. On the **Log On** page, in the **Password** field and the **Confirm password** field, type the new password, and then click **OK**.

What to do next

To change the password for the DB2Admin service instance, repeat these steps, selecting the DB2Admin service. For example, select **DB2 - DB2Admin**.

Changing the ldapdb2 user password

You might need to configure IBM Security Identity Manager to use a new password for the ldapdb2 user.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must be a system administrator on the IBM Security Identity Manager Server to have access to this task.

About this task

To change the password for the LDAP database user, complete these steps:

Procedure

1. Navigate to the *drive*:\idsslapd-ldapb2\etc directory.
2. Edit the `ibmslapd.conf` file with a text editor.
3. In the `ibmslapd.conf` file, locate `ibm-slapdDbInstance: ldapdb2`.
4. Change the password for the `ibm-slapdDbUserPW` property. The password currently in the file is encrypted. Replace the old password by typing the new password in clear text, and save the change.

Chapter 6. Organization administration

If you are granted the appropriate authority, you can add, delete, and modify elements in the organization tree. You cannot delete an element that has dependent units in it.

The following elements are in the organization tree:

Organization

Identifies the top of an organizational hierarchy, which might contain subsidiary entities such as organization units, business partner organization units, and locations. The organization is the parent node at the top of the node tree.

Organization Unit

Identifies a subsidiary part of an organization, such as a division or department. An organization unit can be subordinate to any other container, such as organization, organization unit, location, and business partner organization.

Business Partner Organization Unit

Identifies a business partner organization, which is typically a company outside your organization that has an affiliation, such as a supplier, customer, or contractor.

Location

Identifies a container that is different geographically, but contained within an organization entity.

Admin Domain

Identifies a subsidiary part of an organization as a separate entity with its own policies, services, and access control items, including an administrator whose actions and views are restricted to that domain.

Administrator domains

An *administrator domain* (admin domain) identifies a subsidiary part of an organization as a separate entity. The entity has its own policies, services, and access control items. The entity also has an administrator whose actions and views are restricted to that domain.

Domain administrators can do only the administrative tasks on their domains. They cannot do system configuration tasks, which are configuration settings that affect the entire system.

An admin domain is considered a type of organization node. To add, change or delete admin domains, complete the steps for adding, changing, or deleting a node in an organization tree.

You can specify an Security Identity Manager user as the administrator of an admin domain. Enter the Security Identity Manager user in the administrator field. The assignment is confirmed. Then, the Security Identity Manager user is granted the appropriate privileges (access control items, or ACIs) to do administration tasks in that domain.

Any Security Identity Manager user who can add, modify, or delete an admin domain can also specify the administrator for the admin domain. This user is either an Security Identity Manager administrator or an Security Identity Manager user. The user has rights to add, modify, or delete an admin domain through ACIs.

Note: Before Security Identity Manager version 5.0, users were not automatically granted rights as the administrator of an admin domain. Instead, ACIs were required to be added manually. With Security Identity Manager version 5.0 and later, the default ACIs automatically grant the domain administrator the rights for administering the admin domain. The domain administrator is a built-in ACI principal.

Related tasks

[Making a user a domain administrator](#)

As an administrator, you can make a user the administrator for a domain.

[Creating a node in an organization tree](#)

As an administrator, or if you have access control item to organizations, you can create a node in an organization tree.

Changing a node in an organization tree

As an administrator, or if you have access control item to organizations, you can change a node in an organization tree.

Deleting a node in an organization tree

As an administrator, or if you have access control item to organizations, you can delete a node in an organization tree.

Transferring a business unit

As an administrator, you can transfer a business unit in an organization tree.

Making a user a domain administrator

As an administrator, you can make a user the administrator for a domain.

About this task

You can specify an IBM Security Identity Manager user as the administrator of an administrator domain. The IBM Security Identity Manager user is granted the appropriate privileges (access control items, or ACIs) to do administration tasks in that domain.

Procedure

1. From the navigation tree, select **Manage Organization Structure**.
2. Click the icon next to the **Organization** node, and then click **Create Admin Domain**.
The **Admin Domain Details** page is displayed.
3. Type the administrator domain name and, optionally, a description.
4. Click **Search** to locate a user.
5. On the **Select People** page, select the check box for the user or users that you want to make domain administrators for the domain, and click **OK**.
6. Click **OK** on the **Admin Domain Details** page.

Related concepts

Administrator domains

An *administrator domain* (admin domain) identifies a subsidiary part of an organization as a separate entity. The entity has its own policies, services, and access control items. The entity also has an administrator whose actions and views are restricted to that domain.

Related tasks

Creating a node in an organization tree

As an administrator, or if you have access control item to organizations, you can create a node in an organization tree.

Changing a node in an organization tree

As an administrator, or if you have access control item to organizations, you can change a node in an organization tree.

Deleting a node in an organization tree

As an administrator, or if you have access control item to organizations, you can delete a node in an organization tree.

Transferring a business unit

As an administrator, you can transfer a business unit in an organization tree.

Creating a node in an organization tree

As an administrator, or if you have access control item to organizations, you can create a node in an organization tree.

Before you begin

Determine a model that meets organization needs for service management and user management.

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

To create a node in the tree structure, complete these steps:

Procedure

1. From the navigation tree, select **Manage Organization Structure**.
2. Click the icon next to the node, and then click **Create**.
Nodes that you can select depend on the position of the specific type of business unit.
For example, click **Create Location** to create a location business unit.
3. Complete the fields for the node that you create and click **OK**.
4. Click **Close**.

What to do next

Add any additional nodes that your business model requires for service management or user management.

Related concepts

Administrator domains

An *administrator domain* (admin domain) identifies a subsidiary part of an organization as a separate entity. The entity has its own policies, services, and access control items. The entity also has an administrator whose actions and views are restricted to that domain.

Related tasks

Making a user a domain administrator

As an administrator, you can make a user the administrator for a domain.

Changing a node in an organization tree

As an administrator, or if you have access control item to organizations, you can change a node in an organization tree.

Deleting a node in an organization tree

As an administrator, or if you have access control item to organizations, you can delete a node in an organization tree.

Transferring a business unit

As an administrator, you can transfer a business unit in an organization tree.

Changing a node in an organization tree

As an administrator, or if you have access control item to organizations, you can change a node in an organization tree.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Nodes that you can select depend on the position or hyperlink of the node that you select within the structure.

To change a node in an organization tree, complete these steps:

Procedure

1. From the navigation tree, select **Manage Organization Structure**.
2. Click the icon next to the node, and then click **Change**.
3. On the **Details** page for the node, change the necessary fields and then click **OK**.
4. Click **Close**.

Related concepts

[Administrator domains](#)

An *administrator domain* (admin domain) identifies a subsidiary part of an organization as a separate entity. The entity has its own policies, services, and access control items. The entity also has an administrator whose actions and views are restricted to that domain.

Related tasks

[Making a user a domain administrator](#)

As an administrator, you can make a user the administrator for a domain.

[Creating a node in an organization tree](#)

As an administrator, or if you have access control item to organizations, you can create a node in an organization tree.

[Deleting a node in an organization tree](#)

As an administrator, or if you have access control item to organizations, you can delete a node in an organization tree.

[Transferring a business unit](#)

As an administrator, you can transfer a business unit in an organization tree.

Deleting a node in an organization tree

As an administrator, or if you have access control item to organizations, you can delete a node in an organization tree.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Remove or migrate any subordinate object that exists in the organization tree, below a node that you intend to delete.

About this task

You cannot delete a higher-level node that contains dependent objects, such as organizational units or locations, or users.

To delete a node in an organization tree, complete these steps:

Procedure

1. From the navigation tree, select **Manage Organization Structure**.
2. Click the icon next to the node, and then click **Delete**.
Nodes that you can select depend on the position that you select within the structure.
3. On the **Confirmation** page, ensure that the object is your intended target for deletion, and then click **Delete**.
4. Click **Close**.

Related concepts

Administrator domains

An *administrator domain* (admin domain) identifies a subsidiary part of an organization as a separate entity. The entity has its own policies, services, and access control items. The entity also has an administrator whose actions and views are restricted to that domain.

Related tasks

Making a user a domain administrator

As an administrator, you can make a user the administrator for a domain.

Creating a node in an organization tree

As an administrator, or if you have access control item to organizations, you can create a node in an organization tree.

Changing a node in an organization tree

As an administrator, or if you have access control item to organizations, you can change a node in an organization tree.

Transferring a business unit

As an administrator, you can transfer a business unit in an organization tree.

Transferring a business unit

As an administrator, you can transfer a business unit in an organization tree.

Before you begin

You can transfer a business unit to an existing business unit that is under the same organization root. Optionally, you can also create a new business unit and then transfer an existing business unit for people and roles. Following are a few restrictions for business unit transfer activity:

- Business unit cannot be transferred across different organization hierarchy.
- Business unit that contains objects that are related to services and policies cannot be transferred.
- Business unit that contains customized Access Control Item (ACI), cannot be transferred.
- Business unit to be transferred must contain an ACI granted for the Modify operation.
- Business unit cannot be transferred to a child of original business unit to be transferred.
- Business unit that contains a subtree, cannot be transferred.

About this task

IBM Security Identity Manager validates that the selected business unit to transfer contains only people and roles data. Any other objects other than people and roles cannot be transferred. An error message is displayed if any other objects such as services, policies, or its subtree business units are the part of business unit that is selected to transfer. Follow the steps to transfer a business unit for people and roles.

Procedure

1. From the navigation tree, select **Manage Organization Structure**.
2. Click the icon next to the node, and then click **Transfer**.
3. Search and then select the organization container to which you want to transfer the business unit and then click **OK**.
4. On the **Confirmation** page, select the schedule for transfer, and then click **Transfer**.

Related concepts

Administrator domains

An *administrator domain* (admin domain) identifies a subsidiary part of an organization as a separate entity. The entity has its own policies, services, and access control items. The entity also has an administrator whose actions and views are restricted to that domain.

Related tasks

Making a user a domain administrator

As an administrator, you can make a user the administrator for a domain.

Creating a node in an organization tree

As an administrator, or if you have access control item to organizations, you can create a node in an organization tree.

Changing a node in an organization tree

As an administrator, or if you have access control item to organizations, you can change a node in an organization tree.

Deleting a node in an organization tree

As an administrator, or if you have access control item to organizations, you can delete a node in an organization tree.

Business unit transfer activity completion might take a long time

You might encounter slow performance during transfer of business unit activity. To improve performance, you can implement the following solutions.

- Add the following indexes:
 - CREATE INDEX "IDSLDAP2"."TESTIDX1" ON "IDSLDAP2"."SN" ("SN" ASC, "EID" DESC) ALLOW REVERSE SCANS COLLECT SAMPLED DETAILED STATISTICS;
 - CREATE INDEX "IDSLDAP2"."TESTIDX2" ON "IDSLDAP2"."OBJECTCLASS" ("EID" ASC, "OBJECTCLASS" DESC) ALLOW REVERSE SCANS COLLECT SAMPLED DETAILED STATISTICS;
 - CREATE INDEX "IDSLDAP2"."TESTIDX3" ON "IDSLDAP2"."LDAP_DESC" ("DEID" ASC, "AEID" DESC) ALLOW REVERSE SCANS COLLECT SAMPLED DETAILED STATISTICS;
- Update the table statistics by using IBM Security Identity Manager performance tuning scripts.
- Perform the business unit transfer activity during the time of least activity on the application server.

Chapter 7. Security administration

After planning system security for IBM Security Identity Manager, you must take additional steps to implement specific groups, views, and access control items.

View management

IBM Security Identity Manager provides default views of the tasks that are available for each default group.

A *view* is a set of tasks that a particular type of user can do in the user interface. If you give a user or group a view, you do not give permissions to the user or group to do the functions within that task. You must also define access control items to give the user or group the necessary permissions for the task.

Creating a view

As an administrator, you can create a view of tasks that IBM Security Identity Manager provides. For example, you might restrict the set of tasks that group members have.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Determine the subset of tasks that group members might see. Determine whether an access control item might control the tasks that the view makes visible.

- **View All Requests** is only intended for users that have full, unrestricted access to the audit trail. There is no ACI checking in this view. Use caution when exposing this task in a user's view.
- **View All Requests by Service** is intended for service and application owners that need in order to view the audit trail related to services they administer. ACIs are applied only when initially searching for a service. ACIs are not applied to any of the request data shown as a result of selecting a service.
- **View All Requests by User** is intended for the help desk administrators and managers that need in order to view the audit trail related to specific users. ACIs are applied only when initially searching for a user. ACIs are not applied to any of the request data shown as a result of selecting a user.

About this task

You can use the **Define Views** page to create additional views.

To create a view, take these steps:

Procedure

1. From the navigation tree, select **Set System Security > Manage Views > Define Views**.
2. On the **Define Views** page, in the **Views** table, click **Create**.
3. In the **General** tab, type the name and a description of the view. Click **Apply** to save your changes and continue.
4. Select the **Configure View** tab and, in the tree of tasks, select the tasks that the view provides. Click **OK** to save the changes.
5. On the **Success** page, click **Close**.

What to do next

You might create a group that has the view that you created.

Changing a view

As an administrator, you can change a view of tasks that IBM Security Identity Manager provides. For example, you might restrict or expand the set of tasks that group members have.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you begin, determine the subset of tasks that group members see. Determine whether changing an access control item is also needed.

About this task

You can use the **Define Views** notebook to change existing views.

To change a view, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Manage Views > Define Views**.
2. On the **Define Views** page, in the **Name** field, type information about the view and click **Search**.
3. In the **Views** table, select a view and click **Change**.
4. In the General tab, change the name or description of the view. Click **Apply** to save your changes and continue. Click **OK** to save the changes.
5. In the Configure View tab, in the tree of tasks, select the tasks that the view provides. Click **OK** to save the changes.
6. On the **Success** page, click **Close**.

What to do next

You might change any associated access control item for the group that has the view that you changed.

Deleting a view

As an administrator, you can delete a view of tasks that IBM Security Identity Manager provides. For example, you might delete a view after creating an alternative view of tasks that group members can use.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Ensure that group members have access to an alternative view of tasks.

About this task

You can use the **Define Views** page to delete existing views.

To delete a view, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Manage Views > Define Views**.
2. On the **Define Views** page, in the **Name** field, type information about the view and click **Search**.
3. In the **Views** table, select a view and click **Delete**.
4. On the **Confirm** page, ensure that the view is the one you want to delete, and then click **Delete**.

5. On the **Success** page, click **Close**.

Defining a custom task

As an administrator, you might want to create a custom task for your business or organization. You must define these custom tasks before you can assign them to a view.

About this task

A custom task represents an external web application that provides services beyond what is supplied by IBM Security Identity Manager. It is defined by a unique identifier, a URL, and optional parameters. The task can be associated with Security Identity Manager views such as Auditor, or Supervisor, and others. Only users that are associated with those views have access to the custom task. Custom tasks are defined in the administrative console, and are available in the Identity Service Center if the user is authorized to access the task.

You can select the **Start task in new window** check box to enable the user to view the custom task in a new browser window. By default, this check box is not selected. If you create a custom task without selecting this check box, when the user starts the task in the Identity Service Center, it is started in the inline frame, or *iframe*, of the browser window that contains the Identity Service Center. However, if you select the check box, when the user starts the task, it is started in a new browser window or tab, depending on the configuration of the browser.

If you create a custom task that specifies a URL corresponding to the Security Identity Manager administrative console, you must select this check box.

Note:

1. If the web application cannot run custom tasks in a browser *iframe*, that is, inline frame, you must select the **Start task in new window** check box.
2. You can disable headers on some applications for better integration. For example, you might want to create a custom task in the Identity Service Center for the Self Service user interface. To turn off headers so that it integrates better with the Identity Service Center, see [Customizing website layout](#).

Procedure

1. From the navigation tree, select **Set System Security > Manage Views**.
2. On the **Define Views** page, click **Manage Custom Tasks** in the **Views** table.
3. In the **Manage Custom Tasks** table, click **Create**.
4. On the **Create Custom Task** page, type the task identifier suffix for your task.
The suffix cannot contain spaces, quotation marks, hash tags, or equal signs. The combination of the identifier prefix and the identifier suffix is the name that identifies your custom task.

You can define a label for the custom task by editing the `ISIM_HOME/data/CustomLabels.properties` file. The name of the property is `CUSTOM_<Identifier suffix>` (all in capital letters). The value must be what you want to display in the Identity Service Center. For example, if the identifier suffix is `consoleui`, then the property to add to `CustomLabels.properties` can be `CUSTOM_CONSOLEUI = Identity Manager Console UI`.
5. Optional: Type information that describes the custom task in the **Description** field. To enable the translation of the description, add a prefix `$` to the description string and provide a translation for that property in `ISIM_HOME/data/CustomLabels.properties`, where `ISIM_HOME` is the IBM Security Identity Manager installation directory.

If you want to display `Custom task` as the description of the task in the Identity Service Center, you must enter `$customTask` in the **Description** field. You must also add an entry in `CustomLabels.properties`: `customTask = Custom task`.

If you want to translate the description in another language, you must edit the `CustomLabels_xx.properties` file, where `xx` is the locale. For example, `CustomLabels_fr.properties` might have an entry `customTask = Tâche Personnalisée`.
6. Type the URL that links to your custom task.

7. Optional: Type the URL that links to the image you want to display on the task card.

When you specify the URL for the icon, ensure that you review the following guidelines:

- The default icons that are displayed within the "cards" for the Identity Service Center home page are .png files.

None of these icons exceed the following dimensions of 263 x 65 with a 32-bit color depth.

Use this sizing guideline for custom images so that your custom images display correctly in the Identity Service Center.

- The custom image files can be in the following web browser supported image formats, such as jpg, gif, or png.
- Before you begin, upload your custom image files through the virtual appliance dashboard.
 - a. In the dashboard, go to **Configure > Custom File Management**.
 - b. Upload the files to the ui/images directory.
- The URL for **Icon** must be in the following form:
`custom/ui/images/<your file name>`

8. Optional: Specify a menu category for the header.

You can also select from the two predefined menu categories:

`manageAccess`
`requestStatusTodo`

9. Optional: Select the **Show on home page** check box to display the task card on the home page.

10. Optional: Select the **Start task in new window** check box to display the custom task in a new browser window when the user starts the task in the Identity Service Center. If the custom task URL corresponds to the Security Identity Manager administrative console, you must select this check box.

11. Optional: To specify whether the task is visible only to the logged in user, other users, or both, add a task parameter with parameter name as `viewtype`. Specify one of the following values:

self

The task displays when the persona is set to **Manage Self**.

others

The task displays when the persona is set to **Manage Others**.

both

The task displays when the persona is set to either **Manage Others** or **Manage Self**.

12. Optional: Create custom task parameters.

Repeat these steps for each custom parameter you want to create.

- a) In the **Task Parameters** table, click **Create**.
- b) Specify a parameter name.
- c) Specify a parameter value
- d) Click **OK**.

13. When you are finished, click **OK**.

The **Success** page is displayed.

14. Select an action or click **Close** to return to the **Define Views** page.

What to do next

You can now assign the custom task to a view.

Changing a custom task

As an administrator, you can change the task parameters that you specified for a customized task.

About this task

After a task is created, you cannot change the identifier prefix, the identifier suffix, or the console.

Selecting the **Start task in new window** check box enables the user to view the custom task in a new browser window. By default, this check box is not selected. If you change a custom task without selecting this check box, when the user starts the task in the Identity Service Center, it is started in the inline frame, or *iframe*, of the browser window that contains the Identity Service Center. However, if you select the check box, when the user starts the task, it is started in a new browser window or tab, depending on the configuration of the browser.

If you change a custom task that specifies a URL corresponding to the Security Identity Manager administrative console, you must select this check box.

Procedure

1. From the navigation tree, select **Set System Security > Manage Views**.
2. On the **Define Views** page, click **Manage Custom Tasks** in the **Views** table.
3. In the **Manage Custom Tasks** table, select a task and click **Change**.
4. Optional: Under Task information, modify the parameters that you want to change.
5. In the Identifier suffix field, if needed, you can define a label for the custom task by editing the `ISIM_HOME/data/CustomLabels.properties` file. The name of the property is `CUSTOM_<Identifier suffix>` (all in capital letters). The value must be what you want to display in the Identity Service Center. For example, if the identifier suffix is `consoleui`, then the property to add to `CustomLabels.properties` can be `CUSTOM_CONSOLEUI = Identity Manager Console UI`.
6. Optional: In the **Description** field, to enable the translation of the description, add a prefix `$` to the description string and provide a translation for that property in `ISIM_HOME/data/CustomLabels.properties`, where `ISIM_HOME` is the IBM Security Identity Manager installation directory.

If you want to display `Custom task` as the description of the task in the Identity Service Center, you must enter `$customTask` in the **Description** field. You must also add an entry in `CustomLabels.properties`: `customTask = Custom task`.

If you want to translate the description in another language, you must edit the `CustomLabels_xx.properties` file, where `xx` is the locale. For example, `CustomLabels_fr.properties` might have an entry `customTask = Tâche Personnalisée`.

7. Optional: Create or change custom task parameters.
 - a) In the **Task Parameters** table, click **Create** or select a parameter and click **Change**.
 - b) Specify a parameter name.
 - c) Specify a parameter value
 - d) Click **OK**.
8. Optional: Delete custom task parameters.
 - a) In the **Task Parameters** table, select one or more parameters and click **Delete**.
 - b) On the **Confirm** page, ensure that the parameters are the ones you want to delete, and then click **Delete**.

Note: The parameter changes are not saved until you click **OK** to save the updates to the custom task.

9. When you are finished, click **OK**.

The **Success** page is displayed.

10. Select an action or click **Close** to return to the **Define Views** page.

What to do next

Log in to the Identity Service Center user interface and verify that your changes are applied.

Deleting a custom task

As an administrator, you can delete from IBM Security Identity Manager custom tasks that you created. For example, you might delete a custom task you no longer need it or after you create an alternative custom task that group members can use.

Before you begin

If a custom task is used in any view, you cannot delete it. Ensure that the task is removed from all views.

Procedure

1. From the navigation tree, select **Set System Security > Manage Views**.
2. On the **Define Views** page, click **Manage Custom Tasks** in the **Views** table.
3. In the **Manage Custom Tasks** table, select one or more tasks and click **Delete**.
4. On the **Confirm** page, ensure that the custom tasks are the ones that you want to delete, and then click **Delete**.
The **Success** page is displayed.
5. Select an action or click **Close** to return to the **Define Views** page.

What to do next

Navigate back to the **Manage Custom Tasks** table to verify that the task no longer are displayed in the table.

Access control item management

An *access control item (ACI)* is data that identifies the permissions that users have for a specific type of resource. The system administrator has access to all functions in the system and is not governed by access control items.

As system administrator, you create an access control item to specify a set of operations and permissions. Then, you can identify which groups use the access control item.

You can create, change, or delete an access control item. A group might be designated as the owner of the access control item. Members of the group can also do these operations. Members can set up access control items within any branch or subtree branch in which the owned access control item is specified.

Beginning with IBM Security Identity Manager 6.0.0.3, a **Global operation** category is available when you create an access control item. Users that are assigned to this access control item are granted permission to call the custom operation.

Access control items can apply to:

- Entity types such as:
 - All account classes (*erAccountItem*). It controls access to any account.
 - A specific account class (for example, *erPosixLinuxAccount*). It controls access to specific accounts of this class.
 - A user (for example, *erExpressPerson*, which is all users). The access control item controls access to personal profiles.
- Operations that users might perform on entity types or global operations. Custom operations are included with IBM Security Identity Manager 6.0.0.3 and later.
- Permissions for operations on attributes of an entity type, such as an email address.
- A set of users. This set can include access privileges of a *principal*. A principal is a predefined relationship that can be granted privileges. For example, the role of a manager might require access to

the contact information for immediate subordinates. You can assign an access control item that grants such access to all users with a manager relationship.

IBM Security Identity Manager provides default access control items that define permissions to the user and to members in other groups. For example, a default access control item for accounts grants permission to all users to search for and modify a password on their accounts.

Default access control items

The following tables list the default access control items (ACIs) for IBM Security Identity Manager.

Table 13. Default access control items

Protection category	Name	Type	Principal
Account	Default ACI for Account: Grant All to Help Desk Group for Non-Admin Accounts	erAccountItem	Help Desk Group
Account	Default ACI for Account: Grant All to Supervisor/Domain Admin/Sponsor/Service Owner/Access Owner	erAccountItem	Supervisor Domain Admin Sponsor/Service Owner Access Owner
Account	Default ACI for Account: Grant Search, Add, Change Password, and All groupMember Operations to Self	erAccountItem	Self
Account	Default ACI for Account: Grant Search to Auditor Group	erAccountItem	Auditor Group
Account	Default ACI for Account: Grant Connect to Domain Admin and Account Owner	erAccountItem	Domain Admin Account Owner
Account Default Template	Default ACI for Account Defaults: Grant Add/Modify/Search to Service Owner	erAccountTemplate	Service Owner
Admin Domain	Default ACI for AdminDomain: Grant All to Domain Admin	SecurityDomain	Domain Admin
Admin Domain	Default ACI for Admin Domain: Grant Search to Service Owner Group/Auditor/Supervisor/Help Desk	SecurityDomain	Service Owner Group Auditor Group Supervisor Help Desk Group
Business Partner Organization	Default ACI for BP Org: Grant All to Supervisor/Domain Admin/Sponsor	erBPOrg	Supervisor Domain Admin Sponsor
Business Partner Organization	Default ACI for BP Org: Grant Search to Help Desk/Auditor/Service Owner Groups	erBPOrg	Help Desk Group Auditor Group Service Owner Group

Table 13. Default access control items (continued)

Protection category	Name	Type	Principal
Business Partner Person	Default ACI for BPPerson: Grant All to Supervisor/Domain Admin/Sponsor/Help Desk Group	organizationalPerson	Supervisor/Manager Domain Admin Sponsor Help Desk Group
Business Partner Person	Default ACI for BPPerson: Grant Search and Change Password to Self	organizationalPerson	Self
Business Partner Person	Default ACI for BPPerson: Grant Search to Service Owner and Auditor Group	organizationalPerson	Auditor Group
Dynamic Organizational Role	Default ACI for Dynamic Role: Grant All to Supervisor/Domain Admin/Sponsor	Dynamic role	Supervisor Domain Admin Sponsor
Dynamic Organizational Role	Default ACI for Dynamic Role: Grant Search to Auditor Group	Dynamic role	Auditor Group
Dynamic Organizational Role	Default ACI for Dynamic Role: Grant Search to Everyone	Dynamic role	Everyone
Identity Manager User	Default ACI for ITIM User: Grant Add to Service Owner Group	Identity Manager User	Service Owner Group
Identity Manager User	Default ACI for ITIM User: Grant All to Help Desk Group for Non-Admin Accounts	Identity Manager User	Help Desk Group
Identity Manager User	Default ACI for ITIM User: Grant All to Service Owner	Identity Manager User	Service Owner
Identity Manager User	Default ACI for ITIM User: Grant Delegate to Service Owner/Manager/Help Desk Groups	Identity Manager User	Service Owner Group Manager Group Help Desk Group
Identity Manager User	Default ACI for ITIM User: Grant Search to Self	Identity Manager User	Self
Identity Policy	Default ACI for Identity Policy: Grant All to Domain Admin/Service Owner Group	erIdentityPolicy	Domain Admin Service Owner Group
ITIM Group	Default ACI for ITIM Group: Grant All to Supervisor/Domain Admin/Sponsor	erSystemRole	Supervisor Domain Admin Sponsor
ITIM Group	Default ACI for ITIM Group: Grant Search to Help Desk Group for Non-Admin Group	erSystemRole	Help Desk Group

Table 13. Default access control items (continued)

Protection category	Name	Type	Principal
ITIM Group	Default ACI for ITIM Group: Grant Search to Service Owner Group	erSystemRole	Service Owner Group
Location	Default ACI for Location: Grant All to Supervisor/Domain Admin/Sponsor	Location	Supervisor Domain Admin Sponsor
Location	Default ACI for Location: Grant Search to Help Desk/Auditor/Service Owner Groups	Location	Help Desk Group Auditor Group Service Owner Group
Organizational Unit	Default ACI for Org Unit: Grant All to Supervisor/Domain Admin/Sponsor	Organizational Unit	Supervisor Domain Admin Sponsor
Organizational Unit	Default ACI for Org Unit: Grant Search to Help Desk/Auditor/Service Owner Groups	Organizational Unit	Help Desk Group Auditor Group Service Owner Group
Password Policy	Default ACI for Password Policy: Grant All to Domain Admin/Service Owner Group	erPasswordPolicy	Domain Admin Service Owner Group
Person	Default ACI for Person: Grant All to Supervisor/Domain Admin/Sponsor/ Help Desk Group	inetOrgPerson	Supervisor/Manager Domain Admin Sponsor Help Desk Group
Person	Default ACI for Person: Grant Change Password to Service Owner Group	inetOrgPerson	Service Owner Group
Person	Default ACI for Person: Grant Search/ Change Password/View and Change Role to Self	inetOrgPerson	Self
Person	Default ACI for Person: Grant Search to Service Owner and Auditor Group	inetOrgPerson	Auditor Group
Person	Default ACI for Person: Grant Search and role assignment to Privileged Administrator Group	erPersonItem	Privileged Administrator Group
Provisioning Policy	Default ACI for Provisioning Policy: Grant All to Domain Admin/Service Owner Group	erProvisioningPolicy	Domain Admin Service Owner Group
Provisioning Policy	Default ACI for Provisioning Policy: Grant Search to Auditor Group	erProvisioningPolicy	Auditor Group
Recertification Policy	Default ACI for Recertification Policy: Grant All to Service Owner Group	erRecertificationPolicy	Service Owner Group

Table 13. Default access control items (continued)

Protection category	Name	Type	Principal
Recertification Policy	Default ACI for Recertification Policy: Grant Search to Auditor/Manager Groups	erRecertificationPolicy	Auditor Group Manager Group
Report	Default ACI for Access Control Item (ACI) Report: Grant Run to Auditor Group	Access Control Item	Auditor Group
Report	Default ACI for Access Report: Grant Run to Auditor/Service Owner Groups	Access Report	Auditor Group Service Owner Group
Report	Default ACI for Account Report: Grant Run to Auditor Group	Account Report	Auditor Group
Report	Default ACI for Account Requests by an Individual Report: Grant Run to Auditor/Manager Groups	Account Operations Done by an Individual	Auditor Group Manager Group
Report	Default ACI for Account Requests Report: Grant Run to Auditor/Manager Groups	Account Operations	Auditor Group Manager Group
Report	Default ACI for Account on a Service Report: Grant Run to Auditor/Service Owner Groups	Summary of Accounts on Service	Auditor Group Service Owner Group
Report	Default ACI for Approval/Rejection Report: Grant Run to Auditor/Manager Groups	Approvals and Rejections	Auditor Group Manager Group
Report	Default ACI for Audit Events Report: Grant Run to Auditor Group	Audit Events	Auditor Group
Report	Default ACI for Dormant Accounts Report: Grant Run to Auditor/Service Owner Groups	Dormant Accounts	Auditor Group Service Owner Group
Report	Default ACI for Entitlements Granted to an Individual Report: Grant Run to Auditor Group	Entitlements Granted to an Individual	Auditor Group
Report	Default ACI for Individual Access Report: Grant Run to Auditor/Manager/Service Owner Groups	Individual Access	Auditor Group Manager Group Service Owner Group
Report	Default ACI for Noncompliant Accounts Report: Grant Run to Auditor Group	Noncompliant Accounts	Auditor Group
Report	Default ACI for Operation Report: Grant Run to Auditor/Manager Groups	Operation Report	Auditor Group Manager Group
Report	Default ACI for Orphan Accounts Report: Grant Run to Auditor/Service Owner Groups	Orphan Accounts	Auditor Group Service Owner Group

Table 13. Default access control items (continued)

Protection category	Name	Type	Principal
Report	Default ACI for Pending Approvals Report: Grant Run to Auditor/Manager Groups	Pending Approvals	Auditor Group Manager Group
Report	Default ACI for Pending Recertification Report: Grant Run to Auditor/Manager/Service Owner Groups	Accounts/Access Pending Recertification Report	Auditor Group Manager Group Service Owner Group
Report	Default ACI for Policies Governing a Role Report: Grant Run to Auditor Group	Policies Governing a Role	Auditor Group
Report	Default ACI for Policies Report: Grant Run to Auditor Group	Policies	Auditor Group
Report	Default ACI for Recertification History Report: Grant Run to Auditor/Manager/Service Owner Groups	Recertification History Report	Auditor Group Manager Group Service Owner Group
Report	Default ACI for Recertification Policies Report: Grant Run to Auditor/Manager/Service Owner Groups	Recertification Policies Report	Auditor Group Manager Group Service Owner Group
Report	Default ACI for Reconciliation Statistics Report: Grant Run to Auditor/Service Owner Groups	Reconciliation Statistics	Auditor Group Service Owner Group
Report	Default ACI for Rejected Report: Grant Run to Auditor/Manager Groups	Rejected Report	Auditor Group Manager Group
Report	Default ACI for Services Report: Grant Run to Auditor/Service Owner Groups	Services	Auditor Group Service Owner Group
Report	Default ACI for Suspended Accounts Report: Grant Run to Auditor Group	Suspended Accounts	Auditor Group
Report	Default ACI for Suspended User Report: Grant Run to Auditor Group	Suspended Individuals	Auditor Group
Report	Default ACI for User Accounts by Role Report: Grant Run to Auditor Group	Individual Accounts by Role associated with Provisioning Policy	Auditor Group
Report	Default ACI for User Accounts Report: Grant Run to Auditor/Manager Groups	Individual Accounts	Auditor Group Manager Group
Report	Default ACI for User Requests Report: Grant Run to Auditor/Manager Groups	User Report	Auditor Group Manager Group
Separation of Duty Policy	Default ACI for Separation of Duty Policy: Grant All to Owner	erSeparationOfDutyPolicy	Owner

Table 13. Default access control items (continued)

Protection category	Name	Type	Principal
Separation of Duty Policy	Default ACI for Separation of Duty Policy: Grant Search to Auditor Group	erSeparationOfDutyPolicy	Auditor Group
Service	Default ACI for ITIM Service: Grant All to Domain Admin	ITIM	Domain Admin
Service	Default ACI for Service: Grant Add/Reconcile to Service Owner Group	erServiceItem	Service Owner Group
Service	Default ACI for Service: Grant All to Domain Admin	erServiceItem	Domain Admin
Service	Default ACI for Service: Grant Rights to Everyone	erServiceItem	Everyone
Service	Default ACI for Service: Grant Search/Modify/Remove/Reconcile/recertOverride/customizeAccountForm/enforcePolicy/restartService to Owner	erServiceItem	Owner
Service	Default ACI for Service: Grant Search to Access Owner/Supervisor/Auditor Group	erServiceItem	Access Owner Supervisor Auditor Group
Service Group	Default ACI for Service Group: Grant All to Service Owner	erGroupItem	Service Owner
Service Group	Default ACI for Service Group: Grant Search/View Access to Everyone	erGroupItem	Everyone
Service Group	Default ACI for Service Group: Grant Search to Auditor Group/Supervisor	erGroupItem	Auditor Group Supervisor
Service Group	Default ACI for Service Group: Grant All (except for Add operation) to Access Owner	erGroupItem	Access Owner
Service Selection Policy	Default ACI for Service Selection Policy: Grant All to Domain Admin	erHostSelectionPolicy	Domain Admin
Static Organizational Role	Default ACI for Org Role: Grant All to Supervisor/Domain Admin/Sponsor	Organizational Role	Supervisor Domain Admin Sponsor
Static Organizational Role	Default ACI for Org Role: Grant Search/Modify for Everyone	Organizational Role	Everyone
Static Organizational Role	Default ACI for Org Role: Grant Search to Help Desk/Auditor Groups	Organizational Role	Help Desk Group Auditor Group
Workflow Design	Default ACI for Workflow: Grant All to Domain Admin/Service Owner Group	erWorkflowDefinition	Domain Admin Service Owner Group

Creating an access control item

As an administrator, you can create an access control item to specify a set of operations and permissions. Then, you can apply the access control item to the roles and groups that you want to be governed by the access control item.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

If you create an access control item that applies to a new group, create the group first.

About this task

You can use the **Create access control item** wizard to create additional access control items.

To create an access control item, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Manage Access Control Items**.
2. On the **Manage Access Control Items** page, in the **Access Control Items** table, click **Create**.
3. On the **Create Access Control Item** wizard, on the **General** page, specify the name of the access control item and a protection category. If you selected **Account** as your protection category, specify an object class. Specify on which business unit the access control item applies, and whether business subunits are also controlled. Specify whether to apply protection to all objects, or to a subset of objects that are selected by a filter statement that you provide. Then, click **Next**.
4. On the **Operations** page, select one or more operations, and set the permission to Grant, Deny, or None. Then, click **Next**.
5. On the **Permissions** page, for each **Read** or **Write** field for each attribute, select Grant, Deny, or None. The table might contain multiple pages of attributes. Click the right arrow button to set permissions for other attributes on the other pages. Then, click **Next**.
6. On the **Membership** page, specify the focus for roles or group membership that this access control item governs.
7. Click **Finish**.
8. On the **Success** page, click **Close**.

What to do next

You might associate the access control item with a customized group that you previously created.

After you create an access control item or change an existing access control item, run a data synchronization to ensure that other Security Identity Manager processes, such as the reporting engine, use the new or changed access control item.

Changing an access control item

As an administrator, you can change an access control item if necessary.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

If you change an access control item, investigate in advance which business units and objects are affected by the change.

About this task

You can use the **Change access control item** notebook to change an existing access control item.

To change an access control item, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Manage Access Control Items**.
2. On the **Manage Access Control Items** page, type information about the access control item in the **Search information** field, and click **Search**.
3. In the **Access Control Items** table, select an access control item, and then click **Change**.
4. On the **General** page, you might change the name of the access control item. You can specify applying protection to all objects. Alternatively, you can specify applying protection to a subset of objects that is selected by a filter statement that you provide. Then, click **Apply** to save your changes, or click another tab.
5. On the **Operations** page, change the permissions for one or more operations. Then, click **Apply** to save your changes, or click another tab.
6. On the **Permissions** page, change the permissions for one or more attributes. Then, click **Apply** to save your changes, or click another tab.
7. On the **Membership** page, change who this access control item governs. Then, click **Apply** to save your changes, or click another tab.
8. Click **OK** to save the changes.
9. On the **Success** page, click **Close**.

What to do next

After you create an access control item or change an existing access control item, run a data synchronization to ensure that other Security Identity Manager processes, such as the reporting engine, use the new or changed access control item.

Deleting an access control item

As an administrator, you can delete an access control item if necessary. For example, you might create another access control item that replaces the access control item that you intend to delete.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Deleting an access control item revokes any authorization granted to the user (member of the access control item) for a particular protection category. Apply your organization's process that changes or transfers the membership of an access control item before deleting the access control item from the system.

About this task

To delete an access control item, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Manage Access Control Items**.
2. On the **Manage Access Control Items** page, type information about the access control item in the **Search information** field, and click **Search**.

3. In the **Access Control Items** table, select an access control item, and then click **Delete**. Although you can delete a default access control item that IBM Security Identity Manager provides, you might want to first ensure that an alternative access control item exists.
4. On the **Confirm** page, ensure that the name of the access control item is correct, and then click **Delete**.
5. On the **Success** page, click **Close**.

Chapter 8. Role administration

Organizational roles are a method of providing users with entitlements to managed resources. Organization roles determine which resources are provisioned for a user or set of users who share similar responsibilities. A role is a job function that identifies the tasks that a person can do and the resources to which the person has access.

If users are assigned to an organizational role, managed resources that are available to that role then become available to the users in that role. The resources must be properly tied to that role.

You can assign a user to one or more roles. Additionally, roles can themselves be members of other roles, in what is termed *child roles* that contribute to role hierarchy.

A role might be a child role of another organizational role, which then becomes a parent role. That child role inherits the permissions of the parent role. A role might be a child role of another organizational role in a provisioning policy. That child role also inherits the permissions of provisioning policy.

Activities are often assigned to roles rather than to individuals. This role-based model lowers the risk that individuals might gain more system access than required by their job function. You can also define policies to prevent users from having multiple roles that result in a conflict of interest.

Role overview

A role, also termed an organizational role, is a modeling concept that serves as a convenience in administering policy.

The descriptive properties of a role, particularly its name, are significant and imply the purpose of the role. For example, a role might be named manager, designer, or auditor. In IBM Security Identity Manager, a role is used to support user and access provisioning.

A role can be used to support different provisioning models:

- Role-based, to automate and to accelerate the process of granting access to resources. A role-based model lowers the risk of individuals who might gain more system access than required by their job or other relationship to a company.

The operational needs of an enterprise determine the assignment of users to roles. For example, a user might have a role as a help desk assistant or auditor. In a role-based model, users receive a specific set of accounts and access rights based on role membership. When a user is removed from a role, the entire set of accounts and access rights are also removed.

The role might be a child role of another organizational role, which then becomes a parent role. The child role inherits the permissions of the parent role.

- Request-based provisioning, in which a role represents an access to an IT resource that can be directly searched and requested by a user.

The access entitlements of the role are defined by a provisioning policy. Approval processing can be supported for a role request; the user is assigned to the role after the request is approved. When the user is a member of a role, access rights are granted. Removing a user from that role also removes the entire set of access that the role granted.

If a role is a child role of another organizational role in a provisioning policy, then that child role also inherits the permissions of provisioning policy.

Using the processes provided by Security Identity Manager, a user in a business unit might have a role as illustrated in the simplified diagram in [Figure 1 on page 668](#):

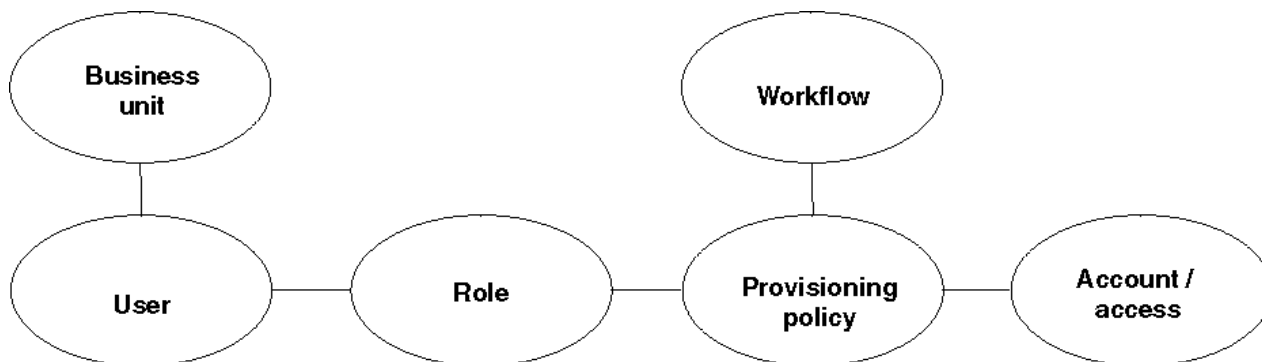


Figure 1. User access to resources

To enable the user to access one or more resources, a provisioning policy can be configured so that the reference role in the policy is granted with the set of entitlements for the resources.

Security Identity Manager also supports two ways to define an organizational role: static role and dynamic role. For a static organizational role, assigning a person to a static role is a manual process. For a dynamic role, role membership is specified as a filter in the role definition that selects role members based on some attribute, such as a business title.

Role hierarchy change enforcement

The people affected by the role hierarchy change operation are evaluated against all applicable policies in the system. Evaluation includes policies that are not related to any of the parent roles. As a result, you might find accounts not related to the role hierarchy change that is being enforced.

For example, you might have a group of new users from an HR feed that did not have workflow enabled. This group of people is entitled to accounts on *Service A* automatically, but the accounts are not created because the HR feed bypassed policy evaluation. A role hierarchy change operation might affect the same group of users so that they are provisioned to *Service B*. Accounts on both *Service A* and *Service B* are created.

Creating roles

You can create roles to allow users to use managed resources, depending on their membership in the role.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Determine the range of roles that organization members require to access resources.

About this task

To create a role, complete these steps:

Procedure

1. From the navigation tree, select **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, in the **Roles** table, click **Create**.
The **Create Role** wizard is displayed.
3. On the **Role Type** page, specify the appropriate values and click **Next**.

The pages vary, depending on whether you specify a static or a dynamic role. Complete each page to specify the necessary information for the role.

Note: On the **Access Information** page, you can provide owner information and other access information such as access type, name, description, search terms, or badges.

4. Click **Finish** when you are done specifying all the expected information.
5. On the **Success** page, click **Close**.

What to do next

You might associate a provisioning policy with the role that you created.

Modifying roles

You can modify roles that allow users or other roles to use managed resources, depending on their membership in the role.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Determine the effects of the change. For example, determine whether changing the scope or the filter definition for a dynamic role correctly limits or expands which users can access resources.

About this task

Procedure

1. From the navigation tree, click **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**.
A list of roles that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Roles** table, click the icon () next to the role that you want to modify, and then click **Change**.
The **Change Role** wizard is displayed.
3. On the **Change Role** wizard, edit or modify the existing information on each corresponding page for the role.
The pages vary, depending on whether you specify a static or a dynamic role.
Note: On the **Access Information** page, you can provide owner information and other access information such as access type, name, description, search terms, or badges.
4. Click **OK** when you are done specifying all the expected information on one or all the pages.

Results

A **Success** page is displayed, indicating that you successfully updated the role.

What to do next

On the **Success** page, click **Close**.

Values and formats for CSV access data (role)

A role access CSV file can contain multiple values and supported formats.

Consider these points before you work with any CSV files for a role access:

- If you use a custom label for AccessType, specify the key in the CSV file.
- If you use a custom label for badge text, add a \$ prefix on the key. For example, \$mail.
- Define multiple values for search terms and badges with a semicolon (;) separator.
- Define the AccessType hierarchy with a colon (:) separator.
- Use the badgeText~badgeStyle format for badges.

Define CSV columns for a role access as follows:

Field name	Value
ROLE_DN, ROLE_NAME	Not modifiable.
DEFINE_AS_ACCESS	TRUE or FALSE. If you do not assign any value, then FALSE is assumed.
ACCESS_NAME	Required for services and groups, and contains a maximum length of 240 characters. This field is not available for roles.
ACCESS_TYPE	Required. You must specify an access type that is defined in IBM Security Identity Manager.
ACCESS_DESCRIPTION	Contains a maximum length of 240 characters.
ICON_URL	Provide a valid icon URL value on the access definition.
SEARCH_TERMS	Each search term contains a maximum length of 80 characters. You can have multiple search terms.
ADDITIONAL_INFORMATION	Contains a maximum length of 1024 characters.
BADGES	The maximum length for each badge text is 512 characters. You can have multiple badges. The badge text that is prefixed with a \$ sign cannot contain delimiter characters such as ., ;, =, or white space.

A role access CSV file for an export or import operation in the IBM Security Identity Manager administration console contains these columns with sample values and supported formats:

ROLE_NAME	DEFINE_AS_ACCESS	ACCESS TYPE	ICON_URL
admin	TRUE	Application:Role:Manager	/itim/ui/custom/ui/images/homepage/RequestAccess.png
AIX Role	TRUE	Mail:Role	http://www-03.ibm.com/ibm/history/exhibits/logo/images/920911.jpg
Default Role	FALSE	AccessRole	/itim/ui/custom/ui/images/homepage/RequestAccess.png

ROLE_NAME	SEARCH_TERMS	ADDITIONAL_INFORMATION	BADGES	SERVICE_DN
admin	Application; Role access	Role that is used by a client user.	\$admin~yellow;custom~green	erglobalid=5628670506891199803,ou=roles,erglobalid=000000
AIX Role	Employee;Role;Role access	Used by the customer to deploy server.	Role~grey	erglobalid=5628669752130902869,ou=roles,erglobalid=000000
Default Role	Mail;Unique ID	BVT server that is used to run BVT from developer and tester.	\$mailrisk~red	erglobalid=5628670337030215245,ou=roles,erglobalid=000000

Exporting access data for a role

Export the access data for a role in a comma-separated value (CSV) file format by using the IBM Security Identity Manager Console.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you export a role, you must have ACI privileges for Search Operations, and read permissions for the Access Options attribute, on the role that you want to view. If the necessary privileges do not exist, then the role is not exported.

The **Export Access Data** button is not active until you select some role accesses to activate it. Only the role access that you selected is exported as access data.

About this task

Export the selected role access data in a CSV file format for your requirements.

Procedure

1. From the navigation tree, select **Manage Roles**.

The **Manage Roles** page is displayed.

2. On the **Manage Roles** page, in the **Roles** table, click **Export Access Data**.

The **Export access data** page is displayed. After you submit the export request, a process status indicates the advancement of the export operation.

3. Optional: Click **Cancel** to discontinue the export operation.

4. Click **Download Exported File** to download the CSV file on your local system by using your web browser settings.

The exported CSV file contains all the role access data.

Note: Click **Download Export Log File** to view any error or log information about the export operation. This button is displayed only if the submitted export operation contains any log information or encountered any errors.

Results

The exported CSV file contains all the access data for a role. Click **Close** to exit from the **Export access data** page.

What to do next

Import access data for a role, or you can continue to export access data by clicking **Export Access Data** in the **Manage Roles** page.

Importing access data for a role

Use the IBM Security Identity Manager Console to import the role access data from a comma-separated value (CSV) file.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

The privileged user that uploads the CSV file must have the appropriate permissions.

Before you import a role, you must have ACI privileges for Search Operation, Modify Operation, and read permissions for the Access Options attribute, on the role that you want to update. If the necessary privileges do not exist, then the role is not imported.

Before you import a CSV file, verify that the CSV-related conventions are met. They are as follows:

- The access type hierarchy is represented in the following format, and each access type be separated by a colon (:). For example:

```
AccessType1:AccessType2
```

- The badge information is provided in the following format. For example:

```
badgeText~badgeStyle
```

- Multiple badges can be assigned to accesses in the following format, and each badge must be separated by a semicolon (;). For example:

```
Badge1~red;Badge2~green
```

- Multiple search terms and access types can be specified by using the semicolon (;) separator.
- The relevant keys must be provided in the CSV file for the customized labels that are related to badges and access types.

About this task

Only the accesses with the **Define as Access** set to `True` are defined as accesses, and the corresponding data is imported.

Procedure

1. From the navigation tree, select **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, in the **Roles** table, click **Import Access Data**.
The **Import access data** page is displayed.
3. Click **Browse** in **File to Upload (.CSV)** to locate and upload a valid CSV file that contains all the access data for a role.
4. Click **Import** to import the CSV file.
After you submit the import request, a process status indicates the advancement of the import operation.

Note: If you click **Import** with an invalid file format, a message is displayed to inform you that the file format is not valid.

If any problems occur when you are importing a CSV file, then close the **Import access data** page to continue working with the IBM Security Identity Manager Console. The problems might be due to one of the following conditions:

- The access data CSV file does not exist.
 - The CSV file was renamed.
 - The CSV file does not contain appropriate separators or delimiters.
5. Optional: Click **Cancel** to discontinue the import operation.

Note: Click **Download Import Log File** to view any error or log information about the import operation. This button is displayed only if the submitted import operation contains any log information or encountered any errors.

Results

The imported CSV file contains all the access data for a role. Click **Close** to exit from the **Import access data** page.

What to do next

Export access data for a role, or you can continue to import access data by clicking **Import Access Data** in the **Manage Roles** page.

Defining access by default for a role

When you create a role, you can ensure that access is defined by default.

About this task

If the property attribute **enable.role.access** is set to **true**, access is defined by default during role creation.

Procedure

1. In the administration console, click **Manage Role**.
2. Click **Create Role**.
3. From the **Access Information** tab, ensure that **Enable access for this role** is selected by default.
The default access type is set to **Role** or the first access type if **Role** is removed.

Classifying roles

You can assign a classification to a role.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

You can classify a role during role creation, or after a role is already created.

Procedure

1. From the navigation tree, click **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**.
A list of roles that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Roles** table, click the icon () next to the role, and then click **Change**.
The **Role Type** page is displayed.
3. On the **Role Type** page, complete these steps:
 - a) Select a role classification, such as **Application role** or **Business role**, from the **Role classification** list, and then click **OK**.
By default, no role classification is selected.

Results

A **Success** page is displayed, indicating that you successfully updated the role.

What to do next

On the **Success** page, click **Close**.

Specifying owners of a role

You can specify one or more owners of a role. The owners can be users or roles. You can specify owners of a role during role creation, or after a role is already created.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task



The result of designating people or roles as a role owner include:

- In workflows, role owners can act as participants. In particular, in the approval workflow for assigning roles to users, role owners can act as participants.
- In access control item (ACI) evaluations for management of roles, the role owner can act as a principal. This capability allows more than one person to share this delegated administrative responsibility. A special case of this scenario is when the role is an owner of itself. In that case, the members of the role can also be the administrators. You can set up a structure so that any member of the role can add other members.
- In exporting roles, the relationships to the role owners are also exported. Relationships to users that are role owners are exported, but the users themselves are not exported. On import, the ownership relationships are created only if the users exist in the import.

In any of these scenarios, being a child or member of a child role of a role owner is equivalent to being a child or member of the role itself.

To specify roles and users that have ownership of the role, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**.
A list of roles that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Roles** table, click the icon () next to the role, and then click **Change**.
The **Role Type** page is displayed.
3. Click **Access Information**.
4. On the **Access Information** page, complete these steps:
 - a) Click the twisty icon  next to **Owners**.
The **Role Owners** and **User Owners** tables are displayed.
 - b) Click **Add** to add owners to a list of role owners or user owners.

You can select role owners, user owners, or a combination of both.

The **Select Roles** or **Select Users** page is displayed.

- c) On the **Select Roles** or **Select Users** page, search for and select the owners to have ownership of the role, and then click **OK**.

Results

The **Access Information** page is displayed, and the list of owners is updated in the **Role Owners** and **User Owners** tables.

What to do next

You can continue adding or removing owners of the role, or click **OK**.

Displaying a role-based access in the user interface

You can display an access based on a role to users who request access in the Identity Service Center user interface.

Before you begin


Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

You can use the **Manage Roles** page to display an access in the Self Service or the Identity Service Center user interface.

To display an access in the Self Service or the Identity Service Center user interface, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether the search is done against role names or descriptions, or against business units, and then click **Search**.
A list of roles that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Roles** table, click the icon () next to the role that you want to modify, and then click **Change** to display the **Role Type** page.
3. Click the **Access Information** tab.
4. On the **Access Information** page, click **Enable access for this role**.
5. For a static role, click **Show this role as a common access** to show the role as an access that a user can select.
6. On the **Access Information** page, select an access type, such as **Application** in the **Select access type** tree.

You can also specify other access information such as description, search terms, more information, or badges.

7. Click **OK**.

Results

A **Success** page indicates that you successfully updated the role.

What to do next

On the **Success** page, click **Close**.

You might change the provisioning policy that is associated with the role that has the access type.

Role assignment attributes

You can define role assignment attributes. The attributes can be associated with a person-role relationship.

Optional role assignment attributes tasks are:

- Defining role assignment attributes when creating or modifying a static role.
- Associating a custom label with each assignment attribute.
- Specifying assignment attribute values when adding user members to the role. For example, a static role named *Clerk* has an assignment attribute defined as `CreditLimit`. When adding user members to this role, you can specify the `CreditLimit` value for each user as part of the role assignment.
- Specifying assignment attribute values to the existing user members of the role.

Note:

1. Only static roles support assignment attributes.
2. Only the string type and text widget of assignment attributes are supported.

ACI capabilities for role assignment attributes

Both the default and new ACIs supports attribute-level permissions for role assignment attributes like other attributes in the role definition. You can now modify or create ACIs. You can set attribute-level permissions for granting or denying usage of these role assignment attributes within the role definition. Only authorized users can read or write assignment attributes. Additionally, you can:

- Set ACIs to read or write assignment attribute values when adding a user to the role.
- Set assignment attribute values to the existing user members.

ACI works the same way as it does for other entities. There is no ACI on specific role assignment attributes. The following attributes are available:

- `erRoleAssignmentKey` is on the role that dictates the permission to define role assignment attributes on the role and an attribute.
- `erRoleAssignments` is on the person that dictates the permission to assign values for the assignment attributes.

To view the role assignment attribute value on a person form, the logged in user must have read permissions on `erRoles`, `erRoleAssignmentKey` and `erRoleAssignments`.

To edit the role assignment attribute value on a person form, the logged in user must have read permissions on `erRoles`, `erRoleAssignmentKey` and write permissions on `erRoleAssignments`.

You cannot define ACI on the assignment attribute that you defined on the role.

JavaScript capabilities for role assignment attributes

You can access these capabilities for role assignment attributes within the JavaScript interface:

- The role assignment attributes of the role schema. For example, you can access a role object inside an entitlement workflow.
- The role assignment attributes and their values for users in role membership. For example, you can access a person object within a JavaScript provisioning policy entitlement.

JavaScript APIs include:

- Person
 - Person.getAllAssignmentAttributes()
 - Person.getRoleAssignmentData()
 - Person.getRoleAssignmentData(String roleAssignedDN)
 - Person.removeRoleAssignmentData()
 - Person.updateRoleAssignmentData()
 - Person.getRemovedRoles()
 - Person.isInRole()
 - Person.removeRole()
- Role
 - Role.getAssignmentAttributes()
 - Role.getAllAssignmentAttributes()
 - Role.setAssignmentAttributes()
- RoleAssignmentAttribute
 - RoleAssignmentAttribute.getName()
 - RoleAssignmentAttribute.getRoleName()
 - RoleAssignmentAttribute.getRoleDN()
- RoleAssignmentObject
 - RoleAssignmentObject.getAssignedRoleDN()
 - RoleAssignmentObject.getDefinedRoleDN()
 - RoleAssignmentObject.addProperty()
 - RoleAssignmentObject.getChanges()
 - RoleAssignmentObject.getProperty()
 - RoleAssignmentObject.getPropertyNames()
 - RoleAssignmentObject.removeProperty()
 - RoleAssignmentObject.setProperty()

For more information, see the reference pages in the *IBM Security Identity Manager Reference Guide*.

Role assignment attributes and the Self Service or the Identity Service Center user interface

For more information about adding or modifying role assignment attributes for a user profile in the user interface, see [Modifying role assignment attributes for your personal profile](#) in the Service Center documentation.

Defining assignment attributes when creating a role

When creating a role, you can optionally define assignment attributes to be associated with the role.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You can associate a custom label with an assignment attribute by adding an attribute name prefixed with `roleAssignmentAttribute` in the `customLabels.properties` resource bundle. This operation provides the display label for the assignment attribute. For example, `roleAssignmentAttribute.creditLimit="Credit Limit Value"`. The key for the assignment attribute of the same role must be unique.

Procedure

To define assignment attributes to be associated with a role, complete these steps:

1. From the navigation tree, click **Manage Roles**.

The **Manage Roles** page is displayed.

2. On the **Manage Roles** page, click **Create** and proceed through the wizard panels until you reach the **Assignment Attributes** page.

If you selected a role type of Dynamic, the **Assignment Attributes** page is not displayed.

3. In the **Attribute Name** field, specify a name for the assignment attribute you want to add.

Note: You must not enter a space, semi-colon, or both when specifying an assignment attribute name.

4. Click **Add**.

The new attribute is displayed in the assignment attributes table. If the attribute has any display label defined in the `customLabels.properties` resource bundle, then the assignment attribute table displays the same label.

5. Click **Next** to continue through the Role Creation wizard.

Results

A Success page is displayed, indicating that you successfully created the role.

Defining assignment attributes for an existing role

When modifying an existing role, you can optionally define assignment attributes to be associated with the role.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You can associate a custom label with an assignment attribute by adding an attribute name prefixed with `roleAssignmentAttribute` in the `customLabels.properties` resource bundle. This operation provides the display label for the assignment attribute. For example, `roleAssignmentAttribute.creditLimit="Credit Limit Value"`. The key for the assignment attribute of the same role must be unique.

Procedure

To define assignment attributes to be associated with a role, complete these steps:

1. From the navigation tree, click **Manage Roles**.

The **Manage Roles** page is displayed.


2. On the **Manage Roles** page, complete these steps:

- a) Type information about the role in the **Search information** field.

- b) In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**.

A list of roles that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
- c) In the **Roles** table, click the icon () next to the role, and then click **Change**.
The **Role Type** page is displayed.
3. Click **Assignment Attributes**.
The **Assignment Attributes** page is displayed. If you selected a role type of Dynamic, the **Assignment Attributes** page is not displayed.
4. To add an attribute to an existing role, enter a name in the **Attribute Name** field for the assignment attribute you want to add.
Note: You must not enter a space, semi-colon, or both when specifying an assignment attribute name.
5. Click **Add**.
The new attribute is displayed in the assignment attributes table. If the attribute has a display label defined in the `customLabels.properties` resource bundle, then the assignment attribute table displays the same label.
6. Optionally, you can remove existing assignment attributes if no values are set with any user member of the role.

Results

A Success page is displayed, indicating that you successfully updated the role.

Setting assignment attribute values to the user members of a role


You can set assignment attribute values to the user members of a static organizational role if you defined assignment attributes in the role definition.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

To set assignment attributes to the user members in a static role, complete these steps:

1. From the navigation tree, click **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**.
A list of roles that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Roles** table, click the icon () next to the role to which you want to add members, and then click **Manage User Members**.
The **Manage User Members and Child Roles** page is displayed.
3. On the **Manage User Members and Child Roles** page, complete these steps:
 - a) Type information about the user in the **Search information** field.

- b) In the **Search by** field, select the attribute on which you want to search, and then click **Search**, or click **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria.

The **Users** table is displayed, listing the users that match the search criteria.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

- c) In the **Users** table, select the check box next to one or more user members that you want to set assignment attribute values, and then click **Set Assignment Attributes**.

Selecting the check box at the top of this column selects all user members.

The **Associate Role Assignment Attributes** page is displayed.

Note: The **Associate Role Assignment Attributes** page is displayed if you defined role assignment attributes when creating the role. These conditions apply:

- When the role is a child role to one or more parent roles, the role assignment attributes includes the attributes from all of the parent roles.
- When you select a user member, the existing attribute value is displayed if you assigned values when adding user members.
- The values are not displayed if you have not set any of them in the assignment attributes when adding user members.
- When you select multiple user members, the values for assignment attributes are joined.

4. On the **Associate Role Assignment Attributes** page, complete these steps:

- a) Enter values for the role assignment attributes.

In the role assignment attributes table, click the name of the assignment attribute. The **Set Assignment Values** page is displayed.

- b) Enter a value for the attribute and click **Add**. You can add more than one value. When finished, click **OK**.

The **Associate Role Assignment Attributes** table is displayed.

- c) When finished adding values to attributes, click **Continue**.

A confirmation page is displayed.

5. On the **Confirm** page, specify the date and time for the user members to be added with the assignment attribute values. Then click **Submit**. Click **Back** to return to the previous page.

Results

A **Success** page is displayed, indicating that you successfully added the user members to the role membership.

What to do next

View the status of the request, or click **Close**.

Configuring access catalog information for a role

Configure the access catalog information for a role in the Administrator Console so you can use it in the Identity Service Center Request Access.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You can also configure the access catalog information for a new role or for an existing role.

About this task

Configure the access information for a role by defining certain accesses with the use of a badge. You can highlight certain accesses with badges by attaching text that contains some formatting such as color and font type.

Procedure

To configure the role access information, complete these steps:

1. From the navigation tree, select **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, in the **Roles** table, click **Create** to display the **Create Role** wizard.
Alternatively, select an existing role and click **Change** to configure its access catalog information.
3. Specify the appropriate values on the **Role Type** page.
The pages vary, depending on whether you specified a static or a dynamic role.
4. Specify the appropriate values on the **General Information** page.
5. On the **Access Information** page, complete these steps to configure the access information:
 - a) Expand the **Owners** section to specify the roles or users that are the owners of the role.
 - b) Select the **Enable access for this role** check box.
 - c) Expand the **Select access type** or the **Change access type** tree to select an access type.
The tree label depends on whether you want to create or modify a service.
 - d) Provide a uniform resource identifier (URI) string in the **Icon URL** field for the access icon.
 - e) Specify search strings in the **Search terms** field to return specific search terms.
Add or delete the search terms to suit your requirements.
 - f) Specify any free form information about the access item in the **Additional information** field.
 - g) Expand the **Badges** section to specify the badges that are associated with the role.
 - Specify a badge text in the **Badge text** field.
 - Assign a class from the **Badge class** list for the badge text.

You can see the preview of your badge specifications in the **Preview** area.
6. Depending on whether you created or modified the role access information, click **OK** or **Finish** when you are done.

Results

The access information is added to the role object and stored in the Security Identity Manager LDAP server.

What to do next

On the **Success** page, click **Close**. You can also do the following actions:

- Create or modify another role
- Return to the list of roles that you were working with

Deleting roles

You can delete roles that allow users to use managed resources, depending on their membership in the role.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

You cannot delete a role that has user members or child roles. You must remove all of the user members and child roles from the role before you can delete the role.

You cannot delete a static role that has membership in a policy, such as a provisioning or separation of duty policy. You must first remove the static role from the policy.

To delete a role, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against role name or description, or against business units, and then click **Search**.
A list of roles that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Roles** table, select the check box next to the role that you want to delete, and then click **Delete**. Selecting the check box at the top of this column selects all roles.
A confirmation page is displayed.
3. On the **Confirm** page, click **Delete**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully removed the role.

What to do next

Continue working with roles, or click **Close**.

Managing users as members of a role

You can view, add, or remove *user members*, which are users that are members of a role.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To manage user members, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against role name or description, or against business units, and then click **Search**.
A list of roles that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Roles** table, click the icon () next to the role, and then click **Manage User Members**.
The **Manage User Members and Child Roles** page is displayed.
4. On the **Manage User Members and Child Roles** page, complete these steps:
 - a) Select **User member**.
 - b) Type information about the user in the **Search information** field.
 - c) In the **Search by** field, specify the attribute on which you want to search, and then click **Search** or **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria.

Results

The **Users** table is displayed, listing the user members that match the search criteria.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

You can add user members to the role or remove user members from the role. You can also set assignment attribute values to user members of a role.

Click **Close** to close the page.

Adding users to membership of a role

You can add a user to the membership of a static organizational role.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To add a user to membership in a static role, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**.
A list of roles that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Roles** table, click the icon () next to the role to which you want to add members, and then click **Add User Members**.
The **Add User Members** page is displayed.
3. On the **Add User Members** page, complete these steps:
 - a) Type information about the user in the **Search information** field.
 - b) In the **Search by** field, select the attribute on which you want to search, and then click **Search**, or click **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria.
The **Users** table is displayed, listing the users that match the search criteria.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Users** table, select the check box next to one or more users that you want to add to the membership of the role, and then click **OK**.
Selecting the check box at the top of this column selects all users. You cannot select a user that is already a member of the role.
The **Associate Role Assignment Attributes** page is displayed.

Note: The **Associate Role Assignment Attributes** page is displayed only if you defined role assignment attributes when creating the role.
4. On the **Associate Role Assignment Attributes** page, complete these steps:
 - a) Enter values for the role assignment attributes.
 - b) Click **Continue**.
A confirmation page is displayed.
5. On the **Confirm** page, specify the date and time for the user members and role assignment attributes to be added. Then click **Submit**. Click **Back** to return to the previous page.

Results

A **Success** page is displayed, indicating that you successfully added the user members to the role membership.

What to do next

View the status of the request, or click **Close**.

Removing users from membership of a role

You can remove a user from membership in a static role.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To remove a user from membership in a static role, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**.
A list of roles that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Roles** table, click the icon () next to the role, and then click **Manage User Members**.
The **Manage User Members and Child Roles** page is displayed.
3. On the **Manage User Members and Child Roles** page, complete these steps:
 - a) Select **User**.
 - b) Type information about the user in the **Search information** field.
 - c) In the **Search by** field, specify the attribute on which you want to search, and then click **Search**, or click **Advanced**, depending on the type of search you want to do. The advanced search option opens a new page where you can specify additional search criteria.
The **Users** table is displayed, listing the users that match the search criteria.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - d) In the **Users** table, select the check box next to the user member that you want to remove from membership in the role, and then click **Remove**. Selecting the check box at the top of this column selects all user members.
A confirmation page is displayed.
4. On the **Confirm** page, specify the date and time for the membership removal to occur, and then click **Submit**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully removed the user members from the role membership.

What to do next

View the status of the request, view the membership of the role, or click **Close**.

Managing child roles

You can view, add, or remove *child roles*, which are roles that are members of another role. This relationship is a parent-child relationship between an organizational role (a parent role) and its child roles. A child role itself is an organizational role.

Before you begin


Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

When you add child roles to a parent role, ensure that there is not a separation of duty policy violation.

To manage child roles, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against role name or description, or against business units, and then click **Search**.
A list of roles that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Roles** table, click the icon () next to the role, and then click **Manage Child Roles**.
The **Manage User Members and Child Roles** page is displayed.
4. On the **Manage User Members and Child Roles** page, complete these steps:
 - a) Select **Child role**.
 - b) Type information about the role in the **Search information** field.
 - c) In the **Search by** field, specify whether to search against role name or description, or against business units, and then click **Search**.

Results

The **Child Roles** table is displayed, listing the child roles that match the search criteria.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

You can add more child roles to the parent role, or you can remove child roles from the role.

Click **Close** to close the page.

Adding child roles to a parent role

You can add a role (child role) to the membership of an organizational role (parent role). This task defines the roles in a role hierarchy. Circular parent-child relationships are not permitted.

Before you begin


Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

When you add child roles to a parent role, ensure that there is not a separation of duty policy violation.

To add a child role to a parent role, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**.
A list of roles that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Roles** table, click the icon () next to the role, and then click **Add Child Roles**.
The **Add Child Roles** page is displayed.
3. On the **Add Child Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**.
The **Roles** table is displayed, listing the roles that match the search criteria and that can be children of another role.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Roles** table, select the check box next to one or more roles that you want to add to the membership of the role, and then click **Add**.
Selecting the check box at the top of this column selects all roles. You cannot select a role that is already a child role.
 - d) Click **OK** to add the selected roles as children of the organizational role, or click **Cancel**.
4. On the **Confirm** page, specify the date and time for the membership removal to occur, and then click **Submit**, or click **Cancel**.

Results

A **Success** page is displayed, indicating that you successfully added a child role.

The roles are added as children of the organizational role, and the **Manage Roles** page is displayed.

What to do next

You can continue working with roles, or click **Close**.

Removing child roles from a parent role

You can remove a child role from a parent role.

Before you begin


Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Determine how removing the role affects the role hierarchy.

About this task

To remove a child role from a parent role, complete these steps:

Procedure

1. From the navigation tree, click **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**.
A list of roles that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Roles** table, click the icon () next to the role, and then click **Manage Child Roles**.
The **Manage User Members and Child Roles** page is displayed.
4. On the **Manage User Members and Child Roles** page, complete these steps:
 - a) Select **Child role**.
 - b) Type information about the role in the **Search information** field.
 - c) In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**.
The **Roles** table is displayed, listing the roles that match the search criteria and that can be children of another role.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - d) In the **Roles** table, select the check box next to the child role that you want to remove from the parent role, and then click **Remove**. Selecting the check box at the top of this column selects all child roles.
A confirmation page is displayed.
5. On the **Confirm** page, click **Submit**, or click **Cancel**.

Results

A **Success** page is displayed, indicating that you successfully removed the child roles from the parent role.

What to do next

You can continue working with roles, or click **Close**.

Creating an access type based on a role

You can create role-based access to resources.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

You can use the **Manage Access Types** page to create an access type.

To create an access type that is based on a role, complete these steps:

Procedure

1. From the navigation tree, select **Configure System > Manage Access Types**.
The **Manage Access Types** page is displayed.
2. On the **Manage Access Types** page, complete these steps:
 - a) In the **Access Types** tree, click the icon next to **Role**, and then click **Create Type**.
The **Create Access Type** page is displayed.
 - b) On the **Create Access Type** page, in the **Access type key** field, type a unique name for the access type key that you want to create.
 - c) Optional: In the **Description** field, type a description for the access type key that you want to create.
 - d) Click **OK**.

Results

The **Manage Access Types** page is displayed, and the new access type is listed in the **Access Types** tree.

What to do next

You might need to update the `CustomLabels.properties` resource bundle to provide the display label for this new access type.

You might make the new access available to users in the Self Service or the Identity Service Center user interface. To do so, associate the role with the newly created access type.

Transferring roles

As an administrator, you can transfer static and dynamic roles in an organization tree.

Before you begin

You can transfer static and dynamic roles to the business unit that is under the same organization root. Following are a few restrictions for role transfer activity:

- Roles cannot be transferred across different organization hierarchy.
- Static and dynamic roles cannot be transferred together.
- When dynamic roles are transferred, old entitlements might be lost. A user entitlements or membership is recomputed based on the new business unit under which the dynamic role is transferred.
- Roles to be transferred must contain an Access Control Item (ACI) granted for the Modify operation.

Procedure

1. From the navigation tree, select **Manage Roles**.
2. On the **Manage Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against role names or descriptions, or against business units, and then click **Search**.
3. In the **Roles** table, click the icon next to the role that you want to transfer, and then click **Transfer**.
4. Search and then select the business unit to which you want to transfer roles and then click **OK**.
5. On the **Confirmation** page, complete either of these steps:
 - For dynamic roles, select the schedule for transfer, and then click **Transfer**.
 - For static roles, review the selected roles to transfer and then click **Transfer**.

Results

A **Success** page is displayed, indicating that you successfully transferred the roles.

Enabling access for multiple roles

You can enable access for multiple roles.

Before you begin

Ensure that your system administrator grants you the ACI **Modify** at the operation level and the **Access Options** at the permission level in the ACI configuration. These ACI configurations apply to static and dynamic organizational roles.

About this task

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the IBM Security Identity Manager administrative console, click **Manage Roles**.
2. Click **Search** to filter or browse for the available roles.
3. Select the box for each role that you want to enable access.
4. Click **Enable Access**.

Access is not enabled, if the following occurs:

- The existing role is already enabled with access or enabled as common access.
- You have insufficient authorization to enable access on a selected role.

If any of your selected roles are valid, the configuration page for the role is displayed.

5. Optional: To enable the role as common access, select **Enable as common access**.
6. Select an access type.

The default access type for a role is **Role**. If **Role** is removed as an access type, the first access type is the default option.

7. Click **Enable**.

Review the messages to confirm that access is enabled successfully.

8. Click **Cancel** to return to the **Manage Roles** page.

What to do next

Return to the **Manage Roles** page to perform other operations.

Disabling access for multiple roles

You can disable access for multiple roles.

Before you begin

Ensure that your system administrator grants you the ACI **Modify** at the operation level and **Access Options** at the permission level in the ACI configuration. The ACI configurations are for static and dynamic organizational roles.

About this task

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the IBM Security Identity Manager administrative console, click **Manage Roles**.
2. Click **Search** to filter or browse for the available roles.
3. Select the box for each role that you want to disable access.
4. Click **Disable Access**.
5. Click **Disable**.

Review the messages to confirm that access is disabled successfully.

6. Click **Cancel** to return to the **Manage Roles** page.

What to do next

Return to the **Manage Roles** page to perform other operations.

Chapter 9. Services administration

A *service* represents a user repository for a resource, such as an operating system, a database application, or another application that Security Identity Manager manages. For example, a managed resource might be a Lotus Notes application, and a service can be defined for a Lotus Notes User Repository.

Overview

Services are created from service types, which represent a set of managed resources that share similar attributes. For example, there is a default service type that represents Linux systems. These service types are installed by default when IBM Security Identity Manager is installed. Service types are also installed when you import the service definition files for the adapters for those managed resources.

Most services provide an interface for provisioning of accounts to users, which usually involves some workflow processes that must be completed successfully. Users access these services by using an account on the service.

A *service owner* identifies the person who owns and maintains a particular service in IBM Security Identity Manager.

A user's profile is represented as an *account*.

Service administration tasks

Service administration tasks are done by using **Manage Services** from the navigation menu. Service administration tasks include the following tasks:

- Creating services and optionally creating provisioning policies for those services
- Changing or deleting services
- Scheduling an account reconciliation or initiating an immediate account reconciliation, including reconciling supporting data only. An immediate account reconciliation reconciles only the data you need for defining provisioning policies and access information for a group.
- Configuring policy enforcement on services, where you define the enforcement action when an account is noncompliant
- Viewing groups and defining access entitlements on groups
- Requesting accounts
- Displaying, changing, removing, suspending, and restoring accounts
- Assigning accounts to users
- Viewing account recertification status
- Displaying, creating, changing, and removing account defaults

Service prerequisite

A service might have another service defined as a service prerequisite. Users can receive a new account only if they have an existing account on the service prerequisite. For example, Service B has a service prerequisite of Service A. If a user requests an account on Service B, the user must first have an account on Service A to receive an account on Service B.

Service types

A *service type* is a category of related services that share schemas. It defines the schema attributes that are common across a set of similar managed resources.

Service types are profiles, or templates, that create services for specific instances of managed resources. For example, you might have several Lotus® Domino® servers that users need access to. Create one

service for each Lotus Domino server with the Lotus Domino service type. In previous versions of IBM Security Identity Manager, a service type is called a *service profile*.

Some service types are installed by default when Security Identity Manager is installed. Other service types can be installed when you import the service definition files for adapters for managed resources. A service type definition is provided by the Security Identity Manager adapter for a managed resource. There is a service type for each type of managed resource that Security Identity Manager supports. Some examples are UNIX, Linux, Windows, and IBM Security Access Manager.

A service type is defined in the service definition file of an adapter, which is a Java Archive (JAR) file that contains the profile. The service type for an adapter is created when the adapter profile (JAR file) is imported. For example, a service type is defined in the `WinLocalProfile.jar` file. You can also define a service type with the interface for Security Identity Manager.

Security Identity Manager supports the following types of service providers:

- DAML for Windows Local adapter, Lotus Notes adapter
- IDI (IBM Security Directory Integrator for UNIX and Linux adapters)
- Custom Java class for defining your own implementation of a service provider
- Manual for managing user-defined “manual” activities

Default service types

The following default service types are provided with Security Identity Manager:

Identity feed service types:

DSML

A Directory Services Markup Language (DSML) Identity Feed service imports user data, with no account data, from a human resources database or file. The service feeds the information into the Security Identity Manager directory. The service uses a placement rule to determine where in the organization a user is placed. The service can receive the information in one of two ways: a reconciliation or an event notification. This service is based on the DSML Identity Feed Service Profile.

Note: DSMLv2 is deprecated in Security Identity Manager Version 5.0 in favor of the remote method invocation (RMI)-based IDI adapter framework. The use of DSMLv2 continues to be supported in this release.

AD

The AD Identity Feed Service imports user data from Windows Active Directory. The `organizationalPerson` objects are fed into Security Identity Manager and add or update users to Security Identity Manager. The user profiles that are selected from this service must have an objectclass that is derived from the `organizationalPerson` class.

CSV

The CSV Identity Feed Service imports user data from a comma-separated value (CSV) file and adds or updates users to Security Identity Manager. A CSV file contains a set of records that are separated by a carriage return/line feed (CR/LF) pair (`\r\n`). Each record contains a set of fields that are separated by a comma. If the field contains either a comma or a CR/LF, the comma must be escaped with double quotation marks as the delimiter. The first record in the CSV source file defines the attributes that are provided in each of the following records. Attributes must be valid based on the class schema for the selected person profile for this service.

IDI Data Feed

The IDI Data Feed service type uses the Security Directory Integrator to import user data, with no account data, into Security Identity Manager and to manage accounts in the Security Identity Manager data store on external resources. This service is based on the IDI Data Feed Service Profile.

INetOrgPerson

The INetOrgPerson Identity Feed imports user data from the LDAP directory. The `inetOrgPerson` objects are loaded and add or update users in Security Identity Manager.

Account service types:

Security Directory Integrator-based

This service type can be optionally installed during the installation of Security Identity Manager. All of these services are Security Directory Integrator-based adapters; each is a specific service type. Security Directory Integrator is one type of service provider. There can be multiple service types that are defined for the same type of service provider.

ITIM Service

The ITIM service type is used to create accounts in the Security Identity Manager system and represents the Security Identity Manager itself. This type is a standard service with no configuration parameters. All users that need access to the Security Identity Manager system must be provisioned with an Security Identity Manager account.

Hosted Service

The Hosted Service type is used to create a service that is a proxy to the hosting service that is in the service provider organization.

The hosted service connects to the managed resource target through the hosting service indirectly. The configuration details of the hosting service are invisible and protected from administrators in the secondary organization where the Hosted Service is defined. Administrators can define policies for the hosted service, specifically, without affecting the hosting service.

The primary usage of a Hosted Service is to allow users in business partner organizations to have accounts and access to internal IT resources of an organization. A Hosted Service allows administrators in the secondary organization to define specific service policies for the user accounts.

Custom Java class

The custom Java class service type defines your own implementation of a service provider.

Manual service type

The Manual service type is used to create a manual service.

Service status

The IBM Security Identity Manager server tracks its ability to make remote connections and send provisioning requests to adapters on a per service basis. This ability is reflected in the Status for each service on the Manage Services panel. On this panel, you can also search for services with a specific status.

The value options in the **Status** list contain status values for each service:

All

Status values for all services.

Alive

Services that are functioning with no known issues.

Failed

Services that encountered a problem. For example: a connection test might fail, or a request was not completed on an endpoint because of a problem with making a remote connection.

Attempting recovery

Services that encountered a problem and for which the server is attempting to process a previously blocked request.

Locked

Services that are locked because a reconciliation process is running.

Unknown

Services that never attempted a connection test or received and processed a request.

Each status value other than **Alive** provides an icon that links to more detailed information about the state of the service. For example, if the server cannot complete a request due to a network or authentication problem, it marks the service as **Failed**. Until the service recovers from the **Failed** status, provisioning requests cannot be processed. The failing request and any additional account requests are blocked until

the problem with the service is corrected. Clicking the **Failed** icon retrieves details about the failure, including the time of the first failure, detailed reason for the failure, and number of blocked requests.

The system periodically checks **Failed** services and attempts to recover the blocked requests. If the problem with the service is corrected, blocked requests can be completed due to this periodic check. The default time interval for the periodic recovery check is 10 minutes.

Restarting of the blocked requests

Retry Blocked Requests provides an option to immediately restart the blocked requests from the Manage Services panel. This action tests a service to see whether the problem is corrected. If the test is successful, it restarts any blocked requests for a failed service. Failures are returned to the user interface so that all configuration problems with the service can be corrected.

When the recovery process is started for a service, the service is placed in **Attempting recovery** status until all blocked requests are restarted. During this time, new requests can proceed normally.

Provisioning requests can also be blocked during reconciliation with the locking feature enabled. In this case, the service status shows **Locked** until the reconciliation completes. At that time, the service status is updated to **Attempting recovery** until any blocked requests are processed. When all blocked requests are restarted, the service returns to the **Alive** status.

Retry Blocked Requests is controlled by a task in the view definitions defined in **Set System Security > Manage Views** in the IBM Security Identity Manager administrative console. To restart the blocked requests of a service immediately, select **Manage Services** from the IBM Security Identity Manager administrative console. From the **Services** table and under **Service Name**, click an arrow to the right of the service and select **Retry Blocked Requests**.

Creating services

Create an instance of a service from a service type, such as the Linux profile or another adapter profile that you installed.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can create a service in IBM Security Identity Manager, you must create a service type. Alternatively, use one of the service types that were automatically created when you installed the IBM Security Identity Manager Server. You can create a service type by importing the adapter profile. Alternatively, you can add new schema classes and attributes for the service to your LDAP directory. Before you can create a service for an adapter, the adapter must be installed, and the adapter profile must be created.

About this task

If you choose to create a provisioning policy as part of this task, the service is automatically added to the provisioning policy as an entitlement. In addition, a membership of “All” is defined for the provisioning policy. You can later edit the provisioning policy and change the membership after the service is created.

The service name and description that you provide for each service are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

To create a service instance, complete these steps:

Procedure

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create**.

- The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.
The **Business Unit** page is displayed.
 4. On the **Business Unit** page, complete these steps:
 - a) Type information about the business unit in the **Search information** field.
 - b) Select a business type from the **Search by** list, and then click **Search**.
A list of business units that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.
The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
 5. On the **Select the Type of Service** page, select a service type, and then click **Next**.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance.
The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.
 7. On the **Authentication** page, configure authentication (either password-based or key-based) for the service, and then click **Next** or **Finish**.
The **Authentication** page is displayed only if you are creating a POSIX service instance.
 8. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes, and then click **Next** or **OK**.
The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based services.
 9. Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable.
Specify the expected access information and any other optional information such as description, search terms, more information, or badges.
 10. On the **Status and Information** page, view information about the adapter and managed resource, and then click **Next** or **Finish**.
The adapter must be running to obtain the information.
 11. On the **Configure Policy** page, select a provisioning policy option, and then click **Next** or **Finish**.
The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.
Note: If you are creating a service for an identity feed, the **Configure Policy** page is not displayed.
 12. Optional: On the **Reconcile Supporting Data** page, either do an immediate reconciliation for the service, or schedule a supporting data reconciliation, and then click **Finish**.
The **Reconcile Supporting Data** page is displayed for all services except for identity feed services.
The **supporting data only** reconciliation option retrieves only the supporting data for accounts. The supporting data includes groups that are defined on the service. The type of supporting data is defined in the adapter guide.

13. Optional: On the **Service Information** or **General Information** page, click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

Results

A message is displayed, indicating that you successfully created the service instance for a specific service type.

What to do next

Select another services task, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table and display the new service instance.

Creating a service that has manual connection mode

If you did not install the adapter for the managed resource, use this task to create an instance of a service. You can use the manual connection mode to manage account requests instead of creating a manual service. After you install the adapter, you can change the connection mode from manual to automatic.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

To create a service in IBM Security Identity Manager, you must create a service type. Alternatively, use one of the service types that were automatically created when IBM Security Identity Manager Server was installed. To create a service type either:

- Import the adapter profile, or
- Add the new schema classes and attributes for the service to your LDAP directory

You must add the `exconnectionmode` attribute to the customized form for the service type to enable connection mode. See [“Enabling connection mode” on page 700](#).

About this task

This task is for creating a service with manual connection mode before the adapter is installed. After the adapter installation, to create a service with an automatic connection, select **Automatic** and follow the task for creating a service. See [“Creating services” on page 696](#).

If you choose to create a provisioning policy as part of this task, the service is automatically added to the provisioning policy as an entitlement. In addition, a membership of All is defined for the provisioning policy. You can later edit the provisioning policy and change the membership after the service is created.

The service name and description that you provide for each service are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

To create a service instance that has manual connection mode, complete these steps:

Procedure

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is opened.
2. On the **Select a Service** page, click **Create**.
The **Create a Service** wizard is opened.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.

- The **Business Unit** page is opened.
4. On the **Business Unit** page, complete these steps:
 - a) Type information about the business unit in the **Search information** field.
 - b) Select a business type from the **Search by** list, and then click **Search**.
A list of business units that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.
The **Select the Type of Service** page is opened, and the business unit that you specified is shown in the **Business unit** field.
 5. On the **Select the Type of Service** page, select a service type, and then click **Next**.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance. Then, click **Test Connection** to validate that the data in the fields is correct.
If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.
Note: The content of the **Service Information** or **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.
 7. For the **Connection mode** option, select **Manual**.
Selecting **Manual** enables the **Participants** page, the **Messages** page, and a different **Reconciliation** page in the navigation area.
Note: This option is available only if the `erconnectionmode` attribute is added to the service form. Connection mode is not supported on the ITIM Service or any type of identity feed service, hosted service, or manual service types. For information about adding the `erconnectionmode` attribute, see [“Enabling connection mode” on page 700](#).
 8. On the **Users and Groups** page, specify user and group information for the service.
Note: The **Users and Groups** page is opened only if you are creating certain service instances.
 9. On the **Authentication** page, configure authentication (either password-based or key-based) for the service, and then click **Next** or **Finish**.
Note: The **Authentication** page is displayed only if you are creating a POSIX service instance.
 10. Optional: On the **Dispatcher Attributes** page, specify information about the dispatcher attributes, and then click **Next** or **Finish**.
Note: The **Dispatcher Attributes** page is displayed only for Directory Integrator-based services.
 11. Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable.
Specify the expected access information and any other optional information such as description, search terms, more information, or badges.
 12. Optional: On the **Status and Information** page, you can view information about the adapter and managed resource, and then click **Next** or **Finish**.
 13. On the **Participants** page, specify the users who are involved in completing the activities for the manual service. Specify the amount of time before the service is escalated. Click **Next**.
 14. Optional: On the **Messages** page, complete these steps, and then click **Next** or **Finish**:
 - a) Select the default email message that you want to change, and then click **Change**.

The **Change Message** page is opened.

b) Modify the **Subject** and **Body** fields, and then click **OK**.

15. On the **Configure Policy** page, select a provisioning policy option, and then click **Next** or **Finish**.

The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only the Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.

Note: If you are creating a service for an identity feed, the **Configure Policy** page is not opened.

16. Optional: On the **Reconciliation** page, click **Browse** to locate the reconciliation file, and then click **Upload File** to load the new reconciliation file.

You can also choose whether to reconcile supporting data only.

Note: The file type that is supported for the reconciliation file is CSV. For more information, see [“Example comma-separated value \(CSV\) file”](#) on page 720.

Results

A message is shown, indicating that you successfully created the service instance for a specific service type.

What to do next

Select another services task, or click **Close**. When the **Select a Service** page is opened, click **Refresh** to refresh the **Services** table and display the new service instance.

Enabling connection mode

Use connection mode to create a service that can function like either an automated or a manual service.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Only individuals who are part of the administrator group can access this feature.

About this task

Before you install the adapter, use connection mode to create a service and to specify the account request route. The account route can be specified as either automatic or manual.

Automatic

Specifies to route account requests to a service provider. This selection is the default setting.

Manual

Specifies to route account requests to a specific user.

Note: Selecting Manual enables the Participants page and a different Reconciliation page in the navigation area of the Create a Service wizard.

The advantage of using connection mode is that you do not need to create and later remove a manual service. After installing the adapter, to change to an automated service, change the connection mode from manual to automated. See [“Changing connection mode from manual to automatic”](#) on page 704.

Note: Connection mode is not supported on ITIM service or any type of identity feed service, hosted service, or manual service types. Do not add the `erconnectionmode` attribute to the forms for those service types.

To enable connection mode, add the `erconnectionmode` attribute to the service form.

Procedure

1. From the navigation tree, click **Configure System > Design Forms**.
The form designer applet is displayed.
2. In the left pane, double-click the **Service** folder to display the profiles for the service types. Double-click the service type profile to open the template for that profile.
The form template associated with the service type profile is displayed in the middle pane.
3. Select the tab to which you want to add the attribute.
4. In the Attribute List pane, double-click **erconnectionmode**.
The attribute is added to the form.
5. Right click **erconnectionmode**. Click **Change To > Dropdown Box**.
6. Click **Custom Values**.
The Select Editor is displayed to design the drop-down menu.
7. Define the menu.
 - a) Under **Data Value** type AUTOMATIC.
 - b) Under **Display Value** type \$automatic.
 - c) Click the **Add Row** icon.
 - d) Under **Data Value** type MANUAL.
 - e) Under **Display Value** type \$manual.
 - f) Click **OK**.
8. Right click **erconnectionmode**. Click **Move Up Attribute** or **Move Down Attribute** to position the field on the form.
9. Click **Form > Save Form Template**, and then click **OK** when a message is displayed, indicating that the form template is saved successfully.
10. Click **Close** to exit Form Designer.

What to do next

Verify that connection mode was added to the service form.

1. Click **Manage Services > Create**.
2. Select the service type profile that you modified for connection mode. Click **Next**.
3. Verify that Connection mode is displayed on the form.

Creating manual services

Create a manual service instance when IBM Security Identity Manager does not provide an adapter for the managed resource.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can create a manual service in Security Identity Manager, you must create a service type. Add new schema classes and attributes for the manual service to your LDAP directory.

About this task

A manual service is a type of service that requires manual intervention to complete the request. For example, a manual service might be defined for setting up voice mail for a user. A manual service generates a work order activity that defines the manual intervention that is required.

If you choose to create a provisioning policy as part of this task, the service is automatically added to the provisioning policy as an entitlement. In addition, a membership of "All" is defined for the provisioning policy. Also, an ownership type of "Individual" is defined for the provisioning policy. You can later edit the provisioning policy and change the membership and ownership types after the service is created.

The service name and description that you provide for each service are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

To create a manual service instance, complete these steps:

Procedure

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create**.
The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.
The **Business Unit** page is displayed.
4. On the **Business Unit** page, complete these steps:
 - a) Type information about the business unit in the **Search information** field.
 - b) Select a business type from the **Search by** list, and then click **Search**.
A list of business units that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.
The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
5. On the **Select the Type of Service** page, select a manual service type, and then click **Next**.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
6. On the **General Information** page, specify the appropriate values for the manual service instance, and then click **Next**.
The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require additional steps.
7. On the **Participants** page, specify the users who are involved in completing the activities for the manual service. Specify the amount of time before the service is escalated. Click **Next**.
8. Optional: On the **Messages** page, complete these steps, and then click **Reconciliation**:
 - a) Select the default email message that you want to change, and then click **Change**.
The **Change Message** page is displayed.
 - b) Modify the **Subject** and **Body** fields, and then click **OK**.
9. Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable.
Specify the expected access information and any other optional information such as description, search terms, more information, or badges.
10. On the **Configure Policy** page, select a provisioning policy option, and then click **Next** or **Finish**.

The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.

11. Optional: On the **Reconciliation** page, click **Browse** to locate the reconciliation file, and then click **Upload File** to load the new reconciliation file.

You can also choose whether to reconcile supporting data only.

Note: The file type that is supported for the reconciliation file is CSV. For more information, see the topic "Example comma-separated value (CSV) file" in the *IBM Security Identity Manager Administration Guide*.

12. Click **Finish**.

Results

A message is displayed, indicating that you successfully created the manual service instance for a specific service type.

What to do next

Select another services task, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table and display the new service instance.

Changing services

You can change the information for a service instance.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can change a service in IBM Security Identity Manager, you must create a service instance.

Procedure

To change a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, select the check box next to the service that you want to change, and then click **Change**.
4. On the **Service Information** or **General Information** page, change the appropriate values for the service instance, and then click **OK**.

5. On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable. Clearing the check box disables these fields.

Change any access information or any other optional information such as description, search terms, more information, or badges.

Results

A message is displayed, indicating that you successfully changed the service instance.

What to do next

Select another services task, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Changing connection mode from manual to automatic

After installing the adapter, you can automate the routing of account requests to the managed resource.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can change a service, you must create the service instance with connection mode. The corresponding adapter for the managed resource must also be installed. For more information about enabling connection mode and creating a service with connection mode, see these topics:

- [“Enabling connection mode” on page 700](#)
- [“Creating a service that has manual connection mode” on page 698](#)

About this task

Use connection mode to change the account request routing from manual to automatic. You do not have to delete a manual service or create a service for the adapter.

Note: If you have pending work orders prior to switching the connection mode, a popup message reminds you. Use the **View Activities** option to resolve requests that are already in the activity list. After the switch to automatic, complete reconciliation to sync with the end point. Alternately, use the **View Requests by Service** option to cancel any current requests on the service. You can resolve the requests either before or after changing to automatic connection mode. After the change to automatic connection mode, the managed resource handles all new account requests.

Procedure

To change the connection mode for a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, select the check box next to the service that you want to change, and then click **Change**.
 4. On the **Service Information** or **General Information** page, change the connection mode from manual to automatic. Then click **Test Connection** to validate that the data in the fields is correct.
If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.
Note: The content of the **Service Information** or **General Information** page depends on the type of service that you are changing.
 5. Change any other appropriate values for the service instance, and then click **OK**.

Results

A message is displayed, indicating that you successfully changed the service instance. The managed resource handles all account requests.

What to do next

Select another services task, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Changing a manual service

Change information for a manual service instance.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can change a service in IBM Security Identity Manager, you must create a service instance.

Procedure

To change a manual service instance, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether the search must be done against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, select the check box next to the manual service that you want to change, and then click **Change**.
4. On the **General Information** page, change the appropriate values for the service instance, and then click **Participants**.

5. On the **Participants** page, change the participants type, escalation time in days, or escalation participant type.
6. Optional: On the **Messages** page, complete these steps, and then click **Reconciliation**:
 - a) Select the email message that you want to change, and then click **Change**.
The **Change Message** page is displayed.
 - b) Modify the **Subject** and **Body** fields as wanted, and then click **OK**.
7. Optional: On the **Reconciliation** page, click **Browse** to locate the reconciliation file, and then click **Upload File** to load the new reconciliation file.
You can also choose whether to reconcile supporting data only.
Note: The file type supported for the reconciliation file is CSV. For more information, see the topic "Example comma-separated value (CSV) file" in the *IBM Security Identity Manager Planning Guide*.
8. Click **OK** to save the changes and to close the page.

Results

A message is displayed, indicating that you successfully changed the service instance.

What to do next

Select another services task, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Values and formats for CSV access data (service)

A service access CSV file can contain multiple values and supported formats.

Consider these points before you work with any CSV files for a service access:

- If you use a custom label for AccessType, specify the key in the CSV file.
- If you use a custom label for badge text, add a \$ prefix on the key. For example, \$mail.
- Define multiple values for search terms and badges with a semicolon (;) separator.
- Define the AccessType hierarchy with a colon (:) separator.
- Use the badgeText~badgeStyle format for badges.

Define CSV columns for a service, group, or a role access as follows:

Field name	Value
SERVICE_DN, SERVICE_NAME	Not modifiable.
DEFINE_AS_ACCESS	TRUE or FALSE. If you do not assign any value, then FALSE is assumed.
ACCESS_NAME	Required for services and groups, and contains a maximum length of 240 characters. This field is not available for roles.
ACCESS_TYPE	Required. You must specify an access type that is defined in IBM Security Identity Manager.
ACCESS_DESCRIPTION	Contains a maximum length of 240 characters.
ICON_URL	Provide a valid icon URL value on the access definition.
SEARCH_TERMS	Each search term contains a maximum length of 80 characters. You can have multiple search terms.
ADDITIONAL_INFORMATION	Contains a maximum length of 1024 characters.
BADGES	The maximum length for each badge text is 512 characters. You can have multiple badges. The badge text that is prefixed with a \$ sign cannot contain delimiter characters such as ., ;, =, or white space.

A service access CSV file for an export or import operation in the IBM Security Identity Manager administration console contains these columns with sample values and supported formats:

SERVICE_NAME	DEFINE_AS_ACCESS	ACCESS_NAME	ACCESS_TYPE	ACCESS_DESCRIPTION	ICON_URL
admin	TRUE	Access	Application:Finance	This access is for the admin service.	/itim/ui/custom/ui/images/homepage/RequestAccess.png

Table 18. Part 1 of 2: Service access CSV file values, formats (continued)

SERVICE_NAME	DEFINE_AS_ACCESS	ACCESS_NAME	ACCESS TYPE	ACCESS_DESCRIPTION	ICON_URL
AIX Service	FALSE	AIX Service	Application:Finance:Payroll	This access is for the AIX Service.	http://www-03.ibm.com/ibm/history/exhibits/logo/images/920911.jpg
Default Service	TRUE	default access	MailService	This access is a default service access.	http://www-03.ibm.com/ibm/history/exhibits/logo/images/920911.jpg

Table 19. Part 2 of 2: Service access CSV file values, formats

SERVICE_NAME	SEARCH_TERMS	ADDITIONAL_INFORMATION	BADGES	SERVICE_DN
admin	Service Access; Manager	Service that is used by a client user.	admin~green	erglobalid=5628670506891199803,ou=services,erglobalid=000000
AIX Service	Employee;Service;AccessService	Used by the customer to deploy server.	\$roleaccess~red	erglobalid=5628669752130902869,ou=services,erglobalid=000000
Default Service	Mail;Unique ID	BVT server that is used to run BVT from developer and tester.	\$mail~green;Risky~red	erglobalid=5628670337030215245,ou=services,erglobalid=000000

Exporting access data for a service

Export the access data for a service in a comma-separated value (CSV) file format by using the IBM Security Identity Manager Console.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you export a service, you must have ACI privileges for **Modify Operation** on the service that you want to view. If the necessary privileges do not exist, then the service is not exported.

The **Export Access Data** button is not active until you select some service accesses to activate it. Only the service access that you selected is exported as access data.

About this task

Export the selected service access data in a CSV file format for your requirements.

Procedure

1. From the navigation tree, select **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, in the **Services** table, click **Export Access Data**.
The **Export access data** page is displayed. After you submit the export request, a process status indicates the advancement of the export operation.
3. Optional: Click **Cancel** to discontinue the export operation.
4. Click **Download Exported File** to download the CSV file on your local system by using your web browser settings.
The exported CSV file contains all the service access data.

Note: Click **Download Export Log File** to view any error or log information about the export operation. This button is displayed only if the submitted export operation contains any log information or encountered any errors.

Results

The exported CSV file contains all the access data for a service. Click **Close** to exit from the **Export access data** page.

What to do next

Import access data for a service, or you can continue to export access data by clicking **Export Access Data** in the **Select a Service** page.

Importing access data for a service

Use the IBM Security Identity Manager Console to import the service access data from a comma-separated value (CSV) file.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

The privileged user that uploads the CSV file must have the appropriate permissions.

Before you import a service, you must have ACI privileges for Search Operation and Modify Operation on the service that you want to update. If the necessary privileges do not exist, then the service is not imported.

Before you import a CSV file, verify that the CSV-related conventions are met. They are as follows:

- The access type hierarchy is represented in the following format, and each access type be separated by a colon (:). For example:

```
AccessType1:AccessType2
```

- The badge information is provided in the following format. For example:

```
badgeText~badgeStyle
```

- Multiple badges can be assigned to accesses in the following format, and each badge must be separated by a semicolon (;). For example:

```
Badge1~red;Badge2~green
```

- Multiple search terms and access types can be specified by using the semicolon (;) separator.
- The relevant keys must be provided in the CSV file for the customized labels that are related to badges and access types.

About this task

Only the accesses with the **Define as Access** set to `True` are defined as accesses, and the corresponding data is imported.

Procedure

1. From the navigation tree, select **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, in the **Services** table, click **Import Access Data**.
The **Import access data** page is displayed.
3. Click **Browse** in **File to Upload (.CSV)** to locate and upload a valid CSV file that contains all the access data for a service.
4. Click **Import** to import the CSV file.

After you submit the import request, a process status indicates the advancement of the import operation.

Note: If you click **Import** with an invalid file format, a message is displayed to inform you that the file format is not valid.

If any problems occur when you are importing a CSV file, then close the **Import access data** page to continue working with the IBM Security Identity Manager Console. The problems might be due to one of the following conditions:

- The access data CSV file does not exist.
- The CSV file was renamed.
- The CSV file does not contain appropriate separators or delimiters.

5. Optional: Click **Cancel** to discontinue the import operation.

Note: Click **Download Import Log File** to view any error or log information about the import operation. This button is displayed only if the submitted import operation contains any log information or encountered any errors.

Results

The imported CSV file contains all the access data for a service. Click **Close** to exit from the **Import access data** page.

What to do next

Export access data for a service, or you can continue to import access data by clicking **Import Access Data** in the **Select a Service** page.

Configuring access catalog information for a service

Configure the access catalog information for a service in the Administrator Console so you can use it in the Identity Service Center Request Access workflow.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must create a service type before you can configure the access catalog information for a service in IBM Security Identity Manager.

You can also configure the access catalog information for an existing service.

About this task

Configure the access information for a service by defining certain accesses with the use of a badge. You can highlight certain accesses with badges by attaching text that contains some formatting such as color and font type.

Procedure

To configure the service access information, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create** to display the **Create a Service** wizard.
Alternatively, select an existing service and click **Change** to configure its access catalog information.
3. Specify appropriate values in the corresponding tabbed pages.
4. On the **Access Information** page, complete these steps to configure the access information:
 - a) Select the **Define an Access** check box to activate the access definition fields.
 - b) Specify an appropriate name in the **Access name** field.
 - c) Expand the **Select access type** or the **Change access type** tree to select an access type.

- The tree label depends on whether you want to create or modify a service.
- d) Provide a uniform resource identifier (URI) string in the **Icon URL** field for the access icon.
 - e) Specify search strings in the **Search terms** field to return specific search terms.
Add or delete the search terms to suit your requirements.
 - f) Specify any free form information about the access item in the **Additional information** field.
 - g) Expand the **Badges** section to specify the badges that are associated with the role.
 - Specify a badge text in the **Badge text** field.
 - Assign a class from the **Badge class** list for the badge text.
- You can see the preview of your badge specifications in the **Preview** area.
5. Depending on whether you created or modified the service access information, click **OK** or **Finish** when you are done.

Results

The access information is added or updated to the service object and stored in the Security Identity Manager LDAP server.

What to do next

On the **Success** page, click **Close**. Select another services task, or click **Close**.

Deleting services

Delete service instances when necessary. For example, you might delete a service instance for an obsolete application.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can delete a service in IBM Security Identity Manager, a service instance must exist.

Procedure

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, select the check box next to the service that you want to remove, and then click **Delete**.
Selecting the check box at the top of this column selects all service instances.
A confirmation page is displayed.
4. On the **Confirm** page, click **Delete** to remove the selected service instance, or click **Cancel**.

The services are removed automatically from all provisioning policies, identity policies, password policies, adoption policies, and recertification policies that currently reference them. If all services referenced by a policy are deleted by this operation, the entire policy is also deleted. All accounts that are related to that service are also deleted from Security Identity Manager. However, they are not de-provisioned from the managed resource.

Results

A message indicates that you successfully deleted the service instance.

What to do next

Select another services task, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Management of reconciliation schedules

Reconciliation is the process of synchronizing the accounts and supporting data to the IBM Security Identity Manager Server central data repository from a managed resource. Reconciliation is required when accounts and supporting data can be changed on the managed resource so that IBM Security Identity Manager Server data is consistent and up-to-date with the remote resource.

During the reconciliation process, new accounts created on the managed resource will be created in the IBM Security Identity Manager Server repository and assigned to the user based on the adoption policy that is applicable for the service. If there is no user match for the account, the account will be displayed in IBM Security Identity Manager Server as an orphan account that can be manually assigned to a user by a IBM Security Identity Manager Server administrator. Modified accounts on the managed resource will be updated to the IBM Security Identity Manager Server repository. Removed accounts on the managed resource are also removed from IBM Security Identity Manager Server.

You can manage schedules for reconciliation, or initiate a reconciliation activity immediately. To determine an ownership relationship, reconciliation compares account information with existing user data stored on the IBM Security Identity Manager Server by first looking for the existing ownership within the IBM Security Identity Manager Server and, secondly, applying adoption rules configured for the reconciliation.

If there is a match of user login IDs to an account, the IBM Security Identity Manager Server creates the ownership relationship between the account and the person. The IBM Security Identity Manager Server also verifies that the accounts fit within the constraints of a defined policy. If there is not a match, the IBM Security Identity Manager Server lists the unmatched accounts as orphaned accounts.

You run reconciliation to perform the following tasks:

- Load accounts and account supporting data information, including groups, into IBM Security Identity Manager

Promptly after IBM Security Identity Manager is installed, you should submit reconciliation requests for all resources whose accounts are managed by IBM Security Identity Manager. Reconciliation inserts accounts from the managed resources into the IBM Security Identity Manager directory.

- Monitor accesses granted outside of IBM Security Identity Manager

During reconciliation, records of all accesses granted outside of IBM Security Identity Manager are inserted into the IBM Security Identity Manager directory. You can view these records by user after your data is reconciled.

Reconciliation allows you to enable policy checking. In this case, you should reconcile your data on a scheduled basis for your organization's ongoing security audits.

Managed service accounts can be excluded from reconciliation on the IBM Security Identity Manager Server and, for some adapters, on the managed service itself. If you filter accounts from reconciliation at the adapter and do not also filter them when you define your server-side scheduled or immediate reconciliations, the server will consider the reconciliation a "full" reconciliation for all accounts and will

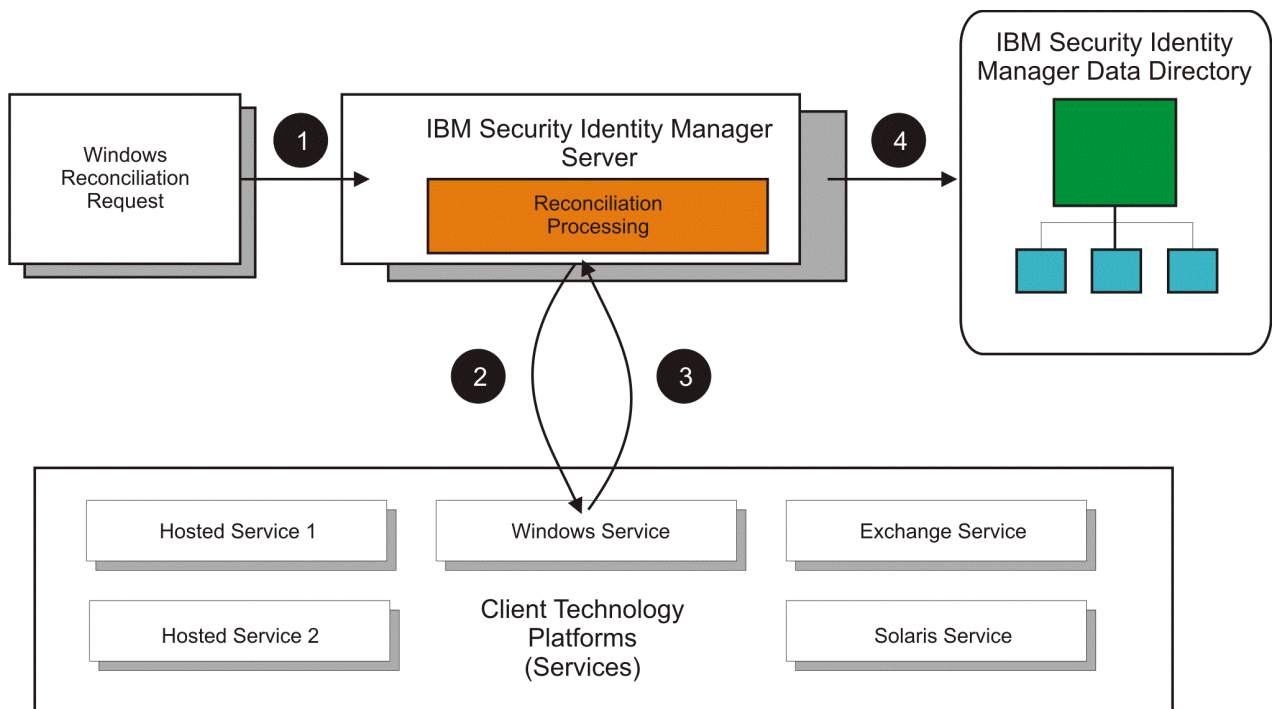
remove any accounts from its directory that it does not receive during the reconciliation (because it will appear to the server that they have been removed from the managed resource).

Consider the following best practices for using reconciliation:

- Perform supporting data reconciliation separately from accounts. The separation is useful during initial deployment for the service and also useful for sync up changes of metadata without accounts, which is very time-consuming. Supporting data includes group configuration information, which contains key information about access privileges on the resource. Bringing back the group data ahead of time allows policies to be configured promptly before accounts are reconciled, so that the policies can be enforced.
- Set up reconciliation schedules appropriately based on the frequency of data changes. Leave enough time between two reconciliations. Avoid unnecessary reconciliations.
- Queries are used to break reconciliation into smaller packets. Reconcile only the data that is changed by using Query. Reconciliation is an expensive process, especially when policy checking is enabled.
- If you are working with a large data repository (that is, a large number of accounts), consider using Query to segment the data and perform the reconciliation in smaller chunks on different schedules.
- Specify a subset of account attributes to bring back to improve performance.

Overview of the reconciliation process

The following illustration is an overview of the reconciliation process. In this example, IBM Security Identity Manager reconciles Windows Server data.



The numbered steps in the table below correspond to the illustration.

Step	Description
1	An administrator submits a reconciliation request to a system whose security is managed by IBM Security Identity Manager.
2	The IBM Security Identity Manager Server sends the reconciliation request to the selected service.
3	The service collects information from the system and sends the information to the IBM Security Identity Manager Server.

Step	Description
4	The IBM Security Identity Manager Server reads the information and reconciles the IBM Security Identity Manager directory with account information from the service.
5	The IBM Security Identity Manager Server attempts to find the account owner.
6	If an owner is found, the changes to the account are evaluated against a provisioning policy.
7	The account is modified according to configured policy enforcement options.

Maximum duration setting on reconciliation schedule

The reconciliation timeout, or 'Maximum duration' setting that you configure when you set up a reconciliation schedule is not honored under certain conditions.

The following prerequisites are assumed:

- The dispatcher or adapter is running for the entire duration of the reconciliation process.
- The resource is running for the entire duration of the reconciliation process.

When the reconciliation process (either manual or scheduled) starts on IBM Security Identity Manager, the following sequence of activities occurs on IBM Security Identity Manager server and on the dispatcher or adapter.

1. IBM Security Identity Manager sends a request to the dispatcher/adapter to start the reconciliation operation and waits for the dispatcher to return the first batch of entries.
2. Depending on the batch size property, that is specified on the dispatcher, the dispatcher or adapter prepares a batch of entries, and returns that batch to IBM Security Identity Manager Server for processing.
3. After the first batches of entries are processed on IBM Security Identity Manager server, IBM Security Identity Manager sends a request to the dispatcher to send the next batch of entries. This process continues until all the entries are reconciled and processed by IBM Security Identity Manager or an exception that is causing the process to end.

If the reconciliation process runs for more than the configured time duration (“Maximum duration”), then IBM Security Identity Manager server attempts to stop the reconciliation, after the maximum duration time elapses. Following are the two conditions where the behavior of IBM Security Identity Manager differs when the maximum duration is reached.

Note: The behavior of IBM Security Identity Manager that is described in the following section is for Security Directory Integrator-based adapters only. For ADK/DAML based adapters, IBM Security Identity Manager always honors the “Maximum Duration” that is specified in the reconciliation schedule. After the reconciliation process runs for more than the “Maximum duration” time, IBM Security Identity Manager closes the search request and stops the reconciliation request at its end.

Maximum duration time elapses when the following conditions occur:

- [“Condition 1: IBM Security Identity Manager waits to receive the first batch of entries from dispatcher or adapter” on page 713](#)
- [“Condition 2: IBM Security Identity Manager is waiting on or processing the entries from the dispatcher or adapter that are not the first batch” on page 714](#)

Condition 1: IBM Security Identity Manager waits to receive the first batch of entries from dispatcher or adapter

This condition might arise when the following events occur:

- The request hangs on the dispatcher or adapter after it receives a search request from IBM Security Identity Manager and before it might respond back to IBM Security Identity Manager with the first batch of entries. IBM Security Identity Manager keeps on waiting for the response.

- A high value is specified for the batch size on the Security Directory Integrator-based dispatcher and the resource is slow. In this situation, the time that is taken by the dispatcher/adaptor to accumulate the first batch of entries might exceed the maximum duration time that is specified on the IBM Security Identity Manager server for the reconciliation process. IBM Security Identity Manager server keeps on waiting for the initial response.

In these situations, IBM Security Identity Manager does not stop the reconciliation request even if the reconciliation time exceeds the “Maximum Duration” value. IBM Security Identity Manager waits for the dispatcher to return the first batch of entries and then checks the “Maximum duration” value that is specified in reconciliation schedule. If the “Maximum Duration” is elapsed, IBM Security Identity Manager does not process the entries that are returned by dispatcher.

IBM Security Identity Manager then sends a “Search Close” request to dispatcher/adaptor to end the Search operation. If the dispatcher/adaptor hangs, then the reconciliation operation in IBM Security Identity Manager hangs forever and user must manually stop the operation from the IBM Security Identity Manager console.

Condition 2: IBM Security Identity Manager is waiting on or processing the entries from the dispatcher or adaptor that are not the first batch

This condition might arise when the following events occur:

- The request hangs on the dispatcher/adaptor after one or more batches of entries are sent to IBM Security Identity Manager in response to a search request. IBM Security Identity Manager waits for the subsequent batch of entries. Meanwhile the maximum reconciliation duration is reached on the IBM Security Identity Manager server.
- A high value is specified for the batch size on the dispatcher and the resource is slow. In this situation, the time that is taken by the dispatcher to accumulate the next batch of entries might be substantially more. IBM Security Identity Manager waits for the subsequent batch of entries. Meanwhile the maximum reconciliation duration is reached on the IBM Security Identity Manager server.
- The number of entries to be processed are substantially large on the resource and the “Maximum duration” is set to a considerably low value. The maximum reconciliation duration is reached when the reconciliation process is in progress.

In these situations, IBM Security Identity Manager honors the “Maximum Duration” value that is set on the reconciliation schedule. After the reconciliation process runs for more than the “Maximum duration” time, IBM Security Identity Manager sends a “Search Close” request to the dispatcher or adaptor. After the dispatcher or adaptor sends back the response that it closed the search request, IBM Security Identity Manager stop the reconciliation request at its end.

Reconciling accounts immediately on a service

You can initiate a reconciliation activity immediately on a service, rather than scheduling the reconciliation.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you begin this task, you must create a service instance.

To prevent the reconciliation from running again at the scheduled time, change or delete the scheduled reconciliation.

Procedure


To run a reconciliation now, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.

2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Reconcile Now**.

The tasks that you can perform are dependent on the type of service.

The **Select Query** page is displayed.
4. Select one of the following options:
 - **None**. Select this option to include all accounts in the reconciliation.
 - **Use query from existing schedule**. Select this option to view and select reconciliation from an existing schedule.
 - **Define query**. Select this option if you want to allow the reconciliation to filter accounts that fit the selected attributes, or if you want to perform a “supporting data only” reconciliation.
5. Click **Submit** to request an immediate reconciliation activity.

Results

A message is displayed, indicating that you successfully submitted a reconciliation request to run immediately.

What to do next

To view the results of the reconciliation, click **View the status of the reconciliation request**, or click **Close**.

Creating a reconciliation schedule

You can schedule a reconciliation for account and attribute data, or you can schedule a reconciliation only for supporting data from the managed service.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.


Before you begin this task, you must create a service instance.

Procedure

To create a reconciliation schedule, complete these steps:

1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.

- c) Select a service type from the **Search type** list.
- d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Set Up Reconciliation**.
The tasks that you can do are dependent on the type of service.
The **Manage Schedules** page is displayed.
4. On the **Manage Schedules** page, complete the following steps:
 - a) Specify whether a policy evaluates the accounts that the reconciliation returns.
 - b) Click **Create**.
The **Set Up Account Reconciliation** notebook is displayed.
5. On the **General** page, type information about reconciliation schedule.
6. On the **Schedule** page, select a schedule interval for the reconciliation.
The fields displayed depend on the scheduling option that you select.
7. Optional: On the **Query** page, specify that you are doing a "supporting data only" reconciliation, which brings back only metadata for accounts and excludes accounts. Alternatively, use the LDAP filter to specify the subset of accounts or specific type of support data such as a group to be included in the reconciliation. Specify the subset of account attributes to bring back during the reconciliation.
By default, IBM Security Identity Manager brings back all attributes of accounts. By specifying the subset of attributes that is likely to be changed on the remote resource, you can improve reconciliation performance.
8. Click **OK** to save the new schedule and close the page.

Results

A message is displayed, indicating that you successfully created a reconciliation schedule.

What to do next

Select another services task, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Changing a reconciliation schedule

After you create a reconciliation schedule, you can change it if necessary.

Before you begin


Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

A reconciliation schedule must exist.

Procedure

To change a reconciliation schedule, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:

- a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Set Up Reconciliation**.
The tasks that you can do are dependent on the type of service.
The **Manage Schedules** page is displayed.
4. On the **Manage Schedules** page, complete the following steps:
 - a) Specify whether a policy evaluates the accounts that the reconciliation returns.
 - b) On the **Manage Schedules** page, select the check box next to the reconciliation schedule that you want to modify, and then click **Change**.
The **Set Up Account Reconciliation** notebook is displayed.
5. Make the wanted changes on the **General**, **Schedule**, and **Query** pages, and then click **OK**.

Results

A message is displayed, indicating that you successfully updated an existing reconciliation schedule.

What to do next

Select another services task, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Deleting a reconciliation schedule

After you create a reconciliation schedule, you can delete it if necessary.

Before you begin


Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

A reconciliation schedule must exist.

Procedure

To delete a reconciliation schedule, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Set Up Reconciliation**.
The tasks that you can do are dependent on the type of service.
The **Manage Schedules** page is displayed.
 4. On the **Manage Schedules** page, select the check box next to the reconciliation schedule that you want to delete. Selecting the check box at the top of this column selects all reconciliation schedules.
 5. Click **Delete**
A confirmation page is displayed.
 6. On the **Confirm** page, click **Delete** to delete the selected reconciliation schedule, or click **Cancel**.

Results

A message is displayed, indicating that you successfully removed the reconciliation schedule.

What to do next

Select another services task, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Configuring a manual service type to support groups

To support group assignment, but not group management for manual services, the group profile needs to be set up in the manual service type configuration.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To set up a manual service type to support group assignment, but not group management (which includes create, read, update, delete) for manual services, complete these steps:

Procedure

1. Define the group schema as an LDAP objectclass in the IBM Security Identity Manager LDAP server.
2. Define a manual service (complete with service and account objectclasses).

The account objectclass should contain an optional multi-valued attribute that will be used to store the group membership information. This service type should reference the group schema created in the previous step.

The **Manage Service Types** page allows the administrator to select an existing LDAP objectclass for use as the group schema class. If you want to create a new objectclass, you must create it manually and load it directly into the LDAP server.

The mapped **Group ID**, **Group name**, and **Group description** attributes can all reference the same group schema attribute, if desired. You cannot define multiple groups that use the same group ID. The ID must be unique per group.

More than one group schema can be defined for a given service type. The definition of the second and subsequent schemas is performed in the same manner as the first.

3. Modify service and account forms for the service type using the form designer.

This step is required to properly display needed information when creating the service instance as well as creating accounts.

4. Create a manual service instance using the manual service type that you created earlier in this process.

Reconciling accounts immediately on a service

You can initiate a reconciliation activity immediately on a service, rather than scheduling the reconciliation.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you begin this task, you must create a service instance.

To prevent the reconciliation from running again at the scheduled time, change or delete the scheduled reconciliation.

Procedure

To run a reconciliation now, complete these steps:

1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.


2. On the **Select a Service** page, complete these steps:

- a) Type information about the service in the **Search information** field.
- b) In the **Search by** field, specify whether to search against services or business units.
- c) Select a service type from the **Search type** list.
- d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Reconcile Now**.

The tasks that you can perform are dependent on the type of service.

The **Select Query** page is displayed.

4. Select one of the following options:

- **None**. Select this option to include all accounts in the reconciliation.
- **Use query from existing schedule**. Select this option to view and select reconciliation from an existing schedule.
- **Define query**. Select this option if you want to allow the reconciliation to filter accounts that fit the selected attributes, or if you want to perform a “supporting data only” reconciliation.

5. Click **Submit** to request an immediate reconciliation activity.

Results

A message is displayed, indicating that you successfully submitted a reconciliation request to run immediately.

What to do next

To view the results of the reconciliation, click **View the status of the reconciliation request**, or click **Close**.

Example comma-separated value (CSV) file

Create a CSV file for reconciliation of the manual service instance. The CSV file contains both accounts and group definitions that exist on the manual service.

Using a CSV file for reconciliation of a manual service

Here is an example CSV file that contains both account and group information:

```
eruid,description
batman,uses technology
superman,flies through the air
spiderman,uses a web
ghost rider, rides a motorcycle
#GROUP_OBJECT_PROFILE#accessgroupGroupProfile
cn,description
daredevil,this group represents daredevils
superhero,this group represents superheroes
```

The example file creates two groups for this service instance: `daredevil` and `superhero`. Because `cn` is used for both the `id` and `name` attributes in the group schema, list it only one time in the CSV file. The example file also creates four accounts for this service instance: `batman`, `superman`, `spiderman`, and `ghost rider`.

Format of the example CSV file

A CSV file contains a set of records separated by a carriage return/line feed (CR/LF) pair (`\r\n`), or by a line feed (LF) character. Each record contains a set of fields separated by a comma. If the field contains either a comma or a CR/LF, the comma must be escaped with double quotation marks as the delimiter.

The first line of the example CSV file contains the attribute header list for accounts. The list contains the attributes that are defined in the accounts section of the service type definition. Be sure to include any required attributes in this line, or else the reconciliation fails.

The next set of lines (up until the `#GROUP_OBJECT_PROFILE#` line) represents the accounts that are to be loaded into IBM Security Identity Manager. Each line represents one account. The content of these rows is the values to apply to the attributes defined in the first row. All required attributes must have a value, or else the reconciliation of that account fails.

The line that starts with `#GROUP_OBJECT_PROFILE#` is a line that delineates the start of a new group schema (as defined in the **Manage Service Types** task). The string immediately after `#GROUP_OBJECT_PROFILE#` is the name of the group schema as stored in IBM Security Identity Manager. The value is always `objectclassGroupProfile`. In the example file, the `accessgroup` objectclass is used for the group schema, so the value for this line is `accessgroupGroupProfile`. If this line does not reference an existing group profile in IBM Security Identity Manager, the reconciliation fails.

The line immediately following the `#GROUP_OBJECT_PROFILE#` line is the group header line that lists the attributes of the group that is defined on the previous line. This line should contain the three attributes defined on the **Groups** page of the **Manage Service Types** task.

Following the example, the values are the group id, group name, and group description: `cn, cn, description`. If these attributes do not exist in the group profile, the reconciliation fails. Include any attribute that exists in the group schema objectclass that you defined, but only the group name and group description appear in the IBM Security Identity Manager interface.

The next group of lines represents individual groups of the group schema type. Each line represents one group. The values listed on this line correspond to the attribute list on the line immediately following the `#GROUP_OBJECT_PROFILE#` line. If the values on this line are not valid, then the creation of that group in IBM Security Identity Manager fails when the reconciliation is done.

Example CSV file for loading two types of group profiles

More than one type of group can be loaded by using the reconciliation file. To do so, repeat the `#GROUP_OBJECT_PROFILE#` line in the CSV file. Here is an example that loads two types of group profiles:

```
eruid,description
batman,uses technology
superman,flies through the air
spiderman,uses a web
ghostrider, rides a motorcycle
#GROUP_OBJECT_PROFILE#accessgroupGroupProfile
cn,description
daredevil,this group represents daredevils
superhero,this group represents superheroes
#GROUP_OBJECT_PROFILE#aixaccessgroupGroupProfile
aixgroupadminlist,ibm-aixprojectnamelist,ergroupdescription
eadmins,eadmingroup,admins on ephone
eguests,eguestgroup,guests on ephone
```

The two group schemas used in this example are `accessgroup` and `aixaccessgroup`. For the reconciliation to work, both group schemas must be defined on the service type.

Reconciling supporting data only

When you do the reconciliation, you can select a check box for *supporting data only*. If you select the check box, the reconciliation ignores the account information and processes only the group information. If you do not select the check box, both account and group information is processed. The CSV file can contain both accounts and groups, groups only, or accounts only. The reconciliation ignores missing data.

Management of accounts on a service

An *account* is an entity that contains a set of parameters that define the application-specific attributes of a user, including the identity, user profile, and credentials.

An account defines your login information, such as your user ID and password, and your access to the specific resource with which it is associated.

In IBM Security Identity Manager, accounts are created on account types. The types represent the managed resources such as operating systems (such as UNIX), applications (for example, Lotus Notes), or other resources. An account type is defined as part of the service type for the managed resource. The account type contains the account profile object that describes the schema of an account and mapping of account attributes to IBM Security Identity Manager-managed account attributes.

Accounts are either active or inactive. Accounts must be active to log in to the system. An account becomes inactive when it is suspended or if a request to recertify your account usage is declined and the recertification action is suspend. Suspended accounts still exist, but they cannot be used to access the system.

If one of your accounts is inactive and you require access to the system, contact your system administrator to restore the account.

Displaying accounts on a service

You can display the accounts that are associated with the service instance.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can display accounts on a service in IBM Security Identity Manager, you must create a service instance.

Procedure

To display accounts on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.


2. On the **Select a Service** page, complete these steps:

- a) Type information about the service in the **Search information** field.
- b) In the **Search by** field, specify whether to search against services or business units.
- c) Select a service type from the **Search type** list.
- d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Accounts**.

The tasks that you can do are dependent on the type of service.

The **Accounts** page is displayed.

4. On the **Accounts** page, complete these steps:

- a) Type information about the account in the **Account information** field.
- b) In the **Search by** field, specify whether the search is to be done against user IDs or owners.
- c) In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do.

The advanced search option opens a new page where you can specify additional search criteria.

Note: When you select an ownership of type `Individual` from the list to search accounts, the search yields a list of accounts with ownership of types `Individual` and `None`.

Results

A list of accounts that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

Perform a task on the accounts in the **Accounts** table, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Requesting accounts on a service

You can submit a request for an account on a service or schedule submission of the request.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can request accounts on a service in IBM Security Identity Manager, you must create a service instance. In addition, the user must already be provisioned for an account on the service.

Procedure

To request an account on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Request Accounts**.
The tasks that you can do are dependent on the type of service.
The **Select a User** page is displayed.
4. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field.
 - b) In the **Search by** list, select the criteria that you want, and then click **Search** or **Advanced**, depending on the type of search you want to do.
The advanced search option opens a new page where you can specify additional search criteria.
A list of users that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
5. Select the user that you want to request an account for, and then click **Continue**.
The **Select an Ownership Type** page is displayed.
6. Select the ownership type for the account, and then click **Continue**.
The **Account Information** page is displayed.
7. Specify information for the account, including whether to change the password at the next login, and then click one of the following buttons:
 - **Submit Now**. This option submits the account request immediately.
 - **Schedule Submission**. This option opens the **Schedule** page. Specify whether to schedule the request immediately, or specify the date and time for submitting the account request, and then click **Submit**.

Results

A message is displayed, indicating that you successfully submitted a request to create an account on the service.

What to do next

Select another account request task, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Changing accounts on a service

You can change an account on an existing service if necessary.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can change accounts on a service in IBM Security Identity Manager, you must create a service instance.

In addition, an account must exist, and the account must have an owner. In other words, orphan accounts cannot be changed.

Procedure

To change an account on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.


2. On the **Select a Service** page, complete these steps:

- a) Type information about the service in the **Search information** field.
- b) In the **Search by** field, specify whether to search against services or business units.
- c) Select a service type from the **Search type** list.
- d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Accounts**.

The tasks that you can do are dependent on the type of service.

The **Accounts** page is displayed.

4. On the **Accounts** page, complete these steps:

- a) Type information about the account in the **Account information** field.
- b) In the **Search by** field, specify whether the search is to be done against user IDs or owners.
- c) In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do.

The advanced search option opens a new page where you can specify additional search criteria.

A list of accounts that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

5. In the **Accounts** table, select the check box next to the account that you want to change, and then click **Change**.

The **Account Information** page is displayed.

6. Change information for the account, and then click **Submit Now** or **Schedule Submission**.

The schedule submission option opens a new page where you can specify the date and time for submitting the changes to the account.

Results

A message is displayed, indicating that you successfully submitted a request to change an account on the service.

What to do next

Select another account task, or click **Close**. When the **Accounts** page is displayed, click **Refresh** to refresh the **Accounts** table, or click **Close**.

Deleting accounts from a service

You can delete an account from a service instance if necessary.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can delete accounts from a service in IBM Security Identity Manager, you must create a service instance.

Procedure

To delete an account from a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.


2. On the **Select a Service** page, complete these steps:

- a) Type information about the service in the **Search information** field.
- b) In the **Search by** field, specify whether to search against services or business units.
- c) Select a service type from the **Search type** list.
- d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Accounts**.

The tasks that you can do are dependent on the type of service.

The **Accounts** page is displayed.

4. On the **Accounts** page, complete these steps:

- a) Type information about the account in the **Account information** field.
- b) In the **Search by** field, specify whether the search is to be done against user IDs or owners.
- c) In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do.

The advanced search option opens a new page where you can specify additional search criteria.

A list of accounts that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

5. In the **Accounts** table, select the check box next to the account that you want to delete, and then click **Delete**. Selecting the check box at the top of this column selects all accounts.
A confirmation page is displayed.
6. On the **Confirm** page, specify the date and time for the deletion to occur, and then click **Delete**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully submitted a request to delete an account from the service.

What to do next

Select another account task, or click **Close**. When the **Accounts** page is displayed, click **Refresh** to refresh the **Accounts** table, or click **Close**.

Suspending accounts on a service

You can suspend an account on a service. This action makes the account inactive.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.


Before you can suspend accounts on a service in IBM Security Identity Manager, you must create a service instance.

In addition, an account must exist, and the account must have an owner.

Note: Suspension of an account does not automatically terminate active sessions that use the suspended account. The account owner is notified when the account is suspended. For privileged accounts that have special privileges to access sensitive information in the system or application, the account owner must follow up manually to ensure that the suspended account can no longer be used to access the system or application immediately after the account is suspended.

Procedure

To suspend an account on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Accounts**.
The tasks that you can do are dependent on the type of service.
The **Accounts** page is displayed.

4. On the **Accounts** page, complete these steps:
 - a) Type information about the account in the **Account information** field.
 - b) In the **Search by** field, specify whether the search is to be done against user IDs or owners.
 - c) In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do.

The advanced search option opens a new page where you can specify additional search criteria.
A list of accounts that matches the search criteria is displayed.

If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
5. In the **Accounts** table, select the check box next to the account that you want to suspend, and then click **Suspend**.

A confirmation page is displayed.
6. On the **Confirm** page, specify the date and time for the suspension to occur, and then click **Suspend**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully submitted a request to suspend an account on the service.

What to do next

Select another account task, or click **Close**. When the **Accounts** page is displayed, click **Refresh** to refresh the **Accounts** table, or click **Close**.

Restoring accounts on a service

You can restore an inactive account on a service and make the account active again.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can restore accounts on a service in IBM Security Identity Manager, you must create a service instance.

The account must be inactive, and it must have an owner.

Procedure


To restore an account on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Accounts**.
The tasks that you can do are dependent on the type of service.
The **Accounts** page is displayed.
 4. On the **Accounts** page, complete these steps:
 - a) Type information about the account in the **Account information** field.
 - b) In the **Search by** field, specify whether the search is to be done against user IDs or owners.
 - c) In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do.
The advanced search option opens a new page where you can specify additional search criteria.
A list of accounts that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 5. In the **Accounts** table, select the check box next to the account that you want to suspend, and then click **Restore**.
The **Schedule** page is displayed.
 6. On the **Schedule** page, specify the date and time for the restoration to occur, and then click **Submit**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully submitted a request to restore an account on the service.

What to do next

Select another account task, or click **Close**. When the **Accounts** page is displayed, click **Refresh** to refresh the **Accounts** table, or click **Close**.

Assigning an account to a user

You can assign an account to a user.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must create a service instance and do a reconciliation.

Procedure

To assign an account to a user, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.

- d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon (▶) next to the service to show the tasks that can be done on the service, and then click **Accounts**.
The tasks that you can do are dependent on the type of service.
The **Accounts** page is displayed.
4. On the **Accounts** page, complete these steps:
 - a) Type information about the account in the **Account information** field.
 - b) In the **Search by** field, specify whether the search is to be done against user IDs or owners.
 - c) In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do.
The advanced search option opens a new page where you can specify additional search criteria.
A list of accounts that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
5. In the **Accounts** table, click the icon (▶) next to the account to show the tasks that can be done on the account, and then click **Assign to User**.
The **Select a User** page is displayed.
6. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Search information** field, select an attribute from the **Search by** list, and then click **Search**.
 - b) In the **Users** table, select the name of the user that you want to assign the selected account to, and then click **Continue**.
If the provisioning policy entitles more than one ownership type, the **Select an Ownership Type** page is displayed. Otherwise a confirmation page is displayed.
7. On the **Select an Ownership Type** page, choose an ownership type for the account.
The provisioning policy for the service determines the number of ownership types available. This page is displayed only if more than one ownership type is entitled on the service.
A confirmation page is displayed.
8. On the **Confirm** page, specify the date and time for the account assignment to occur, and then click **Assign to User**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully submitted a request to assign an account to a user.

What to do next

Select another account task, or click **Close**. When the **Accounts** page is displayed, click **Refresh** to refresh the **Accounts** table, or click **Close**.

Orphan accounts

Orphan accounts are accounts on the managed resource whose owner in the IBM Security Identity Manager Server cannot be determined.

Orphan accounts are identified during reconciliation when the applicable adoption rule cannot successfully determine the owner of an account. You can also make an account into an orphan account if the current owner of the account is not correct.

Orphan accounts are included in the list of accounts that are associated with a service. You can suspend or delete orphan accounts or assign them to users.

- When you assign an orphan account to a user, the user becomes the owner of the account. Also, the policies that are applicable to the users are evaluated and enforced for the account. The owner can manage the account with the Self Service or the Identity Service Center user interface.
- When you suspend an orphan account, it is suspended on the Security Identity Manager Server and on the managed resource.
- When you delete an orphan account, it is deleted on the managed resource.

Making an orphan account

You can change an account so that it is an orphan account.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must create a service instance and either created an account or done a reconciliation on an existing account.


Procedure

To change an account so that it is an orphan account, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Accounts**.
The tasks that you can do are dependent on the type of service.
The **Accounts** page is displayed.
4. On the **Accounts** page, complete these steps:
 - a) Type information about the account in the **Account information** field.
 - b) In the **Search by** field, specify whether the search is to be done against user IDs or owners.
 - c) In the **Ownership type** field, select an ownership type, and then click **Search** or **Advanced**, depending on the type of search you want to do.

The advanced search option opens a new page where you can specify additional search criteria. A list of accounts that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
5. In the **Accounts** table, click the icon () next to the account to show the tasks that can be done on the account, and then click **Orphan**.
A confirmation page is displayed.
 6. On the **Confirm** page, specify the date and time for the orphan operation to occur, and then click **Orphan**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully submitted a request to change an account to an orphan account.

Note: When an account becomes an orphan account, it no longer has an ownership type. Provisioning policies do not apply to orphan accounts.

What to do next

Select another account task, or click **Close**. When the **Accounts** page is displayed, click **Refresh** to refresh the **Accounts** table, or click **Close**.

Management of account defaults on a service

You can define default values for account attributes either on a service or on a service type.

Note: In previous versions of IBM Security Identity Manager, account defaults were specified with provisioning policy. Account defaults differ from a provisioning policy. Account defaults do not define the set of users who are allowed to have accounts or what attribute values are compliant. Defaults define the default values for a new account. The change of account default configuration does not affect the compliance status of user accounts. A service might be granted for a subset of users (for example, users who belong to specific organization roles). In this case, these global account defaults might be duplicated in multiple provisioning policies that are specific for each role. By using account defaults, you avoid duplicated configurations.

The following list highlights the differences between the use of account defaults and provisioning policies:

- Like "default" provisioning parameters, account defaults specify the default values for account attributes during provisioning.
- Unlike "default" provisioning parameters, account defaults are not scoped by membership. They apply to all users.
- Unlike "default" provisioning parameters, account defaults do not have implications on compliance. A value specified as an account default is not automatically treated as an "allowed" value.
- Values that are specified as account defaults do not occur within the entitlement parameter list. They are entirely independent from provisioning policy.
- Provisioning parameters take precedence over account defaults. Specifically, mandatory and default provisioning parameters override an account default for the same attribute.

Here is an example to illustrate the differences. In this example, we want to define default values and compliance around the "Local Groups" attribute of WinLocal accounts.

In one case, Case A, we define the default value as a provisioning parameter. In the other case, Case B, we define the default value as an account default.

- Case A:

Default provisioning parameter

Guests

Allowed provisioning parameter

Print Operators

- Case B:

Account default

Guests

Allowed provisioning parameter

Print Operators

In both cases, it's clear that **Print Operators** is an allowed value for the attribute. It is also true that in both cases the default value for the attribute is **Guests**. The difference is that defining the value of **Guests** as a provisioning parameter in Case A makes **Guests** an allowed value. An account with **Local Groups = Guests** is compliant. In Case B, an account with **Local Groups = Guests** is not compliant because account default values do not have any implications on compliance.

Consider the following tips for using Account Defaults instead of Provisioning Policy:

- Use account default to set up default account values for attributes that do not affect security concerns. Use provisioning policy to set up account attribute constraints for security compliance. Avoid using the same attributes for both purposes.
- Use default parameters in provisioning policy to set up default values for security sensitive attributes. The defaults can be automatically given to a user when the account is created.
- Use allowed parameters or exclude all but the wanted parameters in provisioning policy to grant access privilege to a user.
- Use mandatory parameters in a provisioning policy to support "required" (must have) access privilege for a user. IBM Security Identity Manager ensures that these values are set for new account. The values are out to an existing account when policy enforcement is set to `correct` and `alert`.

Adding account defaults to a service

You can add default values for attributes. When you create an account for this service, the default values are provided.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must create a service instance before you begin this task.

Consider doing a "supporting data only" reconciliation to sync up account metadata before you configure the account defaults.

About this task

If account defaults are already defined on the service type for this service, a message is displayed. It indicates that account defaults are defined for the service type. If you click **OK**, then the account defaults for the service type are copied to the service. You can either change the account defaults on the service or remove them from the service. Any changes (including removals) do not affect the account defaults on the service type.

Procedure

To add account defaults to a service, complete these steps:


1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.

2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Account Defaults**.

The tasks that you can do are dependent on the type of service.

The **Select an Account Attribute** page is displayed.
4. On the **Select an Account Attribute** page, click **Add** to add an attribute.

The **Select an Attribute to Default** page is displayed.
5. On the **Select an Attribute to Default** page, select an account attribute, and then click one of the following options:
 - **Add**, to add a default value for the selected attribute. Complete the appropriate fields, which vary depending on the type of service, and then click **OK**. The attribute default is added to the list on the **Select an Attribute to Default** page.
 - **Add (Advanced)**, to add a script that specifies a default value for the selected attribute. Type the JavaScript code in the **Script** field, and then click **OK**. The attribute default is added to the list on the **Select an Attribute to Default** page.
6. On the **Select an Account Attribute** page. When you are finished adding attribute defaults to the service instance, click **OK** to save the changes and to close the page.

For JavaScript APIs that are available for account defaults, see the JavaScript document and look for JavaScript Extensions for host component "Account Default."

Results

A message is displayed, indicating that you successfully saved the account defaults on the service.

What to do next

Select another account task, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Changing account defaults for a service

You can change the account defaults for a service instance.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.


You must create account defaults for the service or service type before you begin this task.

About this task

You can change the default values for attributes. The changed default values will **not** affect existing accounts but will be used for new accounts that are created on the service.

Procedure

To change account defaults for a service, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon () adjacent to the service to show the tasks that can be done on the service, and then click **Account Defaults**.
The tasks that you can do are dependent on the type of service.
The **Select an Account Attribute** page is displayed.
4. On the **Select an Account Attribute** page, select the check box adjacent to the attribute that you want to modify, and then click one of the following options:
 - **Change**, which allows you to change the default value for the selected attribute. Complete the appropriate fields, which vary depending on the type of service, and then click **OK**. The template value for the attribute is updated in the list on the **Select an Attribute to Default** page.
Note: If you select this option when an attribute currently has a scripted default value, the existing script will be overwritten with the template value that you specify.
 - **Change (Advanced)**, which allows you to add or change a script that specifies a default value for the selected attribute. Type the wanted JavaScript code in the **Script** field, and then click **OK**. The template value for the attribute is updated in the list on the **Select an Attribute to Default** page.
5. On the **Select an Account Attribute** page, when you are finished changing attribute defaults for the service instance, click **OK** to save the changes and to close the page.

Results

A message is displayed, indicating that you successfully saved the account defaults on the service.

What to do next

Select another account task, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Removing account defaults from a service

You can remove account defaults from a service instance.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must create account defaults for the service or service type before you begin this task.

About this task

Account defaults for the service type are used.

Procedure

To remove account defaults from a service, complete these steps:

1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.


2. On the **Select a Service** page, complete these steps:

- a) Type information about the service in the **Search information** field.
- b) In the **Search by** field, specify whether to search against services or business units.
- c) Select a service type from the **Search type** list.
- d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Account Defaults**.

The tasks that you can do are dependent on the type of service.

The **Select an Account Attribute** page is displayed.

4. On the **Select an Account Attribute** page, select the check box next to the attribute that you want to remove, and then click **Remove**. Selecting the check box at the top of this column selects all attributes.

The attribute default is removed from the list on the **Select an Attribute to Default** page.

5. On the **Select an Account Attribute** page, finish removing attributes from the service instance. Click **OK** to save the changes and to close the page.

Results

A message is displayed, indicating that you successfully removed the account defaults from the service.

What to do next

Select another account task, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Using global account defaults for the service type

Instead of adding account defaults to a service instance, you can use the global account defaults for the service type.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Selecting this option prevents new account defaults from being created on the service, and prevents existing account defaults from being changed or removed. The **Add**, **Change**, and **Remove** buttons are disabled when you choose to use global account defaults.

Procedure

To use the global account defaults for the service type, complete these steps:

1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.


2. On the **Select a Service** page, complete these steps:

- a) Type information about the service in the **Search information** field.
- b) In the **Search by** field, specify whether to search against services or business units.
- c) Select a service type from the **Search type** list.
- d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Account Defaults**.

The tasks that you can do are dependent on the type of service.

The **Select an Account Attribute** page is displayed.

4. On the **Select an Account Attribute** page, select the check box for **Use the global account defaults for the service type**, and then click **OK**.

The buttons and attributes on the **Select an Account Attribute** are disabled.

5. On the **Select an Account Attribute** page, click **OK** to save the changes and to close the page.

Results

A message is displayed, indicating that you successfully saved the account defaults on the service.

What to do next

You can choose to use the account defaults instead of using the global account defaults by clearing the **Use the global account defaults for the service type** check box on the **Select an Account Attribute** page.

Select another account task, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Service tagging

A service tag is used for grouping services. Security Identity Manager, starting with Version 6.0, provides an *ertag* attribute to the service objects. With this attribute, you can group services of the same type by tagging them together. Because the *ertag* attribute is a multi-value attribute, a service can have one or more service tags. Services with the same service tag belong to the same group of services.

The provisioning policies are enhanced to support the service tag entitlement. A service tag entitlement is a service type entitlement with one or more tags. It applies to all services of the specified type with at least one matching tag. For example, if a service tag entitlement might be defined for a Linux service type with the service tag *mytag1* and *mytag2*. Only services of the Linux type that are tagged with either *mytag1* or *mytag2* are subject to the provisioning policy entitlement. Or, if two service tag entitlements are defined as *mytag1* and *mytag2*, then a service with both tags is subject to both entitlements.

A service type entitlement is different from a service tag entitlement in a way that it applies to all services of the specified type. For example, when managing a provisioning policy, you might select POSIX AIX profile as the service type without adding any service tags. All AIX services that you create are governed by this provisioning policy, regardless of whether they have tags or not.

When the service tag attribute is modified, accounts can become noncompliant. You must use Enforce policy on a service task to reevaluate all policies that govern the service. The policy enforcement gathers all policies that affect the selected service, reevaluates the existing accounts, and provisions new accounts.

It is important to understand that the Change service operation does not automatically start policy enforcement. You must manually enforce policies on the service.

Adding the tag attribute to the service template

About this task

Follow these steps to configure the service template.

Procedure

1. Log on to the Security Identity Manager administrative console.
2. From the navigation tree, click **Configure System** > **Design Forms**. The form designer applet opens.
3. In the left pane, double-click the **Service** folder to open the object profiles for the service types available.
4. Double-click the wanted object profile.
For example, POSIX AIX profile, to open the template for that profile. The form template that is associated with the object profile, that is, POSIX AIX profile, is opened in the middle pane.
5. Select the tab to which you want to add the tag attribute.
For example, `$servicetabgeneral`.
6. In the **Attribute List** pane on the right, double-click the `ertag` attribute. The tag attribute is added to the form.
7. To add a multi-value tag attribute, follow these steps:
 - a) Right-click **[TextField]** of `$ertag` from the middle pane.
 - b) Select **Change to** > **Editable Text List**. **[TextField]** becomes **[Editable Text List]**.
8. Click **Form** > **Save Form Template** > **OK** to save the new template.

Adding tags to the service

When you have the tag attribute ready in the service template form, you can add tags to the services.

About this task

Follow these steps to add the tags.

Procedure

1. Log on to the Security Identity Manager administrative console.
2. From the navigation tree, click **Manage Services**.
3. Click **Create** from the Services table. The **Create Service** page opens.
4. Select the type of the service, for example, POSIX AIX profile, and then click **Next**.
5. Specify information about a service instance.
6. In the **Tag** field at the bottom of the page, type the name of the tag and click **Add**. Add more tags when necessary, for example, `mytag1`, `mytag2`.
7. Proceed to finish creating a service.

Policy enforcement

Policy enforcement reevaluates accounts to determine whether they violate provisioning policies.

Provisioning policies govern the access rights of users for specific services. Provisioning enforcement is incorporated into all business processes that manage the identities and access rights of users on a

managed resource. *Policy enforcement* performs appropriate actions to ensure that user access rights comply with the corporate policies.

Policy enforcement is automatically triggered when you create, modify, or delete the provisioning policies. The following table lists the activities that can automatically start policy enforcement.

Class	Operations
Account	Create, modify, delete, request account
Service Group	Request access
Service	Configure policy enforcement, reconcile
Provisioning policy	Change policy
Role	modify membership

However, you must manually start policy enforcement when:

- You create a new service.
- You tag a service or change a service tag.

These situations can cause accounts to become noncompliant or require new accounts to be provisioned. The policies governing this service must be reevaluated to ensure that all accounts are compliant with the provisioning policies. If policy enforcement finds any missing accounts for users who are automatically entitled to an account, it provisions new accounts for them.

You can configure policy enforcement globally or for a specific service. You can choose these enforcement actions:

- Mark
- Suspend
- Correct
- Alert
- Use Global Enforcement: Mark

All services except DSML Identity Feed services have policy enforcement. You can perform policy enforcement at any time. When you select to enforce a policy, policy enforcement is scheduled to take action.

Policy enforcement actions

To resolve noncompliant accounts on a service, you can take one of these actions:

Mark

Flags the disallowed account or an account that has noncompliant attribute value.

Suspend

Deactivates the disallowed account or an account that has noncompliant attribute value.

Correct

Replaces a noncompliant attribute on an account with the correct attribute.

The disallowed accounts from the policy evaluation can be exempt from this **Correct** action. IBM Security Identity Manager provides the default exemption handler. This handler uses the `correct.enforcement.exemption.account.criteria` property in the `enRole.properties` file to determine the matching criteria of exempt accounts. The accounts that match any of the specified criteria are orphaned instead of being removed. The exempt action is defined by the `correct.enforcement.exemption.account.action` property value specified in the `enRole.properties` file.

You can also plug in your own custom exemption handler. You can implement the `com.ibm.itim.policy.dynanalysis.ICorrectEnforcementExemptionHandler` Java

Interface and specify the implementation class name in the `correct.enforcement.exemption.account.handler` property of the `enRole.properties` file. For more information about the Java interface and writing your own exemption handler, see the API documentation.

Alert

Notifies the user about a disallowed account or value.

Use Global Enforcement Action: Mark

Uses the current global enforcement action for a noncompliant account value.

Policy enforcement alerts

Policy enforcement alerts notify a dedicated user about security compliance violations so that they can correct them. When an account becomes noncompliant, the person designated in the compliance alert configuration is notified. To make a noncompliant account compliant, a service owner can then create a compliance process for Security Identity Manager to bring the account back into compliance.

Depending on the privilege rules defined on the account attributes, accounts are considered noncompliant when users:

- Possess account privileges for reasons that are no longer valid.

In this situation, you must revoke the privileges to make the accounts compliant. When privileges are revoked, you must define a compliance process for policy enforcement. When the policy enforcement action is set as **Alert**, the compliance alert process is triggered.

- Do not possess account privileges that they must have.

In this situation, you must grant privileges to these users to make the accounts compliant. If an account is noncompliant because additional privileges are needed, those privileges are granted automatically.

When you define a compliance process to enforce a policy, the noncompliant accounts are flagged. Separate compliance alert items are generated for each privilege to be revoked for each account. For example, if an account has two groups that violate the provisioning policies, you address these two groups separately. You can remove one group while you can add a policy to the other group to make it compliant. Different people can perform these corrective actions at different times.

Two types of operations can trigger policy enforcement:

- System-triggered operations, also called indirect operations. They include service reconciliation, policy change, and identity change operations.
- Manually triggered operations, also called direct operations. They include the operations performed directly or manually on an account.

The following actions might trigger a policy enforcement action:

- Changing a policy.
- Performing a service reconciliation.
- Changing an identity in the user interface or through an identity feed. You can revoke privileges through dynamic role changes or entitlement parameter recalculation based on identity information.
- Adding a role to a user.
- Removing a role from a user.
- Changing the definition for a dynamic role.
- Manually modifying an account.

The following table shows the default compliance alert settings.

Table 20. Default compliance alert settings

Operation type	Check box status	Required changes	Action taken for		Account state	Request state
			Granting changes	Revoking changes		
System-triggered	Checked	Granting	Added	-	Compliant	Success
		Revoking	-	Alerted	Noncompliant	#
		Both	Added	Alerted	Noncompliant	#
		None	-	-	Compliant	Success
	UNCHECKED**	Granting	Added	-	Compliant	Success
		Revoking	-	Removed	Compliant	Success
		Both	Added	Removed	Compliant	Success
		None	-	-	Compliant	Success
Manually triggered	Checked	Granting	Alerted	-	Noncompliant	#
		Revoking	-	Alerted	Noncompliant	#
		Both	Alerted	Alerted	Noncompliant	#
		None	-	-	Compliant	Success
	UNCHECKED**	Granting	Exception*	-	Same as previous state	Failed
		Revoking	-	Exception*	Same as previous state	Failed
		Both	Exception*	Exception*	Same as previous state	Failed
		None	-	-	Compliant	Success

Notes:

- * Generates the workflow exception CREATE_ACCOUNT_IS_DISALLOWED.
- ** UNCHECKED results in the same behavior as selecting `Correct` as the enforcement action.
- # The request remains in the `Pending` state until the compliance process completes.

Compliance alerts

When a change to an account causes privileges to be revoked, the system can generate a compliance alert and send it to a designated user. The **Compliance Alert To Do** item in the compliance alert contains information about the noncompliant account. The recipient of the alert can either accept or reject some or all of the changes to this account.

Configuring policy enforcement behavior

You can configure the policy enforcement behavior for accounts that do not comply with existing provisioning policies.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can configure policy enforcement behavior on a service in IBM Security Identity Manager, you must create a service instance.

Procedure

To configure the policy enforcement behavior, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Configure Policy Enforcement**.
The tasks that you can do are dependent on the type of service.
The **Select Action** page is displayed.
4. On the **Select Action** page, select an enforcement action:
 - Select **Mark** to mark a disallowed account or an account that has a noncompliant attribute value, and then click **Continue**.
 - Select **Suspend** to suspend an account that is disallowed or that has noncompliant attribute values, and then click **Continue**.
 - Select **Correct** to remove an account or replace noncompliant attributes on an account with the correct attributes, and then click **Continue**. Disallowed accounts can be exempt from this action if they meet the criteria of exempt accounts, which is defined in the `enRole.properties` file. See *Policy enforcement actions* in [“Policy enforcement” on page 737](#).
 - Select **Alert** to issue an alert for an account that is disallowed or that disallows attribute values (revoking attribute values), and then click **Continue**.
 - Select **Use Global Enforcement Action** to use the current global enforcement action for an account that has a noncompliant attribute, and then click **Continue**.
5. On the **Confirm** page, specify the date and time for the enforcement action to occur, and then click **Submit**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully saved the policy enforcement settings for the service.

What to do next

View the status of the request, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Configuring compliance alert rules

Configure compliance alert rules to specify when compliance alerts are sent.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can configure policy enforcement behavior on a service in IBM Security Identity Manager, you must create a service instance.


About this task

Security Identity Manager must make an informed decision about which account change operations are granting additional privileges and which are revoking privileges for noncompliance resolution. This decision allows users to be informed about accounts that are disallowed or privileges to be revoked before Security Identity Manager removes it from the user. For multi-valued attributes, Security Identity Manager accomplishes this choice through a simple subset relation. For single-valued attributes, Security Identity Manager consults privilege rules to differentiate between granting and revoking actions.

If no privilege rules are defined for an attribute, then any change in a single-valued attribute is assumed to be a revoke action that leads to creation of a compliance alert.

Procedure

To configure compliance alert rules, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Configure Policy Enforcement**.
The tasks that you can do are dependent on the type of service.
The **Select Action** page is displayed.
4. On the **Select Action** page, select **Alert**, and then click **Continue**.
The **Configure Policy Enforcement Behavior** notebook is displayed.
5. On the **General** tab of the notebook, complete the following steps:
 - a) In the **Alert name** field, type a descriptive name for the alert.
 - b) Select the participants to receive the alerts.
The participant fields vary, depending on the type of participants you select.
 - c) Specify the time intervals.
 - d) Select the process types for which an alert is generated.
If no process type is selected, the system automatically corrects a noncompliant account for that process type. The correction can modify or delete the account.

6. On the **E-mail** tab of the notebook, either use the default template, or provide text for the alert notification email message.
7. Click **Submit**.
A confirmation page is displayed.
8. On the **Confirm** page, specify the date and time for the enforcement action to occur, and then click **Submit**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully saved the policy enforcement settings for the service.

What to do next

View the status of the request, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Enforcing policies

When a service is tagged or a service tag changes, use this task to reevaluate the governing provisioning policies for the service.


Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Reconcile the new service before you enforce policies. Enforcing policies on a new service without reconciling first might cause enforcement errors.

Procedure

To schedule policy enforcement on a service, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon () next to the service to show the tasks that you can do on that service.
4. Click **Enforce Policy**.
The tasks that you can do depend on the type of service.
The **Schedule** page is displayed.
5. Select either **Immediate** or **Effective date** to schedule the policy enforcement.
6. Click **Submit**.

Results

A message indicates that you successfully submitted a request to enforce policy on the service.

Account recertification

You can view the status of recertification on accounts, or override the recertification rejection status for accounts.

Account recertification is a process that is used to determine whether accounts are still needed. If the accounts are still needed, then more justification might be required. If the accounts are no longer needed, then certain actions need to be taken. System administrators can create recertification policies for all services, while service owners can create recertification policies for services they own.

All services other than the identity feed service are eligible for recertification. A service can be a member of only one recertification policy.

Orphaned accounts are not included for recertification targets.

You can view the latest recertification status of accounts by service instance.

The administrator or service owner can override certain recertification rejection actions by recertifying accounts on a service. Suspended accounts are not reactivated during the recertification process. The override actions are logged in the recertification log table for reporting.

Displaying account recertification status

You can display the recertification status for accounts that are associated with the service instance.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can display account recertification status on a service in IBM Security Identity Manager, you must create a service instance.

Procedure

To display the recertification status for accounts on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.

2. On the **Select a Service** page, complete these steps:

- a) Type information about the service in the **Search information** field.
- b) In the **Search by** field, specify whether to search against services or business units.
- c) Select a service type from the **Search type** list.
- d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Account Recertification Status**.

The tasks that you can do are dependent on the type of service.

The **Account Recertification Status** page is displayed.

4. On the **Account Recertification Status** page, complete these steps:

- a) Type information about the account in the **Account information** field.
- b) In the **Search by** field, specify whether to search against user IDs or owners, and then click **Search** or **Advanced**, depending on the type of search you want to do.
The advanced search option opens a new page where you can specify more search criteria.

Results

A list of accounts that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

Perform a task on the accounts in the **Account Recertification Status** table, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Recertifying accounts on a service

You can manually recertify accounts that are associated with the service instance. You can also override the recertification status of the account on the service.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.


Before you can recertify accounts on a service in IBM Security Identity Manager, you must create a service instance.

About this task

Accounts that have a rejection status or that are not certified and that can be overridden, have a check box.

Procedure

To recertify the accounts on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Account Recertification Status**.
The tasks that you can do are dependent on the type of service.

The **Account Recertification Status** page is displayed.

4. On the **Account Recertification Status** page, complete these steps:

- a) Type information about the account in the **Account information** field.
- b) In the **Search by** field, specify whether to search against user IDs or owners, and then click **Search** or **Advanced**, depending on the type of search you want to do.

The advanced search option opens a new page where you can specify additional search criteria.

A list of accounts that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

5. In the **Account Recertification Status** table, select the check box next to the account that you want to recertify, and then click **Recertify**. Selecting the check box at the top of this column selects all accounts.

A confirmation page is displayed.

6. On the **Confirm** page, type a reason for the recertification in the **Justification** field, and then click **Recertify**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully overrode the recertification status of the account on the service.

What to do next

Select another recertification task, or click **Close**. When the **Account Recertification Status** page is displayed, click **Refresh** to refresh the **Account Recertification Status** table, and then click **Close**.

Management of groups or access on a service

You can define access, manage group membership, or view the recertification status for the group. Groups are supported in most services managed by IBM Security Identity Manager to allow sets of users to be administered collectively for access control purposes.

Access privileges to IT resources are based on membership of a group. In IBM Security Identity Manager Version 4.6, groups were treated as one of the supporting data on the managed service. Group membership was an attribute on an account. In IBM Security Identity Manager Version 5.0 and there after, groups are treated as supporting data. Groups are also a new type of entity in the IBM Security Identity Manager model. In addition, access that is represented by a group is made available for users to directly request.

Administrators can do these management functions for groups and accesses:

- Review the groups on the managed service
- Assign members to a group or remove members from a group
- Provide business-friendly names, categories, and descriptions of the access represented by the group
- Expose the access to users so that users can directly request or remove access
- Specify owners of access and specify approval of group access requests
- Define policies to enforce the recertification of group access

When access information for the group is defined and enabled in the access view, group membership affects the access list for a user. When a user is added to a group, the access that is granted to the user is displayed in the user's access list. When a user is removed from a group, the access is revoked from the user and removed from the access list.

Approval process for groups and accesses

The approval process might be different for managing groups or accesses, depending on how the request is initiated and submitted. When you manage group members from the Manage Services task, the request is treated as *account* request. Therefore, the request goes through the *account* approval. If the same group is exposed as an access and is requested through an *access* request, then the request goes through the *access* approval. The request does not go through account approval. Only when there is no access approval defined, the request continues to use account approval.

Define access for a group

A service owner can provide business-friendly names, categories, and descriptions of the access represented by the group. The service owner can expose the access to users so that users can directly request or remove access. Service owners can specify the owner of the access, the approval process for the access, and the notification options for access provisioning.

Access types

The following access types are included with IBM Security Identity Manager:

- Application
- Shared Folder
- Mail Group
- Role

Groups on a service are defined with supporting data. The relevant target group information is reconciled as supporting data, which uses a filtered reconciliation on the associated service on the target, pulling back only the groups. The access itself is then defined from groups on a service.

The definition of each access is a one-to-one mapping with a group defined for the adapter type.

After an access is provisioned, the requester effectively becomes a member of the group who is defined by the access entitlement on the target. For access, this reconciliation of supporting data is critical. After the groups are reconciled, access definitions can be created.

Access owner

Access owner is a dedicated IBM Security Identity Manager user who is responsible for the access. ACIs can be set up to grant privileges on the access for the owner. The access owner is often involved in the approval process.

Access approval

Access approval specifies the access request workflow for access request. The access request workflow is defined with the **Access Request Workflow** task. Typically, this workflow is used to define the approval process for the access request.

Access notification

Access notification defines whether the email notifications are sent to the user when access is provisioned or de-provisioned for them.

Clearing access

You can clear an access from its association with the service instance.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can clear access on a service in IBM Security Identity Manager, you must create a service instance.

About this task

This task allows the service owner to clear the access definition for a group.

Procedure

To clear access from a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.


2. On the **Select a Service** page, complete these steps:

- a) Type information about the service in the **Search information** field.
- b) In the **Search by** field, specify whether to search against services or business units.
- c) Select a service type from the **Search type** list.
- d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. In the **Services** table, click the icon () next to the service to show the tasks that can be done on the service, and then click **Manage Groups**.

The tasks that you can do are dependent on the type of service.

The **Manage Groups on Service** page is displayed.

4. On the **Manage Groups** page, complete these steps:

- a) Type information about the group in the **Group information** field.
- b) In the **Search by** field, specify whether to search against groups or accesses, and then click **Search**.

A list of groups or access that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

- c) In the **Groups** table, select the group that has the access that you want to clear, and then click **Change**.

5. On the **General Information** page:

- a) Click the **Access Information** tab to display the **Access Information** page.
- b) Clear the **Define an Access** check box to clear the access and all its data.
- c) Click **OK** to submit your changes.

Results

A list of groups or access that matches the search criteria is displayed. The access information for the group is cleared, and the group is not exposed in the access request.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

Perform a task on the items in the **Group** table, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Enabling access for multiple services

You can enable access for multiple services.

Before you begin

Ensure that your system administrator grants you the ACI **Modify operation** permission.

If the **Enable Access** and **Disable Access** buttons are not visible, configure the view. In the administrator console, go to **Set System Security > Manage Views**. As an administrator, grant permissions for the logged in user. Browse to **User View > Admin Console > Manage Services > Change Service**.

About this task

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the IBM Security Identity Manager administrative console, click **Manage Services**.
The **Select a Service** page is displayed.
2. Click **Search** to filter or browse for the available services.
3. Select the box for each service that you want to enable access.
4. Click **Enable Access**.

Access is not enabled, if the following occurs:

- The existing service is already enabled with access or enabled as common access.
- The existing service can define access. For example: **HR Feed** service.
- You have insufficient authorization to enable access on a selected service.

If any of your selected services are valid, the configuration page for the service is displayed.

5. Optional: To copy the service description to the access description, select **Use service description as access description**.

Note: If selected, the service description overrides the existing access description.

6. Select an access type.

The default access type for a service is **Application**. If **Application** is removed as an access type, the first access type is the default option.

7. Click **Enable**.

Review the messages to confirm that access is enabled successfully.

8. Click **Cancel** to return to the **Manage Services** page.

Enabling access for multiple groups

You can enable access for multiple groups.

Before you begin

Ensure that your system administrator grants you the ACI **Modify** at the operation level and **Access Options** at the permission level in the ACI configuration.

If the **Enable Access** and **Disable Access** buttons are not visible, configure the view. As an administrator, go to **User View > Admin Console > Manage Services > Manage Groups on Service**. Define access for the logged in user.

About this task

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the IBM Security Identity Manager administrative console, click **Manage Groups**.

The **Manage Groups** page is displayed.

2. Select a service.
3. Click **Continue** then click **Select Group**.
4. Click **Search** to filter or browse for the available groups.
5. Select the box for each group that you want to enable access.
6. Click **Enable Access**.

Access is not enabled, if the following occurs:

- The existing group is already enabled with access or enabled as common access.
- You have insufficient authorization to enable access on a selected group.

If any of your selected groups are valid, the configuration page for the group is displayed.

7. Optional: To copy the group description to the access description, select **Use group description as access description**.

Note: If selected, the group description overrides the existing access description.

8. Optional: To enable the group as common access, select **Enable as Common Access**.
9. Select an access type.
The default access type for a group is **Application**. If **Application** is removed as an access type, the first access type is the default option.
10. Click **Enable**.
Review the messages to confirm that access is enabled successfully.
11. Click **Cancel** to return to the **Select Group** page.

Disabling access for multiple groups

You can disable access for multiple groups.

Before you begin

Ensure that your system administrator grants you the ACI **Modify** at the operation level and **Access Options** at the permission level in the ACI configuration.

If the **Enable Access** and **Disable Access** buttons are not visible, ensure that your administrator grants you the necessary permissions. As an administrator, to configure the view, go to **User ViewAdmin ConsoleManage ServicesManage Groups on a Service**. Define access for the logged in user.

About this task

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the IBM Security Identity Manager administrative console, click **Manage Groups**.
The **Manage Groups** page is displayed.
2. Click **Search** to filter or browse for the available services.

3. Select a service and click **Continue**.
4. In the **Select Group** area, click **Search** or **Refresh**.
5. Select the box for each group that you want to disable access.
6. Click **Disable Access**.
7. Click **Disable**.
Review the messages to confirm that access is disabled successfully.
8. Click **Cancel** to return to the **Select Group** page.

What to do next

Return to the **Select Group** or **Manage Groups** page to perform other operations.

Disabling access for multiple services

You can disable access for multiple services.

Before you begin

- Ensure that your system administrator grants you the ACI **Modify operation** permission.
If **Enable Access** is not visible, you might not have permissions to the task. For the logged in user, go to **User View > Admin Console > Manage Services > Change Service**.
- As an administrator, grant permissions for the logged in user. On the administrative console, go to **Set System Security > Manage Views**. Select a view. Click **Configure View**. Grant the following task to the user: **User View > Admin Console > Manage Services > Change Service**.

About this task

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the IBM Security Identity Manager administrative console, click **Manage Services**.
The **Select a Service** page is displayed.
2. Click **Search** to filter or browse for the available services.
3. Select the box for each service that you want to disable access.
4. Click **Disable Access**.
5. Click **Disable**.
Review the messages to confirm that access is disabled successfully.
6. Click **Cancel** to return to the **Manage Services** page.

What to do next

Return to the **Manage Services** page to perform other operations.

Chapter 10. Group administration

IBM Security Identity Manager provides predefined groups. You can also create and modify customized groups.

Creating groups

You can create groups either on the ITIM Service or on managed resources.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

If a new group requires a new business unit, create the business unit first. To limit group activities, you might create an extra view or access control item after you create a group. You might create an access control item on the ITIM Service before creating a group. If the group does not previously exist, the access control item does not have the intended membership.

You might upgrade from IBM Security Identity Manager version 5.0 to version 5.1 and use a service instance that was created with a IBM Security Identity Manager 5.0 profile. If so, you must upgrade to the 5.1 adapter before you create groups on the service.

About this task

You can use the **Create Group** wizard to create more groups.

Procedure

To create a group, complete these steps:

1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.

2. On the **Select a Service** page, complete these steps:

- a) Type information about the service in the **Search information** field.
- b) In the **Search by** field, specify whether to search against services or business units.
- c) Select a service type from the **Search type** list.
- d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. In the **Create Group** wizard, complete these steps:

- a) On the **Select Type** page, click the radio button next to the type of group that you want to create, and then click **Next**.

The **Select Type** page is displayed only if the service supports more than one type of group.

- b) On the **General Information** page, complete the expected fields. Click **Next** to display the **Access Information** page, or click **Finish** to complete the operation without adding access information or any members to the group.

- c) Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Click the radio button for the type of access you want to enable. Specify the expected access information and any other information such as access type, description, access

owner, search terms, approval workflow, notification options, search terms, or badges. Click **Next** to display the **Group Membership** page, or click **Finish** to complete the operation without adding any members to the group.

- d) Optional: On the **Group Membership** page, add members to the group, and then click **Next** to display the **Schedule Add Member Operation** page.
- e) On the **Schedule Add Member Operation** page, specify when to add the members to the group, and then click **Finish**.

The **Schedule Add Member Operation** page is displayed only if you chose to add members to the group on the **Group Membership** page.

Results

A page is displayed, indicating that the operation was successful. The new group is created on the service.

What to do next

You can create another group, add or remove members for the new group, or click **Close** to close the page.

If the new group is created on the ITIM Service, you can create an access control item to associate with this group.

Viewing group membership

You can view members of groups.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

To view members of a group, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. On the **Select Group** page, complete these steps to view the groups that exist for the service:
 - a) Type information about the group in the **Search information** field.

For ITIM service groups

In the **Search by** field, specify whether the search is done against group names or descriptions, or business units, and then click **Search**.


For managed resource groups

In the **Search by** field, specify whether the search is done against group names or descriptions, or access name. Select a type of group from the **Group type** list, and then click **Search**.

A list of groups that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

4. In the **Groups** table, click the icon () next to the group, and then click **Manage Members**.

The **Manage Members** page is displayed.

5. On the **Manage Members** page, complete these steps:

- a) Type information about the user in the **System account information** field.
- b) In the **Search by** field, specify whether the search is done against users or user IDs, and then click **Search**.

Results

A list of users that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

You can add or remove group membership.

Adding members to groups

You can add members to groups.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

To add members to a group, complete these steps:

1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.

2. On the **Select a Service** page, complete these steps:

- a) Type information about the service in the **Search information** field.
- b) In the **Search by** field, specify whether to search against services or business units.
- c) Select a service type from the **Search type** list.
- d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. On the **Select Group** page, complete these steps to view the groups that exist for the service:

a) Type information about the group in the **Search information** field.

For ITIM service groups

In the **Search by** field, specify whether the search is done against group names or descriptions, or business units, and then click **Search**.


For managed resource groups

In the **Search by** field, specify whether the search is done against group names or descriptions, or access name. Select a type of group from the **Group type** list, and then click **Search**.

A list of groups that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

4. In the **Groups** table, click the icon () next to the group, and then click **Add Members**.

The **Add Members** page is displayed.

5. On the **Add Members** page, complete these steps:

a) Type information about the user in the **System account information** field.

b) In the **Search by** field, specify whether the search is done against users or user IDs, and then click **Search**.

A list of users that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

c) In the **System Accounts** table, select one or more users that you want to add to the group, and then click **OK**.

A confirmation page is displayed.

6. On the **Confirm** page, specify when you want the users to be added to the group, and then click **Submit**.

A page is displayed, indicating that the operation was successful.

7. On the **Success** page, click **Close**.

Results

The members are added to the group.

What to do next

You can continue working with groups, add or remove more members, or view your request.

Removing members from groups

You can remove members from groups.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

To remove members from a group, complete these steps:

1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.

2. On the **Select a Service** page, complete these steps:

- a) Type information about the service in the **Search information** field.
- b) In the **Search by** field, specify whether to search against services or business units.
- c) Select a service type from the **Search type** list.
- d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

3. On the **Select Group** page, complete these steps to view the groups that exist for the service:

- a) Type information about the group in the **Search information** field.

For ITIM service groups

In the **Search by** field, specify whether the search is done against group names or descriptions, or business units, and then click **Search**.


For managed resource groups

In the **Search by** field, specify whether the search is done against group names or descriptions, or access name. Select a type of group from the **Group type** list, and then click **Search**.

A list of groups that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

4. In the **Groups** table, click the icon () next to the group, and then click **Manage Members**.

The **Manage Member** page is displayed.

5. On the **Manage Members** page, complete these steps:

- a) Type information about the user in the **System account information** field.
- b) In the **Search by** field, specify whether the search is done against users or user IDs. Then, click **Search**.

A list of users that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

- c) In the **Group Membership** table, select one or more users that you want to remove from the group, and then click **Remove**.

A confirmation page is displayed.

6. On the **Confirm** page, specify when you want the users to be removed from the group, and then click **Remove**.

A page is displayed, indicating that the operation was successful.

7. On the **Success** page, click **Close**.

Results

The members are removed from the group.

What to do next

You can continue working with groups, add or remove more members, or view your request.

Modifying groups

As an administrator, you can modify the attributes of a group. These attributes depend upon the type of service that you selected for the group.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Determine what expansion or limits to set on the tasks the members see, and, which access control items might also require changes.

You cannot change the predefined System Administrator group.

Procedure

To change a group, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search Type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. On the **Select Group** page, to view the groups that exist for the service, type the information about the group in the **Search information** field.

For ITIM service groups

In the **Search by** field, specify whether the search is done against group name or descriptions, or business units and then click **Search**.

For managed resource groups

In the **Search by** field, specify whether the search is done against group names or descriptions, or access name. Select a type of group from the **Group type** list, and then click **Search**.

A list of groups that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
4. In the **Groups** table, select the group that you want to modify, and then click **Change**.
The **Change Group** page is displayed.
 5. On the **Change Group** page, take the following actions:

ITIM service groups

To Change the view, select the wanted view from the **View** menu. Type or change a description in the **Description** field. When your changes are made, click **OK** to complete the operation.

Managed resource groups

The fields that are displayed and that can be modified depend on the type of remote service you selected.

Note: Although the **Group ID number** is a modifiable field, do not change this number because doing so compromises system security.

After you modify the information, click the **Access Information** tab to display the **Access Information** page, or click **OK** to complete the operation without changing access information. On the **Access Information** page, you can modify the information such as access type, description, owner, search terms, approval workflow, notification options, search terms, or badges. Then, click **OK** to complete the operation.

Results

A page is displayed, indicating that the group change operation was successful. The changes that you made to the group are now in effect.

What to do next

On the **Success** page, click **Close**.

Values and formats for CSV access data (group)

A group access CSV file can contain multiple values and supported formats.

Consider these points before you work with any CSV files for a group access:

- If you use a custom label for AccessType, specify the key in the CSV file.
- If you use a custom label for badge text, add a \$ prefix on the key. For example, \$mail.
- Define multiple values for search terms and badges with a semicolon (;) separator.
- Define the AccessType hierarchy with a colon (:) separator.
- Use the badgeText~badgeStyle format for badges.

Define CSV columns for a group access as follows:

Table 21. CSV fields and values. CSV fields and values

Field name	Value
GROUP_DN, GROUP_NAME	Not modifiable.
DEFINE_AS_ACCESS	TRUE or FALSE. If you do not assign any value, then FALSE is assumed.
ACCESS_NAME	Required for services and groups, and contains a maximum length of 240 characters. This field is not available for roles.
ACCESS_TYPE	Required. You must specify an access type that is defined in IBM Security Identity Manager.
ACCESS_DESCRIPTION	Contains a maximum length of 240 characters.
ICON_URL	Provide a valid icon URL value on the access definition.
SEARCH_TERMS	Each search term contains a maximum length of 80 characters. You can have multiple search terms.
ADDITIONAL_INFORMATION	Contains a maximum length of 1024 characters.
BADGES	The maximum length for each badge text is 512 characters. You can have multiple badges. The badge text that is prefixed with a \$ sign cannot contain delimiter characters such as ., ;, =, or white space.

A group access CSV file for an export or import operation in the IBM Security Identity Manager administration console contains these columns with sample values and supported formats:

Table 22. Part 1 of 2: Group access CSV file values, formats

GROUP_NAME	DEFINE_AS_ACCESS	ACCESS_NAME	ACCESS TYPE	ACCESS_DESCRIPTION	ICON_URL
admin	FALSE	Access	Application:Group	This access is for the admin group.	http://www-03.ibm.com/ibm/history/exhibits/logo/images/920911.jpg
AIX Group	TRUE	AIX Group	AccessGroup	This access is for the AIX group.	/itim/ui/custom/ui/images/homepage/RequestAccess.png
Default Group	TRUE	default access	EmailGroup:Department:Location	This access is a default group access.	http://www-03.ibm.com/ibm/history/exhibits/logo/images/920911.jpg

Table 23. Part 2 of 2: Group access CSV file values, formats

GROUP_NAME	SEARCH_TERMS	ADDITIONAL_INFORMATION	BADGES	SERVICE_DN
admin	Group;Group access	Group that is used by a client user.	\$highrisk~red	erglobalid=5628670506891199803,ou=groups,erglobalid=000000

Table 23. Part 2 of 2: Group access CSV file values, formats (continued)

GROUP_NAME	SEARCH_TERMS	ADDITIONAL_INFORMATION	BADGES	SERVICE_DN
AIX Group	Employee;Group;AccessGroup	Used by the customer to deploy server.	Group~yellow	erglobalid=5628669752130902869,ou=groups,erglobalid=000000
Default Group	Mail;Unique ID	BVT server that is used to run BVT from developer and tester.	\$mailer~yellow;highrisk~red	erglobalid=5628670337030215245,ou=groups,erglobalid=000000

Exporting access data for a group

Export the access data for a group in a comma-separated value (CSV) file format by using the IBM Security Identity Manager Console.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you export a group, you must have ACI privileges for Define Access and Search Operations on the group that you want to view. If the necessary privileges do not exist, then the group is not exported.

The **Export Access Data** button is not active until you select some group accesses to activate it. Only the group access that you selected is exported as access data.

About this task

Export the selected group access data in a CSV file format for your requirements.

Procedure

1. From the navigation tree, select **Manage Groups**.
The **Select Group** page is displayed.
2. On the **Select Group** page, in the **Groups** table, click **Export Access Data**.
The **Export access data** page is displayed. After you submit the export request, a process status indicates the advancement of the export operation.
3. Optional: Click **Cancel** to discontinue the export operation.
4. Click **Download Exported File** to download the CSV file on your local system by using your web browser settings.

The exported CSV file contains all the group access data.

Note: Click **Download Export Log File** to view any error or log information about the export operation. This button is displayed only if the submitted export operation contains any log information or encountered any errors.

Results

The exported CSV file contains all the access data for a group. Click **Close** to exit from the **Export access data** page.

What to do next

Import access data for a group, or you can continue to export access data by clicking **Export Access Data** in the **Select Group** page.

Importing access data for a group

Use the IBM Security Identity Manager Console to import the group access data from a comma-separated value (CSV).

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

The privileged user that uploads the CSV file must have the appropriate permissions.

Before you import a group, you must have ACI privileges for Search, Define Access, and Modify Operations on the group that you want to update. If the necessary privileges do not exist, then the group is not imported.

Before you import a CSV file, verify that the CSV-related conventions are met. They are as follows:

- The access type hierarchy is represented in the following format, and each access type be separated by a colon (:). For example:

```
AccessType1:AccessType2
```

- The badge information is provided in the following format. For example:

```
badgeText~badgeStyle
```

- Multiple badges can be assigned to accesses in the following format, and each badge must be separated by a semicolon (;). For example:

```
Badge1~red;Badge2~green
```

- Multiple search terms and access types can be specified by using the semicolon (;) separator.
- The relevant keys must be provided in the CSV file for the customized labels that are related to badges and access types.

About this task

Only the accesses with the **Define as Access** set to `True` are defined as accesses, and the corresponding data is imported.

Procedure

1. From the navigation tree, select **Manage Groups**.
The **Select Group** page is displayed.
2. On the **Select Group** page, in the **Groups** table, click **Import Access Data**.
The **Import access data** page is displayed.
3. Click **Browse** in **File to Upload (.CSV)** to locate and upload a valid CSV file that contains all the access data for a group.
4. Click **Import** to import the CSV file.
After you submit the import request, a process status indicates the advancement of the import operation.

Note: If you click **Import** with an invalid file format, a message is displayed to inform you that the file format is not valid.

If any problems occur when you are importing a CSV file, then close the **Import access data** page to continue working with the IBM Security Identity Manager Console. The problems might be due to one of the following conditions:

- The access data CSV file does not exist.

- The CSV file was renamed.
 - The CSV file does not contain appropriate separators or delimiters.
5. Optional: Click **Cancel** to discontinue the import operation.

Note: Click **Download Import Log File** to view any error or log information about the import operation. This button is displayed only if the submitted import operation contains any log information or encountered any errors.

Results

The imported CSV file contains all the access data for a group. Click **Close** to exit from the **Import access data** page.

What to do next

Export access data for a group, or you can continue to import access data by clicking **Import Access Data** in the **Select Group** page.

Deleting groups

You can delete groups from an ITIM service or from a managed resource.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you delete a group, remove the members from the group, and remove the reference to the group from provisioning policy entitlement parameters.

About this task

You cannot delete a group that has members. If you delete a group that is referenced by provisioning policies, you must remove those references from the provisioning policy parameters. Otherwise, those references might generate warnings for the affected accounts. For ITIM Service groups, members who are logged on during removal from a group continue to have their current tasks. The change in group membership takes effect at the next logon.

Procedure

To delete a group, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. On the **Select Group** page, complete these steps to view the groups that exist for the service:
 - a) Type information about the group in the **Search information** field.

For ITIM service groups

In the **Search by** field, specify whether the search is done against group names or descriptions, or business units, and then click **Search**.

For managed resource groups

In the **Search by** field, specify whether the search is done against group names or descriptions, or access name. Select a type of group from the **Group type** list and then click **Search**.

A list of groups that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

4. In the **Groups** table, select one or more groups that you want to delete, and then click **Delete**.

A confirmation page is displayed.

5. On the **Confirm** page, click **Delete**.

A page is displayed, indicating that the delete operation was successful.

Results

The group is deleted from the service.

What to do next

You can continue working with groups, or click **Close**.

Defining access on a group

Define an access to be associated with the group.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can display groups or access on a service in IBM Security Identity Manager, you must create a service instance. In addition, you must do a supporting data reconciliation on that service.

About this task

This task enables the service owner to define access information for a group.

Procedure

To display the groups or access on a service instance, complete these steps:

1. From the navigation tree, click **Manage Services**.

The **Select a Service** page is displayed.

2. On the **Select a Service** page, complete these steps:

- a) Type information about the service in the **Search information** field.
- b) In the **Search by** field, specify whether to search against services or business units.
- c) Select a service type from the **Search type** list.
- d) Select a status from the **Status** list, and then click **Search**.

A list of services that matches the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.

- Type the number of the page that you want to view and click **Go**.
3. On the **Select Group** page, to view the groups that exist for the service, type the information about the group in the **Search information** field. In the **Search by** field, specify whether to search against group names or descriptions, or access name. Select a type of group from the **Group type** list, and then click **Search**.

A list of groups that matches the search criteria is displayed.

If the table contains multiple pages, you can:

 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 4. In the **Groups** table, select the group for which you want to define an access and then click **Change**.

The **Change Group** page is displayed.
 5. On the **General Information** page, complete these steps:
 - a) Click the **Access Information** tab to display the **Access Information** page.
 - b) Select the **Define an Access** check box to activate the access description fields.
 - c) Select the radio button for the type of access you want to enable.
 - d) Specify an access name in the **Access name** field.
 - e) Specify other information such as icon url, search terms, or badges.
 - f) When you are finished, click **OK**.

Results

A page is displayed, indicating that the group change operation was successful. The access information is added to the group object and stored in the Security Identity Manager LDAP server. If the access is enabled, the user can search and request the access.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

On the **Success** page, click **Close**.

or you can select to:

- Manage groups on a different service
- Return to the list of groups that you were working with

Configuring access catalog information for a group

Configure the access catalog information for a group in the Administrator Console so you can use it in the Identity Service Center Request Access workflow.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You must create a service instance before you can configure the access catalog information for a group in IBM Security Identity Manager.

You can also configure the access catalog information for an existing group.

About this task

Configure the access information for a group by defining certain accesses with the use of a badge. You can highlight certain accesses with badges by attaching text that contains some formatting such as color and font type.

Procedure

To configure the group access information, complete these steps:

1. From the navigation tree, click **Manage Groups**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. Specify appropriate values in the corresponding tabbed pages
4. On the **Access Information** page, complete these steps to configure the access information:
 - a) Select the **Enable access for this group** check box.
 - b) Specify the name, access type, access description, owner, approval, notification options for the group.
You can also specify the icon for the access, search terms, additional information, and badges which are used in the Identity Service Center Request Access.
 - c) Expand the **Select access type** or the **Change access type** tree to select an access type.
The tree label depends on whether you want to create or modify a service.
 - d) Provide a uniform resource identifier (URI) string in the **Icon URL** field for the access icon.
 - e) Specify search strings in the **Search terms** field to return specific search terms.
Add or delete the search terms to suit your requirements.
 - f) Specify any free form information about the access item in the **Additional information** field.
 - g) Expand the **Badges** section to specify the badges that are associated with the role.
 - Specify a badge text in the **Badge text** field.
 - Assign a class from the **Badge class** list for the badge text.
You can see the preview of your badge specifications in the **Preview** area.
5. Depending on whether you created or modified the group access information, click **OK** or **Finish** when you are done.

Results

The access information is added or updated to the group object and stored in the Security Identity Manager LDAP server.

What to do next

On the **Success** page, click **Close**. You can also do the following actions:

- Manage groups on a different service

- Return to the list of groups that you were working with
- Create another group, add, or remove members for the new group
- Create an access control item to associate with this group if the new group is created on the Security Identity Manager service.

Recertifying access on a group

Recertify an access to be associated with the group.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.


Before you can recertify access on a group in IBM Security Identity Manager, you must create a service instance. In addition, you must do a supporting data reconciliation on that service.

About this task

This task allows the service owner to view the recertification status of user access for the selected group. This task also allows the service owner to overwrite the recertification status for access that is either Never Certified or Rejected.

Procedure

To recertify access on a group, complete these steps:

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against services or business units.
 - c) Select a service type from the **Search type** list.
 - d) Select a status from the **Status** list, and then click **Search**.
A list of services that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. Type information about the group in the **Search information** field. In the **Search by** field, specify whether to search against group names or descriptions, or access name, select a type of group from the **Group type** list, and then click **Search**.
A list of groups that matches the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
4. In the **Groups** table, click the icon () next to the group for you want to manage, and then click **Access Recertification Status**.
The **Access Recertification Status** page is displayed.
5. In the **Access Recertification Status** table, select the check box next to the access that you want to recertify, and then click **Recertify**. Selecting the check box at the top of this column selects all accesses.

A confirmation page is displayed.

Results

A list of groups or access that matches the search criteria is displayed. After the recertify operation is complete, the access in the list is marked as **Certified**.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

What to do next

Perform a task on the items in the **Groups** table, or click **Close**. When the **Select a Service** page is displayed, click **Refresh** to refresh the **Services** table.

Enabling automatic group membership

You can set whether automatic membership occurs in a service owner or manager group.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

You can use the **Set Security Properties** page to automatically put the IBM Security Identity Manager accounts of newly named service owners or managers in their groups.

To create a group, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Set Security Properties**.
2. On the **Set Security Properties** page, in the **Group Settings** section, select the **Automatically populate Identity Manager groups** check box, and then click **OK**.

A page is displayed, indicating that the operation was successful.

Results

The automatic action is enabled or disabled immediately. If it is enabled, the Security Identity Manager accounts of newly named managers are placed in the default Managers group.

You do not need to restart the Security Identity Manager Server.

What to do next

On the **Success** page, click **Close**.

Chapter 11. Report administration

IBM Security Identity Manager provides reports for system activity, resources such as accounts that users own, and historical data.

Overview

A *report* is a summary of IBM Security Identity Manager activities and resources. You can generate reports based on requests, user and accounts, services, or audit and security. You can also design custom reports with the report designer.

Report data is staged through a data synchronization process. The process gathers data from the IBM Security Identity Manager directory information store and prepares it for the reporting engine. Data synchronization can be run on demand, or it can be scheduled to occur regularly.

The generated reports are based on the most recent data synchronization, not on current data. Activities that occur after the last data synchronization was done are captured by the next data synchronization. Data in the reports is obtained from the IBM Security Identity Manager database and the directory server.

Access control is available for report management. There are default ACIs for the Manager, Service Owner, and Auditor groups. For example, service owners and managers can search for all persons that they can access. Managers can see direct reports, and service owners can see people on services controlled by ACIs. Auditors can run all reports and see all data. No report access is available for users or members of the Help Desk group.

To generate a report, you must synchronize data at least one time. The report data is based on the most recent data synchronization and is only as accurate as the report data from that synchronization.

Reports are displayed in a separate window; therefore, you must disable pop-up blocking in your browser in order for the reports to be displayed. When you generate a report, be sure to close the report window in your browser before you generate another report. If you do not close the open report window before generating another report, a message displays, instructing you to close the window. Or, the same report might be displayed if it was cached by the browser.

Note: Complex report structures and report query requirements mandate that recertification reports are implemented in Java code rather than in Structured Query Language (SQL). Complex structures include Recertification History, Accounts/Access Pending Recertification and Recertification Policies reports.

Report formats

You can generate reports as a PDF file or as a comma-separated value (CSV) file. By default, reports are generated in PDF format and can be viewed and printed with the Adobe Acrobat Reader. In some cases, PDF formatting produces an additional blank page at the end of the report, which does not indicate that data is missing. You might select a CSV file for the report output. The report is displayed with the application that is mapped to CSV files (for example, Microsoft Excel). If no application is associated with the CSV file type, you are prompted to open or save the file when the report is created.

A PDF report, by default, can contain up to 5000 records. You can change this value with the `enrole.ui.report.maxRecordsInReport` property in the `UI.properties` file. You do not have to restart the server for the changes to take effect. Changes can occur between 30 seconds and 10 minutes. You can increase this value to obtain larger amounts of data in your reports. However, it is possible that you might encounter an `OutOfMemoryError` error by doing so. If this error occurs, increase the application server heap size in the WebSphere Application Server and restart IBM Security Identity Manager.

Report accessibility

The Security Identity Manager reports are accessible in the PDF format.

IBM Cognos reporting framework

Security Identity Manager provides the Cognos® reporting framework to create and analyze reports. You can modify the schema and generate reports in different formats.

Note:

If you work with IBM Cognos Analytics Server, the compatibility with an earlier version of IBM Cognos Analytics Server is not supported. For more information about installation and configuration of IBM Cognos Analytics Server, see https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0.

Note: Cognos reporting does not support Microsoft SQL Server database. Use DB2 database or Oracle database instead.

The IBM Cognos reporting framework includes the following items:

Reporting model

Represents the business view of Security Identity Manager data. You can use the models to customize and generate different types of reports that suit your requirements.

Static reports

Ready-to-use reports that are bundled with the Security Identity Manager reporting packages.

IBM Cognos reporting framework overview

IBM Security Identity Manager Cognos reporting framework customizes the IBM Security Identity Manager reports to your specifications.

This document provides the following information about the IBM Security Identity Manager Cognos report model:

- Prerequisite installation and configuration tasks for the report models.
- Detailed description of the Recertification, Accounts, Provisioning, Roles, Separation of duty, Users, Services, and Access models. The descriptions include the namespaces, query subjects, and query items.
- Types of static reports that are created with the report model.
- References for mapping the attributes and entities, the common tasks for configuring any IBM Cognos report model, or scenario that describes how to customize the report.

IBM Cognos reporting components

The topic describes IBM Cognos reporting components that you might use while you work with IBM Security Identity Manager Cognos report models.

Query Studio

Query Studio is the reporting tool for creating simple queries and reports in IBM Cognos Analytics. To use Query Studio effectively, you must be familiar with your organization's business and its data. You might also want to be familiar with other components of IBM Cognos Analytics.

Report Studio

Report Studio is a Web-based report authoring tool that professional report authors and developers use to build sophisticated, multiple-page, multiple-query reports against multiple databases. With Report Studio, you can create any reports that your organization requires, such as invoices, statements, and weekly sales and inventory reports.

Your reports can contain any number of report objects, such as charts, crosstabs, lists, and also non-BI components such as images, logos, and live embedded applications that you can link to other information.

IBM Cognos Connection

IBM Cognos Connection is the portal to IBM Cognos software. IBM Cognos Connection provides a single access point to all corporate data available in IBM Cognos software.

You can use IBM Cognos Connection to create and run reports and cubes and distribute reports. You can also use it to create and run agents and schedule entries.

Framework Manager

Framework Manager is a metadata modeling tool that drives query generation for IBM Cognos software. A model is a collection of metadata that includes physical information and business information for one or more data sources.

IBM Cognos software enables Performance Management on normalized and denormalized relational data sources and various OLAP data sources. When you add security and multilingual capabilities, one model can serve the reporting, ad hoc querying, and analysis needs of many groups of users around the globe.

Before you do anything in IBM Cognos Framework Manager, you must thoroughly understand the reporting problem that you want to solve.

Prerequisites for IBM Cognos report server

Security Identity Manager supports IBM Cognos Analytics Server.

You must install the software in the following table to work with IBM Security Identity Manager Cognos reports.

Note: Support for prerequisite software is continuously updated. To review the latest updates to this information, see the *Software Product Compatibility Reports* page for "IBM Security Identity Manager" at <https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html>.

Software	For more information, see
IBM Cognos Analytics Server	<ol style="list-style-type: none">1. Access the IBM Cognos Analytics documentation at https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0.2. Search for Cognos Analytics on Premises.3. Search for the Installing and configuring and follow the procedure.
Web server	<ol style="list-style-type: none">1. Access the IBM Cognos Analytics documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html.2. In the content pane, click Supported software environments.3. Click the tab for the supported version of IBM Cognos.4. Under the IBM Cognos Analytics section, click Software in the Requirements by type column.5. In the Supported Software tab, click the Web Servers.

Table 24. Product documentation installation roadmap for IBM Cognos report server (continued)

Software	For more information, see
Data sources	<ol style="list-style-type: none"> 1. Access the IBM Cognos Analytics documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. In the content pane, click Supported software environments. 3. Click the tab for the supported version of IBM Cognos. 4. Under the IBM Cognos Analytics section, in the Requirements by type column, click Software. 5. In the Supported Software tab, click Data sources.

Important: Compatibility with earlier versions of IBM Cognos Analytics Server is not supported. For more information about installation and configuration of IBM Cognos Analytics Server, see https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0.

Installation of IBM Cognos reporting components

Installation of IBM Cognos reporting components is optional. You need these components only if you use the Cognos based reports. You must complete the installation and data synchronization process before you can access and work with IBM Security Identity Manager Cognos reports.

Note: IBM Cognos reporting does not support Microsoft SQL Server database as content store. Use Db2 database or Oracle database instead.

The following table describes the installation and synchronization process.

Table 25. Installation and data synchronization process

Task	For more information
Install Cognos Business Intelligence.	<ol style="list-style-type: none"> 1. Access http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for Install and configure server components.
Install Framework Manager.	<ol style="list-style-type: none"> 1. Access http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for Installing IBM Cognos Framework Manager.
Complete the data synchronization.	<p>See “Data synchronization” on page 894.</p> <p>Note: Run the data synchronization before you generate the reports to obtain the latest report data.</p>

Cognos reporting

Security Identity Manager installs Cognos reports and models. To use these new reports and models, see the Cognos reporting documentation at [IBM Cognos Analytics documentation](#).

Optionally, you can install IBM Framework Manager, if you want to customize the reports or models.

You can find the Cognos reports and models that are specific to Security Identity Manager at:

Note: You must set the locale to English or to any supported language before you run any of the reports. See [“Setting language preferences”](#) on page 783. Otherwise, you might encounter a "Language not supported" issue.

Configuration of IBM Cognos reporting components

After you install the prerequisites for the IBM Security Identity Manager Cognos Analytics server, configure the Framework Manager, and create a content store database. Then, configure the web gateway and web server.

During the database configuration process, ensure that you complete the points in the following note.

Note:

- IBM Cognos reporting does not support Microsoft SQL Server database as content store. Use Db2 database or Oracle database instead.
- Set the JAVA_HOME environment variable to point to the JVM used by the application server.
- You must use the enterprise database as IBM Cognos content store.
- Delete the existing data source and create a new data source to enable an option of generating DDL during creation of the content store database. For information about data source creation, see [“Creating a data source”](#) on page 775.

The following table describes the configuration process.

Each step requires that you search in the Knowledge Center for IBM Cognos Analytics, which is at http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html

<i>Table 26. Configure IBM Cognos reporting components</i>	
Task	For more information
Configure Framework Manager.	Search for Configuring Framework Manager .
Create a content store in the database.	Search for Start IBM Cognos Configuration , complete the steps as per your operating system, then search for Guidelines for creating the content store database .
Configure the web gateway.	Search for Install and configure the gateway .
Configure your web server.	Search for Configure Cognos Analytics with your web server .

Setting report server execution mode

You must have a report server execution mode that is set to 32-bit mode for the report packages that do not use dynamic query mode.

Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** panel, click **Environment**.
3. Click the **Value** box for **Report server execution mode**.
4. Select **32-bit**.
5. From the **File** menu, click **Save**.

What to do next

Restart the IBM Cognos service. Complete the following steps:

1. Access the IBM Cognos Analytics documentation at https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/.
2. Search for **Restarting the IBM Cognos service to apply configuration settings**.

Setting environment variables

You must set the database environment variables for a user before you start the IBM Cognos processes.

Procedure

1. Access the IBM Cognos Analytics documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html.
2. Search for **Suggested settings for creating the content store in IBM Db2 on Linux, Windows and UNIX operating systems**.

What to do next

Start the Cognos service from IBM Cognos Configuration to host the IBM Cognos portal. Complete the following steps:

1. Access the IBM Cognos Analytics documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html.
2. Search for **Starting or stopping the Cognos service**.

Editing the ISIM Environment dashboard refresh interval

You can edit the refresh interval for your software deployment depending on the requirements of your organization.

Procedure

1. Open the ISIM Environment Dashboard in the Report Studio.
2. Navigate to the Page explore tab in the Report Studio.
3. Open the ISIM Environment Dashboard page.
4. Look for the <HTML Item> highlighted on the page.
5. Double click to edit the page. Specify the interval in seconds and save the report.

What to do next

You must do the similar task for the dashboard sub report which contains more dashboard details.

Note: All the sub reports are hidden by default. To view all the hidden reports:

1. Open the Cognos connection portal.
2. Select **My Area > My Preferences**.
3. Select **Show hidden** entries.

Importing the report package

Import the report package to work with the bundled report models and the static reports.

Before you begin

- Copy the ISIMReportingPackage_6.0.x.x.zip file to the directory where your deployment archives are saved. The default location is 10_location/deployment. For more information about the reporting packages, see [“Installation of IBM Cognos reporting components” on page 772](#).
- To access the **Content Administration** area in **IBM Cognos Administration**, you must have the required permissions for the administration tasks secured feature.

Procedure

1. Access the IBM Cognos Gateway URI.

For example, `https://hostname:port/bi/v1/disp`. The *localhost* is the IP address or network host name where IBM Cognos gateway is configured. The *portnumber* is the port on which the IBM Cognos gateway is configured.

2. Go to **Launch**.
3. In the **IBM Cognos Administration** window, click the **Configuration** tab.
4. Click **Content Administration**.
5. Clear the history.
6. On the toolbar, click New Import icon.
The New Import wizard opens.
7. In the **Deployment Archive** box, select **ISIMReportingPackage_6.0.x.x**.
8. Click **Next**.
9. In the **Specify a name and description** window, you can add the description and screen tip.
10. Click **Next**.
11. In the **Select the public folders and directory content** window, select the model that is displayed.
12. In the **Specify the general options** page, select whether to include access permissions and references to external namespaces, and an owner for the entries after they are imported.
13. Click **Next**. The summary information opens.
14. Review the summary information. Click **Next**.
15. In the **Select an action** page, click **Save and run once**.
16. Click **Finish**.
17. Specify the time and date for the run.
18. Click **Run**.
19. Review the run time. Click **OK**.
20. When the import file operation is submitted, click **Finish**.

Results

You can now use the report package to create reports and to run the sample reports. The sample reports are available in the reporting model on the **Public Folders** tab in the IBM Cognos portal.

Creating a data source

To work with the IBM Security Identity Manager Cognos reports, you must create a data source.

Before you begin

- You must use the data source name as ISIM.
- If you are working with DB2 database client, copy the file `db2cli.dll` from the DB2 client installation directory to the `<IBM Cognos installation directory>/bin` folder.
- The data source must be pointed to the IBM Security Identity Manager enterprise database. For example, IBM DB2. After the data synchronization, the data is in the IBM Security Identity Manager enterprise database.

Procedure

1. Access the IBM Cognos Analytics documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html.
2. Search for **Creating a data source** and complete the steps.

What to do next

Note: Corrupted attribute names are displayed in the reports for Arabic, Chinese, Hebrew, Japanese, Korean, and Russian languages. Double-byte character set (DBCS) characters appear to be corrupted in the reports. Edit the data source so that the data flow is in Unicode format. Complete the following steps:

1. On the **Work with Reports** page, click **Launch > IBM Cognos Administration**.
2. Click **Configuration** to open the data source connection.
3. Click **ISIM**.
4. Under the **Actions** column, click **Set properties-ISIM**.
5. On the **Set properties-ISIM** window, click **Connection**.
6. In the **Connection String** field, click the pencil symbol to edit the connection string.
7. In the **Collation Sequence** field, type @UNICODE.
8. Click **OK**.
9. Run the report to verify that the text is no longer corrupted.

Enabling the drill-through for PDF format

You must enable the drill-through functionality to run the drill-through reports in the PDF format.

Before you begin

Disable any pop-up blocking software in the browser.

Procedure

1. Open IBM Cognos Configuration.
2. Specify the fully qualified domain name for all the URIs that are defined.
3. Save the configuration.
4. Restart the IBM Cognos service. Complete the following steps:
 - a) Access the IBM Cognos Analytics documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html.
 - b) Search for **Restarting the IBM Cognos service to apply configuration settings**.
5. In the **Explorer** window, click **Environment**.
6. In the **Group Properties** window, copy the value in the **Gateway URI** box.
7. Paste the copied **Gateway URI** value in the supported browser.
8. Run the report that you want.

Results

The drill-through report is run successfully in the PDF format.

Security layer configuration around the data model and reports

An access to the data model and reports can be restricted to a set of authorization roles. The users can create the authorization roles and associate them with the reporting entities. Only entitled users can access the data model or reports.

Authentication and authorization for IBM Cognos reports

IBM Cognos Analytics administrators can set up the folders that store the reports. They can then secure those folders so that only authorized users can view, change, or perform other tasks by using the reports in the folder. To set up access control on the reports, administrators can set up the user authentication and define the access control for the set of users.

User authentication setup by using LDAP

You can configure IBM Cognos components to use an LDAP namespace for authentication when the users are in an LDAP user directory.

Configuring an LDAP Namespace for IBM Directory Server

If you configure a new LDAP namespace for use with the IBM Directory Server, you must modify the necessary settings and change the values for all properties of the IBM Directory objects.

Procedure

1. Open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**.
3. Click **New resource** > **Namespace**.
4. In the **Name** box, type a name for your authentication namespace.
5. In the **Type** list, click **LDAP-General default values**.
6. Click **OK**.

The new authentication namespace resource appears in the **Explorer** window, under the **Authentication** component.

7. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.

Tip: Do not use colons (:) in the Namespace ID property.

For **Host and Port**, specify <Hostname>:<port>.

For example, localhost:389.

8. Specify the values for all other properties to ensure that IBM Cognos Analytics can locate and use your existing authentication namespace.

- For **Base Distinguished Name**, specify the entry for a user search.
- For **User lookup**, specify (uid=\${userID}).
- For **Bind user DN and password**, specify cn=root. For example, cn=root as a user name and secret as a password.

Note: Specify the values if you want an LDAP authentication provider to bind to the directory server by using a specific bind user DN and password. If no values are specified, an LDAP authentication namespace binds as anonymous.

9. If you do not use external identity mapping, use bind credentials to search an LDAP directory server. Complete the following items.
 - Set **Use external identity** to **False**.
 - Set **Use bind credentials for search** to **True**.
 - Specify the user ID and password for **Bind user DN and password**.
10. To configure an LDAP advanced mapping properties, see the values that are specified in the following table.

Mappings	LDAP property	LDAP value
Folder	Object class	organizationalunit, organization, and container
	Description	description
	Name	ou, o, and cn
Group	Object class	groupofnames

Table 27. LDAP advanced mapping values (continued)

Mappings	LDAP property	LDAP value
	Description	description
	Member	member
	Name	cn
Account	Object class	inetorgperson
	Business phone	telephonenumber
	Content locale	(leave blank)
	Description	description
	Email	mail
	Fax/Phone	facsimiletelephonenumber
	Given name	givenname
	Home phone	homephone
	Mobile phone	mobile
	Name	cn
	Pager phone	pager
	Password	userPassword
	Postal address	postaladdress
	Product locale	(leave blank)
	Surname	sn
	Username	uid

If the schema is modified, you must make extra mapping changes.

11. To prevent the anonymous access, complete the following steps:
 - a) Go to **Security > Authentication > Cognos**.
 - b) Set **Allow anonymous access?** to **False**.
12. From the **File** menu, click **Save**.

Results

A new LDAP namespace is configured with the appropriate values.

What to do next

Create the users in an LDAP. See [“Creating users in an LDAP” on page 778](#).

Creating users in an LDAP

See the example in this procedure that uses an LDAP utility to create users in LDAP.

Procedure

1. Open an LDAP utility.
For example, if you are using the IBM Directory Server, the LDAP utility is `idsldapadd`.
2. Import the sample file `LdapEntries.ldif` that lists all the users who are authorized to access the reports. See the following example.

Results

After the successful import operation, you can see the users that are created in `ou=users,ou=SWG`.

Example

A sample file: `LdapEntries.ldif`

In this example, `dc=com` is the root entry. Specify the entry according to the schema that you use.

```
dn: ou=SWG, dc=com
ou: SWG
objectClass: top
objectClass: organizationalUnit

dn: ou=users,ou=SWG, dc=com
ou: users
objectClass: top
objectClass: organizationalUnit

dn: uid=steves,ou=users,ou=SWG, dc=com
uid: steves
userPassword:: hello123
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Wiley
cn: Steves

dn: uid=PortalAdmin,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: PortalAdmin
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Poon
cn: Chuck

dn: uid=william,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: william
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Hanes
cn: William

dn: uid=lucy,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: lucy
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Haye
cn: Lucy
```

What to do next

Authenticate IBM Cognos by using an LDAP user. Complete these steps:

1. Access the IBM Cognos Gateway URI. For example, `http://localhost:portnumber/bi/v1/disp`. The *localhost* is the IP address or network host name where IBM Cognos gateway is configured. The *portnumber* is the port on which the IBM Cognos gateway is configured.
2. Select the configured **Namespace**, and click **OK**.
3. Enter your LDAP user ID and password.
4. Click **OK**.

Access control definition for the reports and reporting packages

You can define the access control for the LDAP users who are the members of a role that is defined in the IBM Cognos namespace. Access can be granted to those users who are the members of a defined role.

A user who has the system administrator privileges can grant the access.

Initially, all users are the members of the system administrator. Therefore, you can log in with your LDAP user authentication in IBM Cognos and access the administration section before you restrict the administration access.

Restricting administration access and adding an LDAP user to system administrator role

You can restrict the IBM Cognos administration access by using the system administrators role in IBM Cognos namespace. You can also add an LDAP user to the system administrator role for IBM Cognos report administration.

Procedure

1. Log in to IBM Cognos with an LDAP user whom you want to assign the system administrator role.
2. Go to **Launch**, and click **IBM Cognos Administration**.
3. Click the **Security** tab.
4. In the **Users, Groups, and Roles** section, click **Cognos**.
5. Navigate to **System Administrator** role.
6. Click the **More** link.
7. Under **Available actions**, click **Set properties**.
8. Click the **Members** tab.
9. Click the **Add** link.
10. Under **Available entries** section, click an LDAP namespace.
11. Select the **Show users in the list** check box.
12. Select the user whom you want to assign the system administrator role and make it into selected entries list.
13. Click **OK**.
14. Select **Everyone** from the members entry.
15. Click the **Remove** link to ensure that only the added users can have the system administration access.
16. Click **OK**.
17. Click the **Permissions** tab.
18. Verify that the system administrators are listed and they are provided all the permissions.
If no permissions are provided, then select the system administrators and grant all the permissions. Select the **Override the access permissions acquired from the parent entry** check box to grant the permissions.
19. Click **OK**.

Results

An LDAP user is added with the system administrator role.

What to do next

Create a role and add LDAP users as the members to that role. See [“Creating a role and adding LDAP users as members”](#) on page 780.

Creating a role and adding LDAP users as members

The topic describes the procedure to create a role in IBM Cognos and add the members from an LDAP namespace to it.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges.
For example, PortalAdmin.
2. Go to **Launch**, and click **IBM Cognos Administration**.

3. Click the **Security** tab.
4. In the **Users, Groups, and Roles** section, click **Cognos**.
5. Click the **New Role** icon from the palette.
6. Specify the name for a role.
For example, ISIMAuditor.
7. Add the description and the screen tip.
8. Click **Next**.
9. Under **Select the members**, click **Add**.
10. Under **Available Entries Directory**, click an LDAP namespace.
11. Select the **Show users in the list** check box.
12. Select the users whom you want to add as the members to the role and make it into selected entries list.
13. Click **OK**.
14. Click **Finish**.

Results

A new role is created and LDAP users are added as the members to the new role.

Defining an access to the report by using a role

You can define an access to the report by using a role. All the members of a role can access the report or reports.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges.
For example, PortalAdmin.
2. Under **Public Folders**, click the ISIMReportingPackage_6.0.0.4.zip.
3. Click the **More** link on the **Actions** toolbar that is associated with the report for which you want to provide the access.
4. Under **Available actions**, click **Set properties**.
5. Click the **Permissions** tab.
6. Select the **Override the access permissions acquired from the parent entry** check box.
7. Click **Add** link at the bottom of the list of entries.
8. Click **Cognos**.
9. Select the role that you want to add and make it to the selected entries.
10. Click **OK**.
11. Select the role and grant the permissions.
12. Optional: Remove other roles for which you do not want to provide the access.
13. Click **OK**.

Results

An access is defined to the report by using a role and all the members of a role can access the reports.

Defining an access to the reporting package by using a role

You can define an access to the report package by using a role. All the members of a role can access the report package.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges.
For example, PortalAdmin.

2. Under **Public Folders**, click the **More** link on the **Actions** toolbar that is associated with the ISIMReportingPackage_6.0.0.4.zip.
3. Under **Available actions**, click **Set properties**.
4. Click the **Permissions** tab.
5. Select the **Override the access permissions acquired from the parent entry** check box.
6. Click the **Add** link at the bottom of the list of entries.
7. Click **Cognos**.
8. Select the role that you want to add and make it to the selected entries.
9. Click **OK**.
10. Select the role and grant the permissions.
11. Optional: Remove other roles for which you do not want to provide the access.
12. Click **OK**.

Results

An access is defined for the reporting package by using a role and the members of a role can access the reporting package.

References for IBM Cognos report security configuration

Use the following references that provide information about the topics that are related to the security configuration for the IBM Cognos reports.

Access the IBM Cognos Analytics documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html and search for the following terms.

- **Security model.**
- **Authentication providers.**
- **Add or remove members of a cognos group or role.**
- **Create a cognos group or role.**
- **Authorization.**
- **Access permissions and credentials.**

Globalization overview

You can use the globalization features of IBM Security Identity Manager Cognos report models to produce the reports in your own language.

Language support overview

IBM Security Identity Manager Cognos reports support the following languages.

- cs=Czech
- de=German
- en=English
- es=Spanish
- fr=French
- hu=Hungarian
- it=Italian
- ja=Japanese
- ko=Korean
- pl=Polish
- pt_BR=Brazilian Portuguese
- ru=Russian

- zh_CN=Simplified Chinese
- zh_TW=Traditional Chinese
- nl=Dutch
- tr=Turkish
- el=Greek - partially supported.

Note:

The IBM Cognos Business Intelligence Server 11.0.13 is not fully translated into the Greek language. Only components like Cognos Viewer, Cognos Connection, Cognos Administration, and Cognos Workspace support translation in Greek language.

Messages or terms related to the globalization

In the reports, some of the column values might display the term Language not supported

When you select the language that is not supported by the reporting model, the value in the column is displayed as Language not supported.

Setting language preferences

You can personalize the way data appears in IBM Cognos workspace by changing your preferences. You can set the product language or content language to get the preferred output format of the reports.

Before you begin

Install and configure the IBM Cognos Analytics Server.

Procedure

1. In IBM Cognos, click **IBM Security Identity Manager Dashboard** menu button.

2. Click the **Action Menu** 

3. Click **My Preferences**.

4. In the **Set Preferences** window, under the **Regional options** section, select **Product language**.
Product language specifies the language that the IBM Cognos user interface uses.

5. In the **Set Preferences** window, under the **Regional options** section, select **Content language**.
Content language specifies the language that is used to view and produce content in IBM Cognos such as data in the reports.

6. Click **OK**.

Results

You can view the reports or user interface in the language that you specified.

Report models

Use the following information about the objects and the report model names, namespaces, and entities to work with the report models.

Report model objects and their definitions

Use these definitions to work with IBM Security Identity Manager Cognos report models.

Query Items

The smallest piece of the model in a report. It represents a single characteristic of something, such as the date that a product was introduced.

Query subjects or dimensions contain query items. For example, a query subject that references an entire table contains query items that represent each column in the table.

Query items are the most important objects for creating reports. They use query item properties of query items to build their reports.

Query Subjects

A set of query items that have an inherent relationship. In most cases, query subjects behave like tables. Query subjects produce the same set of rows regardless of which columns were queried.

Packages

A subset of the dimensions, query subjects, and other objects that are defined in the project. A package is published to the IBM Cognos server. It creates reports, analyses, and ad hoc queries.

Namespaces

Uniquely identifies query items, dimensions, query subjects, and other objects. You import different databases into separate namespaces to avoid duplicate names.

Recertification model

You can use the recertification model to customize the reports that are related to the recertification audit and configuration.

The recertification model for IBM Security Identity Manager consists of these namespaces:

<i>Table 28. Recertification model namespaces</i>	
Namespace	For information about query subjects and query items, see
Recertification Audit	“Recertification Audit namespace” on page 795.
Recertification Config	“Recertification Config namespace” on page 801.

Accounts model

You can use the accounts model to customize the account audit and configuration reports.

The accounts model for IBM Security Identity Manager consists of two namespaces:

<i>Table 29. Accounts model namespaces</i>	
Namespace	For information about query subjects and query items, see
Account Audit	“Account Audit namespace” on page 807.
Account Configuration	“Account Configuration namespace” on page 810.

Provisioning model

You can use the provisioning model to customize the provisioning policy audit and configuration reports.

The provisioning model for IBM Security Identity Manager consists of two namespaces:

<i>Table 30. Provisioning model namespaces</i>	
Namespace	For information about query subjects and query items, see
Provisioning Policy Audit	“Provisioning Policy Audit namespace” on page 819.
Provisioning Policy Config	“Provisioning Policy Config namespace” on page 821.

Roles model

You can use the roles model to create the role audit and configuration reports.

The roles model for IBM Security Identity Manager consists of two namespaces:

<i>Table 31. Roles model namespaces</i>	
Namespace	For information about query subjects and query items, see
Role Audit	“Role Audit namespace” on page 824.
Role Configuration	“Role Configuration namespace” on page 826.

Note: If you want to run a Role and Policy Modeler report for the roles with IBM Security Identity Manager data, you must rewrite the report or use an existing predefined report in the IBM Security Identity Manager 6.0 Cognos package.

Separation of duty model

You can use the separation of duty model to customize the separation of duty policy audit and configuration reports.

The separation of duty model for IBM Security Identity Manager consists of two namespaces:

<i>Table 32. Separation of duty model namespaces</i>	
Namespace	For information about query subjects and query items, see
Separation of Duty Audit	“Separation of Duty Audit namespace” on page 831.
Separation of Duty Configuration	“Separation of Duty Configuration namespace” on page 836.

Users model

You can customize the user configuration reports with the users model.

The users model for IBM Security Identity Manager consists of the User Configuration namespace. For information about query subjects and query items, see [“User Configuration namespace” on page 838.](#)

Services model

You can customize the audit reports with the services model.

The services model for IBM Security Identity Manager consists of the Service Audit namespace. For information about query subjects and query items, see [“Service Audit namespace” on page 844.](#)

Access model

You can customize the audit and configuration reports with the access model.

The access model for IBM Security Identity Manager consists of these namespaces:

Note: The new Access Audit model is developed for Identity Service Center. An old Access Audit model is renamed to Access Audit (Deprecated).

<i>Table 33. Access model namespaces</i>	
Namespace	For information about query subjects and query items, see
Access Audit (Deprecated)	“Access Audit (Deprecated) namespace” on page 847.
Access Configuration	“Access Configuration namespace” on page 856.
Access Audit	“Access Audit namespace” on page 852.

Report descriptions and parameters

The topics provides information about the IBM Security Identity Manager Cognos static reports that are bundled with the package. You can view the list of reports and the namespaces used to create these reports. Use the parameters and their descriptions information while you generate the reports.

Note:

- You must map the attributes to the entities before you work with the following reports. For more information about mapping the attributes, see [“Mapping the attributes and entities” on page 860.](#)
- You must set the locale to English or to any supported language before you run any of the reports. See [“Setting language preferences” on page 783.](#) Otherwise, you might encounter a "Language not supported" issue.

- Use the percent symbol (%) as a default search character in all the reports.
- Any time stamp in the following reports is in Greenwich Mean Time (GMT) format.
- Use the Report Studio to change the column title names in the layout to meet the specific needs of your company.

You can choose the output format of the reports. For more information about the supported report format, complete the following steps.

1. Access the IBM Cognos Analytics documentation at http://www-01.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.svg.ba.cognos.cbi.doc/welcome.html.
2. Search for **Report Formats**.

Note: You can export the report data in plain format if you use formats other than HTML or PDF. The reports that are generated in such formats do not support some of the IBM Cognos interactive features. For example, charts.

Use HTML or PDF formats for running interactive reports.

The following table lists the reports and the namespaces that generate them.

Reports	Namespace used
Access Definition Report	<ul style="list-style-type: none"> • Access Audit • Access Configuration
Account Status Report	Account Audit
Audit History Report	Access Audit and Account Audit
Entitlements Report	Provisioning Policy Configuration
IBM Security Identity Manager Dashboard	Account Configuration, Provisioning Policy Configuration, User Configuration, and Service Audit (Entity Name Service)
Recertification Definition Report	Recertification Config
Separation of Duty Policy Definition Report	Separation of Duty Configuration
Separation of Duty Policy Violation Report	Separation of Duty Audit
Services Report	Service Audit
User Access Report	Access Configuration
User Recertification History Report	Recertification Audit

Note: The access that is defined on groups and roles cannot be displayed in the User Access Report if the access is disabled.

The following table lists the subreports. These reports are the operational reports and the subsets of the main reports. The subreports are hidden and started from the main reports.

Main report	Subreports
Entitlements Report	<ul style="list-style-type: none"> • Entitlements Sub Report • Entitlements Sub_Sub Report
IBM Security Identity Manager Dashboard	Dashboard sub reports

Table 35. Subreports (continued)

Main report	Subreports
Recertification Definition Report	<ul style="list-style-type: none"> • Access Recertification Definition Sub Report • Account Recertification Definition Sub Report • User Recertification Definition Sub Report
Separation of Duty Policy Definition Report	Separation of Duty Policy Definition Sub Report
Separation of Duty Policy Violation Report	Separation of Duty Violation Definition Sub Report
User Recertification History Report	User Recertification History Sub Report

Access Definition Report

The report provides information about the access definitions. Use the report to view the accesses that are configured in an organization.

After you select the parameter values, the **Prompt Page Summary** provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Table 36. Filters for access definition report

Parameter	Description
Access	Displays the list of accesses for which you want to generate a report.
Access Search Terms	Displays the list of search terms that are defined for an access.
Access Badge Text	Displays the description about the badge that is defined for an access.
Access Type	Displays the type of an access. The type of an access can be a role, application, shared folder, email group, or custom access that is defined in an organization.

You must define the base icon URL path in the query of the access definition report to display the icons in the report. For more information, see [“Defining the base icon URL path”](#) on page 794.

Account Status Report

The report shows the status of an account such as compliant, disallowed, orphan, non-compliant, and suspend. Use the report to view the status of accounts that are provisioned on the different managed resources.

After you select the parameter values, the **Prompt Page Summary** provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Table 37. Filters for Account Status Report

Parameter	Description
Service	Displays the list of all the services that have one or more accounts provisioned.

Table 37. Filters for Account Status Report (continued)

Parameter	Description
Account Status	Displays the status and states of the accounts that are created in an organization. The states of an account are compliant, disallowed, orphan, non-compliant, and suspend.

Audit History Report

The Audit History Report provides information about the history of audits. You can generate the audit history reports for access, account, and a user.

You can generate the following types of subreports from the audit history report.

Note: Use the account audit model and reports to view the details about the accounts that are associated with a user. Use the access audit model and reports to view the details about the accesses that are associated with a user. If the account is on the service that is defined as an access, the audit details can be seen only in the Access Audit report.

Table 38. Audit History subreports

Subreport name	In the Audit Report Type drop-down list
Access audit report.	Select Access . For more information about the access audit report parameters and their descriptions, see “Access audit history report” on page 788.
Account audit report.	Select Account . For more information about the account audit report parameters and their descriptions, see “Account audit history report” on page 789.

After you select the values for the parameters, the **Prompt Page Summary** is generated. The **Prompt Page Summary** provides information about the selected parameters and their values in a table.

Access audit history report

Use this report to view the history of actions that are performed on an access in Identity Service Center.

After you select the values for the following parameters, the **Prompt Page Summary** is generated. The **Prompt Page Summary** provides information about the selected parameters and their values in a table.

Note:

- If the account is on the service that is defined as an access, the audit details can be seen only in the Access Audit history report.
- The parameter filter values are displayed if the access is requested through Identity Service Center.

The following table describes the parameters for filtering the report.

Table 39. Filters for access audit history report

Parameter	Description
Audit Report Type	Lists the audit type of reports. Select Access from the list.
Audit Start Date	Displays all audited actions and operations on an access approved from the specified date.
Audit End Date	Displays all audited actions and operations on an access approved until the specified date.
Access Business Unit	Displays the business unit that is associated with an access.
Access Name	Lists the names of all accesses that are available.

Table 39. Filters for access audit history report (continued)

Parameter	Description
Requestee Name	Displays the name for whom the access is requested.
Audit Action	Displays an action that is performed on an access. The supported audit actions are Add Member and Remove Member.
Approver	Displays the name of a user who approves the audit.
Approval Status	Displays the status of the approval. The supported approval statuses are Approved, Rejected, and Pending.

Account audit history report

Use this report to view the history of actions that are performed on an account.

After you select the values for the following parameters, the **Prompt Page Summary** is generated. The **Prompt Page Summary** provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Table 40. Filters for account audit history report

Parameter	Description
Audit Report Type	Lists the audit type of reports. Select Account from the list.
Audit Start Date	Displays all audited actions and operations on accounts approved from the specified date.
Audit End Date	Displays all audited actions and operations on accounts approved until the specified date.
Account Business Unit	Displays the business unit that is associated with an account.
Account Service Name	Displays the list of all the services that have one or more accounts provisioned.
Account Name	Displays the list of all the accounts that are created in an organization. If you want to generate an account audit report for all the accounts that are deleted, then do not provide any filter parameter.
Account Owner	Displays the user who owns one or more accounts in an organization.
Audit Action	Displays an action that is performed on a person or the business partner person. The supported audit actions are Add, Adopt, Delete, Orphan, Restore, Suspend, Synchronize Password, and Change Password.
Approver	Displays the name of a user who approves the audit.
Approval Status	Displays the status of the approval.

Entitlements Report

Use the report to view the list of services to which an individual is entitled. The report also lists all users and their entitlements.

After you select the parameter values, the **Prompt Page Summary** provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

<i>Table 41. Filters for Entitlements Report</i>	
Parameter	Description
Provisioning Policy	Displays the list of provisioning policies.
Entitlement	Displays the list of services to which a user is entitled.

After you generate the report, the provisioning policy definition lists the entitlements and configuration information about the members who are entitled to the provisioning policy.

All Users

All users in the organization who are entitled to the provisioning policy.

Roles

The roles whose members are entitled to the provisioning policy.

All Other Users

All other users who are not granted to the entitlements that are defined by this provisioning policy by way of other policies.

To drill-through information about the users and their entitlements, complete the following steps:

1. Click the link in the **Member** column to list all the members who are entitled to a service.
2. Click the link in the **User First Name** column to list all the entitlements that are granted for a specified user.

IBM Security Identity Manager Dashboard

A dashboard is a group of objects, such as charts, indicators, or tables. View the dashboard to access the detailed information about IBM Security Identity Manager environment.

The dashboard provides a quick summary about the IBM Security Identity Manager environment to an administrator or business user.

The dashboard shows information about the key activities and size metrics. It is more intended as the business side of an environment. For example, you can get a glance of how large is the IBM Security Identity Manager environment in your company.

The dashboard provides information about the following entities. You can specify the scope of the information that is displayed in the dashboard by using the available filters in some of the view types.

The dashboard requires that you map the attributes and entities of the following namespaces:

- Account Configuration
- Provisioning Policy Configuration
- User Configuration
- Service Audit (Entity Name Service)

See [“Mapping the attributes and entities” on page 860](#) for the details.

Environment Overview

This view shows the statistical chart of registered accounts, provisioning policies, resources, roles, separation of duty policy violations and users in the IBM Security Identity Manager environment. Information is presented in a block diagram.

Entity View

This view shows the statistical diagram and chart of managed users, managed resources, managed roles, and provisioning policy memberships for the selected business units. You select the business units that you want to view in the dashboard.

Account Status View

This view shows the statistical chart of non-compliant accounts, orphan accounts, suspended accounts, and disallowed accounts for the selected services. You select the services that you want to view in the dashboard.

Separation Of Duty Policy Violations

This view shows the statistical chart of violations in the organization for each Separation Of Duty policy.

Recertification Definition Report

Use the report to view the recertification policies and their schedule. These recertification policies are filtered by the recertification target type, policy name, and business unit.

You can generate the following types of subreports from the recertification definition report.

Subreport name	In the Recertification Target Type drop-down list
Access recertification definition report	Select Access .
Account recertification definition report	Select Account .
User recertification definition report	Select User .

After you select the values for the following parameters, the **Prompt Page Summary** is generated. The **Prompt Page Summary** provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Parameter	Description
Recertification Policy Business Unit	Displays the business unit.
Recertification Policy Name	Displays the name of the recertification policy.
Recertification Target Type	Displays the type of the recertification. The possible values are Access, Account, and User.

In the **Content** page, you can view the recertification policies that are filtered by the recertification target type, policy name, and business unit that you selected. You can view the configuration details by clicking the recertification policy name.

Separation of Duty Policy Definition Report

Use the report to list the separation of duty policies that are filtered by the policy name and business unit. The report provides information about the owners, rules, and roles that are associated with a separation of duty policy. An owner can be a person, role, or both.

After you select the parameter values, the **Prompt Page Summary** provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Parameter	Description
Separation of Duty Policy	Lists the names of the available separation of duty policies.
Business Unit	Lists the names of the available business units.

After you generate the report, the report page shows the separation of duty policy, business unit, and whether the policy is enabled or not.

Click the policy name to obtain details such as owners, rules, and roles that are associated with a separation of duty policy. An owner can be a person, role, or both.

Separation of Duty Policy Violation Report

This report contains the person, policy, and rules violated, approval, justification (if any), and who requested the violating change.

After you select the values for these parameters, the **Prompt Page Summary** is generated. The **Prompt Page Summary** provides information in tabular format about the selected parameters and their values.

The following table describes the parameters for filtering the report.

Parameter	Description
Separation of Duty Policy Business Unit	Displays the name of the business unit.
Separation of Duty Policy	Displays name of the separation of duty policy.
Separation of Duty Policy Rule Description	Displays the description of the rule name that is associated with the separation of duty policy.

Services Report

The report lists the services that are defined in IBM Security Identity Manager. The report can be filtered by the service business unit, service, and service owner.

After you select the parameter values, the **Prompt Page Summary** provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Parameter	Description
Service Business Unit	Lists the business units of the services.
Service	Displays the list of all the services that are defined in the IBM Security Identity Manager.
Service Owner	Lists the owners of the services.

User Access Report

The User Access Report provides information about the different users in a business unit and their access. The user is entitled to at least one access.

You can generate the following types of subreports from the User Access Report.

Subreport name	In the Report Type list
User Access Report - View by Access	Select View by Access . For more information about the report parameters and their descriptions, see “View by Access” on page 793 .
User Access Report - View by User	Select View by User . For more information about the report parameters and their descriptions, see “View by User” on page 793 .

You must define the base icon URL path in the query of the User Access Report to display the icons in the report. For more information, see [“Defining the base icon URL path” on page 794](#).

View by Access

With this report type, the **User Access Report** focuses on the list of all access. You have the option to view the corresponding user for the selected access.

The following table describes the parameters for filtering the report.

Parameter	Description
Access Name	Displays the list of accesses for which you want to generate a report.
Access Search Terms	Displays the list of search terms that are defined for an access.
Access Badge Text	Displays the description about the badge that is defined for an access.
Access Type	Displays the type of an access. The type of an access can be a role, an application, a shared folder, an email group, or a custom access that is defined in an organization.

Select the values for these parameters, then click **Finish** to generate the report.

The **Prompt Page Summary** provides an overview of the report parameters and the selected values. The next page lists all of the access that you filtered, with their details.

Click the *Access Name* link to view the corresponding user of the selected access. Information about the user such as user type and business unit is provided.

View by User

With this report type, the **User Access Report** focuses on the list of users per business unit. You have the option to view all access corresponding to each of these users.

The following table describes the parameters for filtering the report.

Parameter	Description
User Business Unit	Displays the list of user business units, for which you want to generate a report.
User Profile Type	Displays the profile type of the user with defined access on Role, Group, or Service.
User Name	Displays the full name of the user from a business unit.

Select the values for these parameters, then click **Finish** to generate the report.

The **Prompt Page Summary** provides an overview of the report parameters and the selected values. The next page lists all of the users that you filtered, with their details and sorted based on their business unit.

Click the *User Name* link to view all access corresponding to the selected user.

User Recertification History Report

Use this report to view the recertification history for a user. This report covers the recertification audit history of accounts, groups, and roles that are associated with the user.

After you select the values for these parameters, the **Prompt Page Summary** is generated. The **Prompt Page Summary** provides information about the selected parameters and their values in a table.

The following table describes the parameters for filtering the report.

Table 50. Filters for User Recertification History Report

Parameter	Description
Start Date	Displays the start date of user recertification history.
End Date	Displays the end date of user recertification history.
User Recertification Policy	Displays information about the user recertification policy.
User Business Unit	Displays the business unit name of a user.
User	Displays the user from a business unit.
User Status	Displays status of the user to be selected.
Recertifier	Displays user to be selected as recertifier.


Defining the base icon URL path

You must define the base icon URL path in query of the Access Definition Report or User Access Report to display the icon in the report.

About this task

IBM Security Identity Manager provides a way to define an icon URL for an access. The icon URL can be either a relative path or an absolute path. Assume that a user defined the icon URL "/images/icons/test.gif" in IBM Security Identity Manager. To display the actual image for the icon URL, IBM Cognos application must locate the full path for that image. In such a situation, you must define the base icon URL path in the query of the access definition report.

Procedure

1. Open the report in **Report Studio**.
 - a) Access `https://hostname:port/bi/v1/disp`.
 - b) In **IBM Cognos Team Content** window, click **ISIMReportingModel_6.0.x.x**.
 - c) Select the report, which is applicable.
 - **Access Definition Report** or
 - **User Access Report**
 - d) Click **...**, then click **Edit**.
The report opens.
2. Click **Queries** .
3. Double-click **Access Query**.
4. In the **Data Items** window, double-click **Base Icon URL**.
5. In the **Expression Definition** window, set the base URL for the icons.
For example, 'http://example.com'.
6. Click **OK**.
7. Save the report.

What to do next

Run the report to display the icons.

Query subjects and query items for the report models

Use the query subjects and query items information to customize the IBM Security Identity Manager reports.

Schema mapping

Before you work with the query subjects and query items, you must map the attributes to the entities.

For more information, see [“Report schema mapping”](#) on page 882.

To map the attributes and entities, see [“Mapping the attributes and entities”](#) on page 860.

Recertification Audit namespace

The Recertification Audit namespace provides information about the history of user, role, account, and group recertification.

Query subjects for Recertification Audit namespace

The following table lists the query subjects in the Recertification Audit namespace.

Query subject	Description
User Recertification Policy	Represents the recertification policy that recertifies accounts, group memberships, and roles memberships through user recertification. IBM Security Identity Manager entities are recertified with the recertification policy. You must use this query subject with the User Recert History query subject to obtain information about the recertification policy. Do not use this query subject with Account Recert History and Access Recert History.
User Recert History	Represents the recertification audit history for a user. It covers recertification audit history of accounts, groups, and roles that are associated with the user.
Person	Represents a user entity and some of its configuration attributes. You must use this query subject with the User Recert History query subject to obtain information about the user that is being recertified.
Person Organization	Represents an organization that is associated with a user. These users are being recertified.
User Recert Account	Represents the recertification audit history for an account that is recertified as part of the user recertification. You must use this query subject with the User Recert History. By doing so, you can obtain the information about accounts that are associated with the users that are being recertified.
User Recert Group	Represents the recertification audit history for a group membership that is recertified as part of the user recertification. You must use this query subject with the User Recert History. By doing so, you can obtain the information about memberships of the accounts that are associated with the users that are being recertified.
User Recert Group Service	Represents the service that is associated to a group. You must use this query subject with the User Recert History to obtain more information about the service for the groups that are recertified as a part of the user recertification.
User Recert Role	Represents the recertification audit history for a role membership that is recertified as part of the user recertification. You must use this query subject with the User Recert History. By doing so, you can obtain the information about role memberships of the users that are being recertified.
Account	Represents an account entity and some of its configuration attributes. You must use this query subject with the Account Recert History query subject. By doing so, you can generate recertification history reports of accounts.
Account Service	Represents service that is associated to an account. These accounts participate in the account and access recertification.
Account Owner	Represents user owners of the accounts that are participating in the account and access recertification.
Account Recert History	Represents the recertification audit history for accounts. You must use this query subject with the Account query subjects. By doing so, you can find out the accounts in the recertification audit.

Table 51. Query subjects in the Recertification Audit namespace for the recertification model (continued)

Query subject	Description
Access	Represents the group access and some of its configuration attributes. You must use this query subject with the Access Recert History query subject to generate recertification history reports of access.
Access Recert History	Represents the recertification audit history for access. You must use this query subject with the Access query subjects. By doing so, you can find out the accesses in the recertification audit.

Query items for Recertification Audit namespace

The following table lists the query items in the Recertification Audit namespace.

Table 52. Query items in the Recertification Audit namespace

Query subject	Query items and their description
User Recertification Policy	<p>Recertification Policy Name The name of the recertification policy.</p> <p>Recertification Policy Type The type of an entity that gets recertified by using this policy. The valid values are Account, Access, and Identity.</p> <p>Recertification Policy Description The description of the policy as specified in the policy configuration.</p> <p>Recertification Policy Enabled Shows whether the policy is enabled.</p> <p>Recertification Policy Scheduled The recertification scheduling modes. The valid values are CALENDAR and ROLLING.</p> <p>Recertification Policy Rolling Interval in Days The recertification period if the recertification policy scheduling mode is ROLLING. No value in this query item indicates that the scheduling is not in the ROLLING mode.</p> <p>Recertification Policy Reject Action An action that was taken if the recertification is rejected.</p> <p>Recertification Policy Timeout Period in Days The duration during which a recertifier must act.</p> <p>Recertification Policy Timeout Action The automatic action that must be taken if the recertification times out.</p> <p>Recertification Policy DN An LDAP distinguished name for the recertification policy.</p> <p>Recertification Policy Container DN An LDAP distinguished name for a business unit to which the recertification policy applies.</p> <p>Recertification Policy Is Custom Indicates whether the recertification policy is customized. It is defined in the workflow.</p> <p>Recertification Policy User Class The type of a user to which the recertification policy applies. The valid values are All, Person, and Business Partner Person.</p> <p>Recertification Policy Scope Indicates whether the recertification policy applies to the business unit and its subunits or either of them.</p>

Table 52. Query items in the Recertification Audit namespace (continued)

Query subject	Query items and their description
<p>User Recert History</p>	<p>User Recert History Person Name The full name of a person.</p> <p>User Recert History Person Email The user email identifier.</p> <p>User Recert History Person Status A user status at the end of the recertification workflow process. The valid values are Active and Inactive.</p> <p>User Recert History Person Business Unit Name A business unit to which a user belongs.</p> <p>User Recert History Recertification Policy Name The recertification policy that created a user entity.</p> <p>User Recert History Timeout Shows whether the recertification process is timed out or not. 0 represents Not timed out, and 1 represents Timed out.</p> <p>User Recert History Comments The comments that are entered by a user during the user recertification process.</p> <p>User Recert History Process Comments The comments that are entered by a user during the recertification process.</p> <p>User Recert History Process Submission time The recertification policy submission time.</p> <p>User Recert History Process Start Time The time at which user recertification workflow process was started.</p> <p>User Recert History Process Completion Time A user recertification history process completion time.</p> <p>User Recert History Process Last Modified Time The time at which user recertification workflow process was last modified.</p> <p>User Recert History Process Requester Name The name of a user who submitted the request for recertification.</p> <p>User Recert History Process Requestee Name The name of a user entity for whom the request for recertification was submitted.</p> <p>User Recert History Process Recertifier Name The name of a user who is the final approver in the recertification workflow process.</p> <p>User Recert History Process Result Summary An overall summary of a user recertification workflow process result.</p> <p>User Recert History Process Scheduled The schedule for recertification policy submission.</p> <p>User Recert History Id A unique ID assigned by the IBM Security Identity Manager to a user recertification audit history.</p> <p>User Recert History Person DN An LDAP distinguished name for a user entity in the recertification process.</p> <p>User Recert History Recertification Policy DN An LDAP distinguished name for the recertification policy that recertifies a user entity.</p>
<p>Person</p>	<p>Person Full Name The full name of a user.</p> <p>Person Last Name The surname of a user.</p> <p>Person Status The status of a user.</p> <p>Person Dn An LDAP distinguished name for a user entity.</p> <p>Person Business Unit Dn An LDAP distinguished name for a business unit to which a user belongs.</p> <p>Person Supervisor The name of a user who is the supervisor of a user entity.</p>

Table 52. Query items in the Recertification Audit namespace (continued)

Query subject	Query items and their description
Person Organization	<p>Business Unit Name The name of a business unit to which a user belongs.</p> <p>Business Unit Supervisor A user supervisor of a business unit.</p> <p>Business Unit DN An LDAP distinguished name for the business unit to which a user belongs.</p> <p>Business Unit Container DN An LDAP distinguished name for the parent business unit of an organization entity.</p>
User Recert Account	<p>User Recert Account Name The name of an account in a user recertification.</p> <p>User Recert Account Service Name The name of a service to which an account belongs.</p> <p>User Recert Account Service Description Describes the service that is associated to an account.</p> <p>User Recert Account Status The status of an account at the end of the recertification. The valid values are Approved and Rejected.</p> <p>User Recert Account Recert Id A unique numeric ID assigned by the IBM Security Identity Manager to an account recertification.</p> <p>User Recert Account DN An LDAP Distinguished name for an account entity in the recertification.</p> <p>User Recert Account Service DN An LDAP Distinguished name for the service to which an account entity belongs.</p>
User Recert Group	<p>User Recert Group Name The name of a group in the user recertification.</p> <p>User Recert Group Description Describes the recertification group.</p> <p>User Recert Group Status The status of a group at the end of the recertification. The valid values are Approved and Rejected.</p> <p>User Recert Group Recert Id A unique numeric ID assigned by IBM Security Identity Manager to a group recertification.</p> <p>User Recert Group DN An LDAP Distinguished name for a group entity in the recertification.</p>
User Recert Group Service	<p>Group Name The name of a group.</p> <p>Service Name The name of a service to which the group belongs.</p> <p>Service Type The service profile type.</p> <p>Service Url A URL that connects to the managed resource.</p> <p>Service DN An LDAP distinguished name for a service to which the group belongs.</p> <p>Service Container Dn An LDAP distinguished name for a business unit of the service that is associated with a group.</p> <p>Service Owner Dn An LDAP distinguished name for a user owner of the service.</p> <p>Group Dn An LDAP distinguished name for a group entity in the recertification.</p>

Table 52. Query items in the Recertification Audit namespace (continued)

Query subject	Query items and their description
User Recert Role	<p>User Recert Role Name The name of a role in the user recertification.</p> <p>User Recert Role Description The description of a role.</p> <p>User Recert Role Status The status of a role at the end of the recertification. The valid values are Approved and Rejected.</p> <p>User Recert Role Recert Id A unique numeric identifier that is assigned by IBM Security Identity Manager to a role recertification.</p> <p>User Recert Role DN An LDAP Distinguished name for a role entity in the recertification.</p>
Account	<p>Account Name The name of an account.</p> <p>Account Service Dn An LDAP distinguished name for a service that provisions an account.</p> <p>Account Status The status of an account. The valid values are Active and Inactive.</p> <p>Account Compliance The details about an account compliance. The valid values are Unknown, Compliant, Non Compliant, and Disallowed.</p> <p>Account Ownership Type The ownership type of an account. The valid values are Individual, System, Device, and Vendor.</p> <p>Account Last Access Date The last date when an account was accessed.</p> <p>Account Container Dn An LDAP distinguished name for a business unit to which an account belongs.</p>
Account Service	<p>Service Name The name of a service to which an account belongs.</p> <p>Service Dn An LDAP distinguished name for a service to which an account belongs.</p> <p>Service Container DN An LDAP distinguished name for a business unit of a service that is associated to the accounts.</p> <p>Service Owner DN An LDAP distinguished name for a user owner of the service.</p> <p>Service Url A URL that connects to the managed resource.</p> <p>Service Type The service profile type.</p>
Account Owner	<p>Person Full Name The full name of a user who owns an account.</p> <p>Person Last Name The surname of a user who owns an account.</p> <p>Person Status The status of a user who owns an account.</p> <p>Person DN An LDAP distinguished name for an account owner.</p> <p>Person Business Unit DN An LDAP distinguished name for a business unit that is associated to an account owner.</p> <p>Person Supervisor The supervisor of an account owner.</p>

Table 52. Query items in the Recertification Audit namespace (continued)

Query subject	Query items and their description
<p>Account Recert History</p>	<p>Recert History Service Name The name of a service to which accounts and groups belong. These accounts and groups are involved with an account recertification audit.</p> <p>Recert History Service Profile The profile type of a service.</p> <p>Recert History Status An account status at the end of the recertification workflow process. The valid values are Abort, Approved, Timeout, Pending, and Rejected.</p> <p>Recert History Action The action that is taken on an account at the end of recertification process as defined by the recertification policy. The valid values are Abort, Certify, Delete, Mark, Certify Administrative, and Suspend.</p> <p>Recert History Comments The comments that are entered by a user during recertification process.</p> <p>Recert History Process Start Time The time at which an account recertification workflow process started.</p> <p>Recert History Process Submission Time The time at which recertification policy was submitted.</p> <p>Recert History Process Completion Time The time at which an account recertification workflow process completed.</p> <p>Recert History Process Last Modified Time The last modified time for an account recertification workflow process.</p> <p>Recert History Process Comments The comments that are entered by a user during recertification process.</p> <p>Recert History Process Result Summary The summary of the recertification process result. The valid values are Success, Failed, Pending, Escalated, Skipped, Timeout, and Warning.</p> <p>Recert History Process Requestee Name The name of a user entity for whom the recertification request is submitted. For example, if the entity for recertification is an account, then the query item is the name of the account.</p> <p>Recert History Process Requester Name The name of a user who submitted the recertification request. For example, if administrator submits a request for recertification, then this query item is the name of the administrator.</p> <p>Recert History Recertifier Name The name of a user who is the final approver in the recertification workflow process.</p> <p>Recert History Activity Owner An owner of recertification activity for an account.</p> <p>Recert History Recertifier Id An account identifier of the recertifier.</p>
<p>Access</p>	<p>Group ID An identifier for a group.</p> <p>Group Name The name of a group for which an access is defined.</p> <p>Group Type The profile type of a group.</p> <p>Group Access Name The name of the access that is defined for a group.</p> <p>Group Access Type The type of the access that is defined for a group.</p> <p>Group DN An LDAP distinguished name for a group entity for which an access is defined.</p> <p>Group Container DN An LDAP distinguished name for a business unit that is associated with a group.</p> <p>Group Service DN An LDAP distinguished name for the service that is associated to a group.</p>

Table 52. Query items in the *Recertification Audit* namespace (continued)

Query subject	Query items and their description
Access Recert History	<p>Recert History Service Name The name of a service to which accesses and groups belong. These accesses and groups are involved with an access recertification audit.</p> <p>Recert History Service Profile The profile type of a service.</p> <p>Recert History Status An access status at the end of the recertification workflow process. The valid values are Abort, Approved, Timeout, Pending, and Rejected.</p> <p>Recert History Action The action that is taken on an access at the end of recertification process as defined by the recertification policy. The valid values are Abort, Certify, Delete, Mark, Certify Administrative, and Suspend.</p> <p>Recert History Comments The comments that are entered by a user during recertification process.</p> <p>Recert History Process Start Time The time at which an access recertification workflow process started.</p> <p>Recert History Process Submission Time The time at which recertification policy was submitted.</p> <p>Recert History Process Completion Time The time at which an access recertification workflow process completed.</p> <p>Recert History Process Last Modified Time The last modified time for an access recertification workflow process.</p> <p>Recert History Process Comments The comments that are entered by a user during recertification process.</p> <p>Recert History Process Result Summary The summary of the recertification process result. The valid values are Success, Failed, Pending, Escalated, Skipped, Timeout, and Warning.</p> <p>Recert History Process Requestee Name The name of a user entity for whom the recertification request is submitted. For example, if the entity for recertification is an access, then the query item is the name of the access.</p> <p>Recert History Process Requester Name The name of a user who submitted the recertification request. For example, if administrator submits a request for recertification, then this query item is the name of the administrator.</p> <p>Recert History Recertifier Name The name of a user who is the final approver in the recertification workflow process.</p> <p>Recert History Activity Owner An owner of recertification activity for an access.</p> <p>Recert History Recertifier Id An access identifier of the recertifier.</p>

Recertification Config namespace

The Recertification Config namespace provides information about the defined recertification policies and target that is defined for those policies.

Query subjects for Recertification Config namespace

The following table lists the query subjects in the Recertification Config namespace.

Table 53. Query subjects in the *Recertification Config* namespace

Query subject	Description
Recertification Policy	Represents the recertification policy and its components.
Recertification Policy Schedule	Represents the schedule that is used to auto trigger the recertification policy.
Policy Recertifier	Represents a user who is a recertifier for the recertification policy.
Recert Policy Business Unit	Represents a business unit to which the recertification policy applies.

Table 53. Query subjects in the *Recertification Config* namespace (continued)

Query subject	Description
Recert Policy Role Target	Represents the roles that are recertified by the recertification policy. You must use this query subject with the <i>Recertification Policy</i> to obtain information about the roles that are certified and their configuration attributes.
Recert Policy Access Target	Represents a group access and group membership that are recertified by the recertification policy. You must use this query subject with the <i>Recertification Policy</i> to obtain information about: <ul style="list-style-type: none"> • Group access • Group membership • Configuration attributes of group access and group membership • Informative attributes of a service that are associated with a group
Recert Policy Access Owner	Represents a group access owner that are recertified by the recertification policy. You must use this query subject with the <i>Recertification Policy</i> to obtain information about the group access owner name.
Group Members	Represents the information about the members of a recertified group. You must use this query subject with the <i>Recert Policy Access Target</i> to obtain information about the members of the recertified group.
Recert Policy Account Target	Represents a service on which the accounts are provisioned and recertified by the recertification policy. You must use this query subject with the <i>Recertification Policy</i> to obtain more information about: <ul style="list-style-type: none"> • Account recertified • Service on which these accounts are provisioned
Account	Represents account entity and some of its configuration attributes. You must use this query subject with the <i>Recert Policy Account Target</i> to obtain more information about the accounts that are associated with the service.
Person	Represents a user entity and some of its configuration attributes. You must use this query subject with the <i>Recert Policy Role Target</i> query subject to obtain more information about the members of the role.
Account Owner	Represents a user owner of an account. You must use this query subject with the <i>Account</i> query subject to obtain information about the owners of the accounts.

Query items for Recertification Config namespace

The following table lists the query items in the Recertification Config namespace.

Query subject	Query items and their description
Recertification Policy	<p>Recertification Policy Name The name of the recertification policy.</p> <p>Recertification Policy Type The type of an entity that gets recertified by using this policy. The valid values are User, Account, and Access.</p> <p>Recertification Policy Description The policy description as specified in the policy configuration.</p> <p>Recertification Policy Enabled Shows whether the policy is enabled or not.</p> <p>Recertification Policy Scheduled The recertification scheduling modes. The valid values are CALENDAR and ROLLING.</p> <p>Recertification Policy Rolling Interval in Days The recertification period if the recertification policy scheduling mode is ROLLING. No value in this query item indicates that the scheduling is not in the ROLLING mode.</p> <p>Recertification Policy Reject Action An action that is taken if the recertification is rejected.</p> <p>Recertification Policy Timeout Period in Days The duration during which a recertifier must act.</p> <p>Recertification Policy Timeout Action An automatic action that must be taken if the recertification times out.</p> <p>Recertification Policy DN An LDAP distinguished name for the recertification policy.</p> <p>Recertification Policy Container DN An LDAP distinguished name for a business unit to which the recertification policy applies.</p> <p>Recertification Policy Is Custom Represents whether the recertification policy is customized. It is defined in the workflow.</p> <p>Recertification Policy User Class The type of a user to which the recertification policy applies. The valid values are All, Person, and Business Partner Person.</p> <p>Recertification Policy Scope Indicates whether the recertification policy applies to the business unit and its subunits or either of them.</p>

Table 54. List of query items in the Recertification Config namespace (continued)

Query subject	Query items and their description
<p>Recertification Policy Schedule</p>	<p>Recertification Policy Detailed Schedule The recertification schedule in terms of the units of time.</p> <p>Note: Do not use this query item with Oracle database. This query item is supported only for DB2 database.</p> <p>Recertification Policy Schedule The schedule that automatically triggers the recertification policy. The query item represents the schedule in the numeric format. The format of the schedule is Minute Hours Month DayOfWeek DayOfMonth DayOfQuarter DayOfSemiAnnual. For example, 0 0 0 0 -1 0 0.</p> <ul style="list-style-type: none"> • Minute - Represents the time in minutes. • Hours - Represents the time in hours. -1 indicates that the recertification policy is applied every hour. • Month - Represents the month for the recertification. 1 represents January, 2 represents February, and so on. -1 indicates that the recertification policy is applied every month. • DayOfWeek - Represents the day of a week. 1 represents Sunday, 2 represents Monday, and so on. The positive value indicates that policy is applied weekly on a specific day. -1 indicates that the recertification policy is not applied based on the day of a week. • DayOfMonth - Represents the date. -1 indicates that the recertification policy is applied daily. • DayOfQuarter - Represents the number of days after the start of each quarter. 0 indicates that the policy is not applied quarterly. • DayOfSemiAnnual - Represents the number of days after the start of each half year. 0 indicates that the policy is not applied semi-annually. • The policy is applied annually if the value of Month and DayOfMonth is positive. <p>Recertification Policy DN An LDAP distinguished name for the recertification policy.</p>
<p>Policy Recertifier</p>	<p>Recertifier Type The type of the recertifier. The valid values and their meanings:</p> <ul style="list-style-type: none"> • Account Owner: User being recertified <p>Note: This meaning applies only for the recertification policies that are related to the users. For all other recertification policies, Account Owner is an owner of the account.</p> <ul style="list-style-type: none"> • System Administrator: Administrator • Manager: Manager • Person: Specified user • Role: Specified organizational role • System Role: Specified group <p>Recertifier Name The name of a specific user, role, or group that is defined as an approver of the recertification. When the recertification policy's recertifier is set to User being recertified, then the Recertifier Name is shown as a blank.</p> <p>Recert Policy Dn An LDAP distinguished name for the recertification policy.</p>
<p>Recert Policy Business Unit</p>	<p>Business Unit Name The name of a business unit.</p> <p>Business Unit Supervisor The user supervisor of a business unit.</p> <p>Business Unit Dn An LDAP distinguished name for a business unit.</p> <p>Business Unit Container DN An LDAP distinguished name for the parent organization of a business unit entity.</p>

Table 54. List of query items in the Recertification Config namespace (continued)

Query subject	Query items and their description
<p>Recert Policy Role Target</p>	<p>Role Name The name of the role. If the policy applies to all the roles in a business unit, then ALL ROLES WITHIN POLICY ORGANIZATION is displayed.</p> <p>Role Description The description of a role.</p> <p>Role Type The type of a role. The valid values are Static and Dynamic. The value of a role type is empty if the role name is mentioned as ALL ROLES WITHIN POLICY ORGANIZATION.</p> <p>Role Business Unit Name The business unit to which the role belongs.</p> <p>Role Business Unit Supervisor The user supervisor of a business unit to which the role belongs.</p> <p>Role DN An LDAP distinguished name for the role.</p> <p>Role Business Unit DN An LDAP distinguished name for the business unit to which role belongs.</p> <p>Recert Policy Dn An LDAP distinguished name for the recertification policy.</p>
<p>Recert Policy Access Target</p>	<p>Group Name The name for a group. If the policy applies to all the groups in an organization, then ALL GROUPS WITHIN POLICY ORGANIZATION is displayed. If the policy applies to all the groups for a service, then ALL GROUPS ON A SPECIFIED SERVICE is displayed.</p> <p>Group Description The description of a group.</p> <p>Group Type The profile type of a group.</p> <p>Group Access Name An access name that is defined for a group entity.</p> <p>Group Access Description The description of an access that is defined for a group entity.</p> <p>Group Access Type The type of an access that is defined for a group entity.</p> <p>Group Service Name The name of a service on which the group is provisioned.</p> <p>Group Dn An LDAP distinguished name for a group.</p> <p>Group Service DN An LDAP distinguished name for the service on which a group is provisioned.</p> <p>Group Container DN An LDAP distinguished name for an organization to which a group belongs.</p> <p>Group Service Container Dn An LDAP distinguished name for an organization of the service on which group is provisioned.</p> <p>Recert Policy DN An LDAP distinguished name for the recertification policy.</p>
<p>Recert Policy Access Owner</p>	<p>Group Dn An LDAP distinguished name for a group.</p> <p>Group Access Owner Dn An LDAP distinguished name for an access owner that is defined for a group entity.</p> <p>Group Access Owner Full Name Full name of an access owner that is defined for a group entity.</p>

Table 54. List of query items in the Recertification Config namespace (continued)

Query subject	Query items and their description
<p>Group Members</p>	<p>Account Name The name of an account that is associated with a credential.</p> <p>Account Service Dn An LDAP distinguished name for a service that provisions an account.</p> <p>Account Status The status of an account that indicates whether the account is active or inactive.</p> <p>Account Compliance The details about an account compliance. The valid values are Unknown, Compliant, Non Compliant, and Disallowed.</p> <p>Account Ownership Type The ownership type of the account. The valid values are Individual, System, Device, and Vendor.</p> <p>Account Last Access Date The last accessed date and time of an account.</p> <p>Account Container Dn An LDAP distinguished name for a business unit of an account.</p>
<p>Recert Policy Account Target</p>	<p>Account Service Name The name of the service. If the policy applies to all the accounts in the service, then ALL ACCOUNT WITHIN POLICY ORGANIZATION is displayed.</p> <p>Account Service Business Unit Name The name of the business unit to which a service belongs.</p> <p>Account Service Business Unit Supervisor A user supervisor of a business unit that is associated with the service.</p> <p>Account Service DN An LDAP distinguished name for the service.</p> <p>Account Service Description The description of a service.</p> <p>Account Service Business Unit DN An LDAP distinguished name for a business unit that is associated with the service.</p> <p>Account Service Type The profile type of the service.</p> <p>Account Service Owner DN An LDAP distinguished name for an owner of the service.</p> <p>Account Service Url A URL that connects to the service.</p> <p>Recert Policy DN An LDAP distinguished name for the recertification policy.</p>
<p>Account</p>	<p>Account Name The name of an account that is associated with a credential.</p> <p>Account Service Dn An LDAP distinguished name for a service that provisions an account.</p> <p>Account Status The status of an account that indicates whether the account is active or inactive.</p> <p>Account Compliance The details about an account compliance. The valid values are Unknown, Compliant, Non Compliant, and Disallowed.</p> <p>Account Ownership Type The ownership type of the account. The valid values are Individual, System, Device, and Vendor.</p> <p>Account Last Access Date The last accessed date and time of an account.</p> <p>Account Container Dn An LDAP distinguished name for a business unit of an account.</p>

Table 54. List of query items in the *Recertification Config* namespace (continued)

Query subject	Query items and their description
Person	<p>Person Full Name The full name of a user.</p> <p>Person Last Name The surname of a user.</p> <p>Person Status The status of a user.</p> <p>Person Dn An LDAP distinguished name for a user entity.</p> <p>Person Business Unit Dn An LDAP distinguished name for a business unit to a user entity.</p> <p>Person Supervisor The name of a user for the supervisor of a user entity.</p>
Account Owner	<p>Person Full Name The full name of a user who owns an account.</p> <p>Person Last Name The surname of a user who owns an account.</p> <p>Person Status The status of a user.</p> <p>Person Dn An LDAP distinguished name for a user entity.</p> <p>Person Business Unit Dn An LDAP distinguished name for a business unit to a user entity.</p> <p>Person Supervisor The name of a user for the supervisor of a user entity.</p>

Account Audit namespace

The `Account Audit` namespace pertains to the audit history of the accounts. This namespace contains query subjects that are related to the audit of accounts, reconciliation, and provisioning policy.

Use the account audit model and reports to view the details about the accounts that are associated with a user.

Note: If the account is on the service that is defined as an access, the audit details can be seen only in the `Access Audit` namespace.

Query subjects for Account Audit namespace

The following table lists the query subjects in the `Account Audit` namespace.

Query subject	Description
Account Audit	Represents the audit history for the account entities.
Account	Represents an account entity on which the audit actions are performed. This query subject contains configuration and other attributes that represent the status of the account. You must use this query subject with the <code>Account Audit</code> , <code>Reconciliation Audit</code> , and <code>Provisioning Policy</code> to obtain information about the accounts audit actions and provisioning operations.
Reconciliation Audit	Represents the audit history that is associated with the reconciliation operations.
Provisioning Policy	Represents the provisioning policies and their configuration attributes.

Query items for Account Audit namespace

The following table lists the query items in the Account Audit namespace.

Query subject	Query items and their description
Account Audit	<p>Audit Account Name The name of an account on which the audit action is performed.</p> <p>Audit Action The action that is performed on an account. For example, Add, Delete, Modify, and ChangePassword.</p> <p>Audit Comments The comments that are entered by the audit workflow approver.</p> <p>Audit Account Business Unit The business unit of an account.</p> <p>Audit Process Subject A user who is the owner of an account on which the audit action is performed.</p> <p>Audit Process Service Profile The profile type of a service to which an account belongs.</p> <p>Audit Process Subject Service The service on which an account is provisioned.</p> <p>Audit Initiator Name The name of a user who initiated the audit action.</p> <p>Audit Process Requestee Name The name of an account owner.</p> <p>Audit Process Recertifier Name The name of a user who approves the audit process workflow.</p> <p>Audit Operation Start Time The audit operation initiation date and time.</p> <p>Audit Activity Owner An owner who owns the activity. For example, An owner name who approves the add request for the pending account.</p> <p>Audit Activity Name The name of the audit activity.</p> <p>Audit Activity Start Time The audit activity start date and time.</p> <p>Audit Activity Completion Time The audit activity completion date and time.</p> <p>Audit Process Submission Time The audit process submission date and time.</p> <p>Audit Process Schedule Time The date and time at which an event is scheduled for execution.</p> <p>Audit Process Completion Time The audit process completion date and time.</p> <p>Audit Activity Result Summary The result of the activity within the account audit process.</p> <p>Audit Process Result Summary The result of the account audit process.</p>

Table 56. Query items in the Account Audit namespace (continued)

Query subject	Query items and their description
<p>Account</p>	<p>Account Name The name of an account on which the audit action is performed.</p> <p>Account Service Name The name of a service on which the account is provisioned.</p> <p>Account Status The account status. The valid values are Active and Inactive.</p> <p>Account Is Orphan Indicates whether an account is associated with a user or not. The valid values are Yes and No. Yes represents the account is orphaned, and No represents the account is not orphaned.</p> <p>Account Compliance Indicates whether an account is compliant or not. The valid values are Compliant, Non compliant, Unknown, and Disallowed.</p> <p>Account Last Access Date The last accessed date and time of an account.</p> <p>Account Owner First Name The given name of a user who is the owner of an account.</p> <p>Account Owner Last Name The surname of a user who is the owner of an account.</p> <p>Account Dn An LDAP distinguished name for an account.</p> <p>Account Service DN An LDAP distinguished name for the service to which an account belongs.</p> <p>Account Owner Business Unit Dn An LDAP distinguished name for the business unit to which an account owner belongs.</p> <p>Account Owner Dn An LDAP distinguished name for the account owner.</p>

Table 56. Query items in the Account Audit namespace (continued)

Query subject	Query items and their description
Reconciliation Audit	<p>Reconciliation User Name The name of a user to whom an account is associated during the reconciliation operation.</p> <p>Reconciliation Account Name The name of the reconciled account.</p> <p>Reconciliation Processed Accounts The number of processed accounts that exist during the last run of reconciliation.</p> <p>Reconciliation TIM User Accounts The number of processed accounts that belong to IBM Security Identity Manager users.</p> <p>Reconciliation Local Accounts The total number of local accounts created. It does not include the newly created orphan accounts.</p> <p>Reconciliation Policy Violations The number of policy violations that are found for the accounts during the reconciliation. This number includes:</p> <ul style="list-style-type: none"> • The accounts where an attribute value is different from the local account. • Any attribute value of the account is not compliant with the governing provisioning policies. <p>It does not include the accounts where the attribute values of the local and remote accounts are same, even if the values are noncompliant.</p> <p>Reconciliation Start Time The reconciliation operation initiation date and time.</p> <p>Reconciliation Completion Time The reconciliation operation completion date and time.</p> <p>Reconciliation Policy Compliance Status The reconciliation completion status.</p> <p>Reconciliation Operation The operation that is performed for the entry of the service instance. The possible values for an account entry are New Local, New Orphan, Suspended Account, and Deprovisioned Account.</p> <p>Reconciliation Requester Name The name of an initiator who initiates the reconciliation operation on the account for a service.</p>
Provisioning Policy	<p>Provisioning Policy Name The name of a provisioning policy through which an account is provisioned on the service.</p> <p>Provisioning Policy Dn An LDAP distinguished name for the provisioning policy.</p> <p>Provisioning Policy Container Dn An LDAP distinguished name for the business unit to which the provisioning policy applies.</p> <p>Provisioning Policy Service Name The name of a service to which the provisioning policy applies.</p> <p>Provisioning Policy Service Type The profile type of a service to which the provisioning policy applies.</p> <p>Provisioning Policy Service Business Unit Name The business unit of a service to which the provisioning policy applies.</p>

Account Configuration namespace

The Account Configuration namespace contains the query subjects and query items for configuring the accounts.

Query subjects for Account Configuration namespace

The following table lists the query subjects in the Account Configuration namespace.

Table 57. Query subjects in the Account Configuration namespace	
Query subject	Description
Account	Represents an account entity and its configuration attributes. The query subject also contains the detailed information about the service to which the account belongs.

Table 57. Query subjects in the Account Configuration namespace (continued)

Query subject	Description
Account Owner	Represents a user who owns an account. You must use this query subject with the Account query subject to obtain information about the accounts that are managed by the user.
Account Owner Role Membership	Represents the role information. You must use this query subject with the Account Owner query subject to obtain information about the role membership of the account owners.
Group	Represents the group access and some of its configuration attributes. You must use this query subject with the Account query subject to obtain information about the account members of a group.
Service Business Unit	Represents the business unit to which a service belongs. You must use this query subject with the Account query subject to obtain information about the business unit where the service is located.
Credential	Represents a credential for an account. You must use this query subject with the Account query subject to obtain information about the credential and its configuration attributes.
Credential Pool	Represents a pool of credentials for an account. You must use this query subject with the Account query subject to obtain information about the credential pool and its configuration attributes.
Account ACI	Represents the Access Control Item (ACI) that are applicable on the accounts. You must use this query subject with the Account query subject to obtain information about the accounts that are managed by an ACI.
ACI Operations	Represents the operations that are governed by an ACI. You must use this query subject with the Account ACI query subject to obtain information about an ACI associated with the account.
ACI Attribute Permissions	Represents the attributes and operations that can be performed on an attribute. You must use this query subject with the Account ACI query subject to obtain information about an ACI associated with the account.
Identity Policy	Represents the identity policy and its configuration attributes. You must use this query subject with the Account query subject to obtain information about the accounts that are managed by the policy.
Provisioning Policy	Represents the provisioning policy and some of its configuration attributes. You must use this query subject with the Account query subject to obtain information about the policy that provisioned the account.
Recertification Policy	Represents the recertification policy and some of its configuration attributes. You must use this query subject with the Account query subject to obtain information about the accounts that are recertified by the policy.
Password Policy	Represents the password policy and its configuration attributes. You must use this query subject with the Account query subject to obtain information about the accounts that are managed by the policy.

Query items for Account Configuration namespace

The following table lists the query items in the Account Configuration namespace.

Query subject	Query items and their description
Account	<p>Account Name The name of an account.</p> <p>Account Status An account status. The valid values are Active and Inactive.</p> <p>Account Compliance Indicates whether an account is compliant or not. The valid values are Unknown, Compliant, Non Compliant, and Disallowed.</p> <p>Account Ownership Type The type of the account ownership. The valid values are Device, Individual, System, and Vendor.</p> <p>Account Last Access Date The last accessed date and time of an account.</p> <p>Account Service Name The name of a service in which the account is located.</p> <p>Account Dn An LDAP distinguished name for an account.</p> <p>Account Container Dn An LDAP distinguished name for a business unit to which an account belongs.</p> <p>Account Service Dn An LDAP distinguished name for a service to which the accounts belong.</p> <p>Account Service Container DN An LDAP distinguished name for a business unit of a service that is associated with the accounts.</p> <p>Account Service Url A URL that connects to a managed resource.</p> <p>Account Service Type The service profile type.</p>
Account Owner	<p>Person Full Name The full name of a user who owns an account.</p> <p>Person Last Name The surname of a user who owns an account.</p> <p>Person Dn An LDAP distinguished name for an account owner.</p> <p>Person Business Unit Dn An LDAP distinguished name for the business unit to which an account owner belongs.</p> <p>Person Supervisor The user supervisor of the account owner.</p>
Account Owner Role Membership	<p>Role Name The name of a role.</p> <p>Role Type The type of a role. The valid values are Static and Dynamic.</p> <p>Role Dn An LDAP distinguished name for a role.</p> <p>Role Container DN An LDAP distinguished name for the business unit that is associated with a role.</p>

Table 58. Query items in the Account Configuration namespace (continued)

Query subject	Query items and their description
Group	<p>Group Name The name of a group for which an access is defined.</p> <p>Group Type The profile type of a group.</p> <p>Group Access Name The name of the access that is defined for a group.</p> <p>Group Access Type The type of the access that is defined for a group.</p> <p>Group Supervisor An LDAP distinguished name for a group supervisor.</p> <p>Group DN An LDAP distinguished name for a group to which an access is defined.</p> <p>Group Container Dn An LDAP distinguished name for the business unit that is associated with a group.</p> <p>Group Service Dn An LDAP distinguished name for the service that is associated with a group.</p>
Service Business Unit	<p>Business Unit Name The name of the business unit to which a user belongs.</p> <p>Business Unit Supervisor The user supervisor of the business unit.</p> <p>Business Unit Dn An LDAP distinguished name for the business unit to which a user belongs.</p> <p>Business Unit Container Dn An LDAP distinguished name for the parent the business unit of an organization entity.</p>

Table 58. Query items in the Account Configuration namespace (continued)

Query subject	Query items and their description
<p>Credential</p>	<p>Credential Name The name of a shared credential.</p> <p>Credential Policy Name The name of a policy that provides the entitlements for a credential.</p> <p>Credential Description Describes a credential as specified in the credential configuration.</p> <p>Credential Is Exclusive Indicates whether the credential is exclusive or not. 0 represents Yes, and 1 represents No.</p> <p>Credential Pool Use Global Settings A flag that indicates whether a credential pool uses the shared access global settings. 0 represents Uses global settings, and 1 represents Does not use global settings.</p> <p>Credential Is Searchable Indicates whether a credential is searchable or not. 0 represents Can be searched, and 1 represents cannot be searched.</p> <p>Credential Is Password Viewable Specifies whether a user can view the password on a credential. 0 represents password is viewable, and 1 represents password is not viewable.</p> <p>Credential Reset Password Indicates whether the password of a credential is regenerated on every check-in action. 0 represents Yes, and 1 represents No.</p> <p>Credential MAX Checkout Time The maximum allowed check-out duration for the credential in hours.</p> <p>Credential Service Name The name of a service to which the credential is provisioned.</p> <p>Credential Service Business Unit Name The name of the business unit to which the credential service belongs.</p> <p>Credential Dn An LDAP distinguished name for a credential.</p> <p>Credential Service Dn An LDAP distinguished name for the service on which a credential is provisioned.</p> <p>Credential Service Business Unit Dn An LDAP distinguished name for the business unit of a credential service.</p> <p>Credential Shared Access Member Role Dn An LDAP distinguished name for the role who is a member of the shared access policy that provides entitlement for the credential.</p> <p>Credential Shared Access Policy Id a unique numeric identifier that is assigned to the policy by IBM Security Identity Manager.</p>

Table 58. Query items in the Account Configuration namespace (continued)

Query subject	Query items and their description
<p>Credential Pool</p>	<p>Credential Pool Name The name of the credential pool.</p> <p>Credential Pool Policy Name The name of a policy that provides the entitlements for the credential pool.</p> <p>Credential Pool Service Name The name of the service on which the groups corresponding to the credential pool are provisioned.</p> <p>Credential Pool Service Business Unit Name The name of the business unit to which the credential pool service belongs.</p> <p>Credential Pool Group Name The name of the group corresponding to credential pool.</p> <p>Credential Pool Dn An LDAP distinguished name for the credential pool.</p> <p>Credential Pool Service Dn An LDAP distinguished name for the service on which the groups corresponding to the credential pool are provisioned.</p> <p>Credential Pool Business Unit Dn An LDAP distinguished name for the business unit of a credential pool service.</p> <p>Credential Pool Shared Access Member Role Dn An LDAP distinguished name for the role who is a member of the shared access policy that provides entitlement for the credential pool.</p> <p>Credential Pool Shared Access Policy Id A unique numeric identifier that is assigned to the policy by IBM Security Identity Manager system.</p>

Table 58. Query items in the Account Configuration namespace (continued)

Query subject	Query items and their description
<p>Account ACI</p>	<p>ACI Name The name of an ACI.</p> <p>ACI Business Unit Name The name of a business unit to which an ACI applies.</p> <p>ACI Protection Category The category of an entity that is protected by an ACI. The value of this item must be Account.</p> <p>ACI Target The type of selected protection category that is associated with an ACI. The valid values and their meanings:</p> <ul style="list-style-type: none"> • erAccountItem - All type of the accounts. • erLDAPUserAccount - LDAP accounts. • erPosixAixAccount - POSIX AIX accounts. • erPosixHpuxAccount - POSIX HP-UX accounts. • erPosixLinuxAccount - POSIX Linux accounts. • erPosixSolarisAccount - POSIX Solaris accounts. <p>ACI scope The scope of an ACI. It determines whether an ACI applies to subunits of a business organization or not. The valid values and their meanings:</p> <ul style="list-style-type: none"> • single - The policy applies to a business unit and not its subunits. • subtree - The policy applies to the subunits of a business organization. <p>ACI Member Name The members who are governed by an ACI. The valid values are:</p> <ul style="list-style-type: none"> • All users in the system. • The account owner. • The manager of the account owner. • The owner of the service that the account resides on. • The owner of any access defined on the service that the account resides on. • The sponsor of the business partner organization in which the account resides. • The administrator of the domain in which the account resides. <p>ACI System Group Name Represents the name of the group whose members are governed by an ACI.</p> <p>ACI Business Unit Dn An LDAP distinguished name for the business unit.</p> <p>ACI System Group Dn An LDAP distinguished name for a system group.</p>
<p>ACI Operations</p>	<p>ACI Operation Name The name of an operation that is governed by an ACI.</p> <p>ACI Operation Permission The permission applicable on an ACI operation. The valid values are grant, deny, and none.</p> <p>ACI Business Unit Dn An LDAP distinguished name for the business unit.</p>

Table 58. Query items in the Account Configuration namespace (continued)

Query subject	Query items and their description
<p>ACI Attribute Permissions</p>	<p>ACI Attribute Name The name of an LDAP attribute on which the permissions are controlled by an ACI.</p> <p>ACI Attribute Operation The name of the operation that can be run on an attribute. The valid values are <code>r</code> for read operation, <code>w</code> for write operation, and <code>rw</code> for read and write operations.</p> <p>ACI Attribute Permission The permission applicable on an ACI operation. The valid values are <code>grant</code> and <code>deny</code>.</p> <p>ACI Business Unit Dn An LDAP distinguished name for the business unit.</p>
<p>Identity Policy</p>	<p>Identity Policy Name The name of an identity policy.</p> <p>Identity Policy Scope The scope of an identity policy. It determines whether the policy applies to the subunits of a business organization or not. The valid values and their meanings:</p> <ul style="list-style-type: none"> • <code>single</code> - The policy applies to a business unit and not its subunits. • <code>subtree</code> - The policy applies to the subunits of a business organization. <p>Identity Policy Enabled Shows whether or not the policy is enabled.</p> <p>Identity Policy User Class The type of a user for which the policy applies. The valid values are <code>Person</code> and <code>Business Partner Person</code>.</p> <p>Identity Policy Target Type Determines the type of the service within the policy business unit on which the identity policy is applied. The valid values and their meanings:</p> <ul style="list-style-type: none"> • <code>All Services</code> - All the defined services. • <code>Specific Service</code> - The services that are explicitly added by a user. • <code>PosixLinuxProfile</code> - All the services of type POSIX Linux profile. • <code>LdapProfile</code> - All the services of type LDAP profile. • <code>PosixAixProfile</code> - All the services of type POSIX AIX profile. • <code>PosixSolarisProfile</code> - All the services of type POSIX Solaris profile. • <code>PosixHpuxProfile</code> - All the services of type POSIX HP_UX Profile. • <code>ITIMService</code> - Default service that is used for IBM Security Identity Manager accounts. <p>Identity Policy Dn An LDAP distinguished name for the identity policy.</p> <p>Identity Policy Target Dn An LDAP distinguished name for the service on which the identity policy is applied.</p> <p>Identity Policy Container Dn An LDAP distinguished name for the business unit where the identity policy is located.</p>
<p>Provisioning Policy</p>	<p>Provisioning Policy Name The name of a provisioning policy.</p> <p>Provisioning Policy Member Name The name of the entities that is provisioned by a policy. The valid values are:</p> <ul style="list-style-type: none"> • <code>All users in the organization</code> • <code>All other users who are not granted to the entitlement(s) defined by this provisioning policy via other policies.</code> <p>Provisioning Policy Dn An LDAP distinguished name for the provisioning policy.</p> <p>Provisioning Policy Container Dn An LDAP distinguished name for a business unit to which the provisioning policy applies.</p>

Table 58. Query items in the Account Configuration namespace (continued)

Query subject	Query items and their description
<p>Recertification Policy</p>	<p>Recertification Policy Name The name of the recertification policy.</p> <p>Recertification Policy Type The type of an entity that gets recertified by the policy. The valid values are Account, Access, and Identity.</p> <p>Recertification Policy Description Describes the policy as specified in the policy configuration.</p> <p>Recertification Policy Enabled Shows whether or not the policy is enabled.</p> <p>Recertification Policy Scheduling Mode The recertification scheduling modes. The valid values are CALENDAR and ROLLING.</p> <p>Recertification Policy Rolling Interval The recertification period if the recertification policy scheduling mode is ROLLING. No value in this query item indicates that the scheduling is not in the ROLLING mode.</p> <p>Recertification Policy Reject Action An action that is taken if the recertification is rejected.</p> <p>Recertification Policy Timeout Period in Days The duration during which the recertifier must act.</p> <p>Recertification Policy Timeout Action An automatic action that must be taken if the recertification times out.</p> <p>Recertification Policy DN An LDAP distinguished name for the recertification policy.</p> <p>Recertification Policy Container DN An LDAP distinguished name for a business unit to which the recertification policy applies.</p> <p>Recertification Policy IsCustom Indicates whether this recertification policy is customized. It is defined in a workflow.</p> <p>Recertification Policy User Class The type of a user the recertification policy applies. The valid values are All, Person, and Business Partner Person.</p>

Table 58. Query items in the Account Configuration namespace (continued)

Query subject	Query items and their description
Password Policy	<p>Password Policy Name The name of a password policy.</p> <p>Password Policy Scope The scope of a password policy. It determines whether the policy applies to subunits of a business organization or not. The valid values and their meanings:</p> <ul style="list-style-type: none"> • single - The policy applies to a business unit and not its subunits. • subtree - The policy applies to the subunits of a business organization. <p>Password Policy Enabled Shows whether or not the policy is enabled.</p> <p>Password Policy Target Type Determines the type of a service within the policy business unit on which the password policy is applied. The valid values are:</p> <ul style="list-style-type: none"> • All Services - All the defined services. • Specific Service - The services that are explicitly added by a user. • PosixLinuxProfile - All the services of type POSIX Linux profile. • LdapProfile - All the services of type LDAP profile. • PosixAixProfile - All the services of type POSIX AIX profile. • PosixSolarisProfile - All the services of type POSIX Solaris profile. • PosixHpuxProfile - All the services of type POSIX HP_UX Profile. • ITIMService - Default service that is used for IBM Security Identity Manager accounts. <p>Password Policy Dn An LDAP distinguished name for the password policy.</p> <p>Password Policy Target Dn An LDAP distinguished name for the service on which the password policy is applied.</p> <p>Password Policy Container Dn An LDAP distinguished name for the business unit where the identity policy is located.</p>

Provisioning Policy Audit namespace

The Provisioning Policy Audit namespace pertains to the audit history of the provisioning policies. You can generate the audit reports for the actions that are performed on the provisioning policies and automatically provisioned accounts.

Query subjects for Provisioning Policy Audit namespace

The following table lists the query subjects in the Provisioning Policy Audit namespace.

Table 59. Query subjects in the Provisioning Policy Audit namespace

Query subject	Description
Provisioning Policy Audit	Represents a history of the provisioning policies and accounts.
Provisioning Policy	Represents the provisioning policies on which the audit actions are performed. To obtain more information about the policy and accounts that go through the audit actions, use this query subject with the following query subjects:
	<ul style="list-style-type: none"> • Provisioning Policy Audit • Provisioning Policy Business Unit • Provisioning Policy Service
Provisioning Policy Business Unit	Represents the business unit to which the provisioning policy applies.
Provisioning Policy Service	Represents the managed service to which the provisioning policy applies.

Query items for Provisioning Policy Audit namespace

The following table lists the query items in the Provisioning Policy Audit namespace.

Query subject	Query items and their description
Provisioning Policy Audit	<p>Audit Provisioning Policy Name The name of a provisioning policy.</p> <p>Audit Provisioning Policy Business Unit The name of a business unit to which the provisioning policy applies.</p> <p>Audit Action The action that is performed on the provisioning policy. For example, Add, Modify, and EnforceEntirePolicy.</p> <p>Audit Process Subject A subject of the automatically provisioned audit action. It can be the provisioning policy or the accounts that are provisioned.</p> <p>Audit Subject Type The type of the audit subject. For example, Policy and Account.</p> <p>Audit Process Subject Profile The profile type of the accounts that is provisioned by the provisioning policy. This query item applies only to the accounts.</p> <p>Audit Process Subject Service The service on which the accounts are provisioned. This query item applies only to the accounts.</p> <p>Audit Initiator Name The name of a user who initiated the audit action.</p> <p>Audit Process Requestee Name The name of a user on behalf of whom the audit action is initiated.</p> <p>Audit Comments The comments that are entered by an approver during the audit workflow approval.</p> <p>Audit Operation Start Time The audit operation start date and time.</p> <p>Audit Process Submission Time The audit process submission date and time.</p> <p>Audit Process Schedule Time The date and time at which an event is scheduled for execution.</p> <p>Audit Process Completion Time The audit process completion date and time.</p> <p>Audit Process Result Summary The result summary of the account request workflow process.</p> <p>Activity Name The name of the audit activity.</p> <p>Activity Submission Time The audit activity submission date and time.</p> <p>Activity Completion Time The audit activity completion date and time.</p> <p>Audit Activity Result Summary The result summary of an activity in the account request workflow process.</p> <p>Audit Process Recertifier The name of a user who approves the audit process workflow.</p> <p>Audit provisioning policy Dn An LDAP distinguished name for the provisioning policy on which the audit actions are performed.</p>

Table 60. Query items in the Provisioning Policy Audit namespace (continued)

Query subject	Query items and their description
Provisioning Policy	<p>Provisioning Policy Name The name of a provisioning policy.</p> <p>Provisioning Policy Scope The scope in terms of a hierarchy of the business units to which the provisioning policy applies.</p> <p>Provisioning Policy Dn An LDAP distinguished name for the provisioning policy.</p> <p>Provisioning Policy Business Unit Dn An LDAP distinguished name for the business unit to which the provisioning policy applies.</p>
Provisioning Policy Business Unit	<p>Business Unit Name The name of the business unit to which the provisioning policy applies.</p> <p>Business Unit Supervisor The supervisor of a user for the business unit to which the provisioning policy applies.</p> <p>Business Unit Container Dn An LDAP distinguished name for the business unit where the provisioning policy business unit is located.</p> <p>Business Unit Dn An LDAP distinguished name for the business unit to which the provisioning policy belongs.</p>
Provisioning Policy Service	<p>Service Name The name of a service to which the provisioning policy applies.</p> <p>Service Type The profile type of a service to which the provisioning policy applies.</p> <p>Service Business Unit The business unit of a service to which the provisioning policy applies.</p> <p>Service Dn An LDAP distinguished name for a service to which the provisioning policy belongs.</p> <p>Service Business Unit Dn An LDAP distinguished name for the business unit to which the service belongs.</p> <p>Service Owner Dn An LDAP distinguished name for the user owner of a service.</p>

Provisioning Policy Config namespace

The Provisioning Policy Config namespace pertains to the configuration attributes of a provisioning policy. It encompasses the business units, services, policy members, and the ACIs that are related to the provisioning policies. You can generate the configuration reports for the provisioning policy.

Query subjects for Provisioning Policy Config namespace

The following table lists the query subjects in the Provisioning Policy Config namespace.

Table 61. Query subjects in the Provisioning Policy Config namespace

Query subject	Description
Provisioning Policy	Represents the provisioning policy and its configuration attributes.
Provisioning Policy Parameters	Represents the parameters that are defined for the entitlements of a provisioning policy. You must use this query subject with the Provisioning Policy query subject.
Provisioning Policy Role Members	Represents the user members of a role that is a part of the provisioning policy. You must use this query subject with the Provisioning Policy query Subject.
ACI Attribute Permissions	Represents the permissions that are defined on the attributes by an ACI. You must use this query subject with the Provisioning Policy ACI query subject.
ACI Operations	Represents the permissions that are defined on the class operations by an ACI. You must use this query subject with the Provisioning Policy ACI query subject.
Provisioning Policy ACI	Represents an ACI associated with a provisioning policy. You must use this query subject with the Provisioning Policy query subject.

Query items for Provisioning Policy Config namespace

The following table lists the query items in the Provisioning Policy Config namespace.

Note: The policies that are in the Draft mode cannot be identified. Although the draft policies are in the list, there is no attribute that can identify the draft policies.

Table 62. Query items in the Provisioning Policy Config namespace	
Query subject	Query items and their description
Provisioning Policy	<p>Provisioning Policy Name The name of a provisioning policy.</p> <p>Provisioning Policy Business Unit The name of a business unit to which the provisioning policy applies.</p> <p>Provisioning Policy Is Enabled Represents whether the provisioning policy is enabled or not. The valid values are Enabled and Disabled.</p> <p>Provisioning Policy Priority An integer number greater than zero that indicates the priority of the provisioning policy.</p> <p>Provisioning Policy Scope The scope in terms of a hierarchy of the business units to which the provisioning policy applies. The valid values are Single and Subtree.</p> <p>Provisioning Policy Member Name The name of a role or user who is a member of the provisioning policy. The valid values are All users in the organization, All other users who are not granted to the entitlement(s) defined by this provisioning policy via other policies, or the names of the roles who are the members.</p> <p>Provisioning Policy Dn An LDAP distinguished name for the provisioning policy.</p> <p>Provisioning Policy Business Unit Dn An LDAP distinguished name for the business unit to which the provisioning policy applies.</p> <p>Provisioning Policy Service Name The name of a service to which the provisioning policy applies.</p> <p>Provisioning Policy Service Type The profile type of a service to which the provisioning policy applies.</p> <p>Provisioning Policy Service Url A URL of a service to which the provisioning policy applies.</p> <p>Provisioning Policy Service Business Unit The business unit of a service to which the provisioning policy applies.</p>
Provisioning Policy Parameters	<p>Provisioning Policy Parameter A provisioning policy parameter that is defined by the system administrator.</p> <p>Provisioning Policy Parameter Value The parameter value.</p> <p>Provisioning Policy Parameter Enforcement Type Specifies the rule for the system to evaluate an attribute value validity. The possible values are Mandatory, Allowed, Default, and Excluded.</p> <p>Service Target An LDAP distinguished name for the service that is associated with the provisioning policy.</p>
Provisioning Policy Role Members	<p>Role Member First Name The given name of a role member.</p> <p>Role Member Last Name The surname of a role member.</p> <p>Role Member Status The current state of the role member. The valid values are Active and Inactive.</p> <p>Role Member Dn An LDAP distinguished name for a role member.</p> <p>Role Member Business Unit Dn An LDAP distinguished name for the business unit of a role member.</p> <p>Role Member Supervisor The user supervisor of the role member.</p>

Table 62. Query items in the Provisioning Policy Config namespace (continued)

Query subject	Query items and their description
ACI Attribute Permissions	<p>ACI Attribute Name The name of an attribute that is controlled by an ACI.</p> <p>ACI Attribute Operation The name of an operation that is governed by an ACI.</p> <p>ACI Attribute Permission The permission that applies on an ACI operation. The valid values are <code>grant</code>, <code>deny</code>, and <code>none</code>.</p> <p>ACI Business Unit Dn An LDAP distinguished name for the business unit.</p>
ACI Operations	<p>ACI Operation Name The class operation for an ACI. For example, <code>Search</code>, <code>Add</code>, and <code>Modify</code>.</p> <p>ACI Operation Permission The permission that is associated with a class operation. The valid values are <code>grant</code>, <code>deny</code>, and <code>none</code>.</p> <p>ACI Business Unit Dn An LDAP distinguished name for the business unit to which an ACI applies.</p>
Provisioning Policy ACI	<p>ACI Name The name of an ACI associated with the provisioning policy.</p> <p>ACI Business Unit The name of a business unit to which an ACI applies.</p> <p>ACI Scope The hierarchy of the business units to which an ACI applies.</p> <p>ACI Member Name The members who are governed by an ACI. The valid values are:</p> <ul style="list-style-type: none"> • <code>All Users</code> - All users in the system. • <code>All Group Members</code> - The users who are the members of these groups. • <code>Supervisor</code> - The supervisor of the business unit in which the provisioning policy resides. • <code>Sponsor</code> - The sponsor of the business partner organization in which the role resides. • <code>Administrator</code> - The administrator of the domain in which the account resides. <p>ACI System Group Name The name for IBM Security Identity Manager group that is the part of an ACI. This query item is valid only when ACI member name is the name of the user members of a specified group.</p> <p>ACI Business Unit Dn An LDAP distinguished name for the business unit to which an ACI applies.</p> <p>ACI Role Dn An LDAP distinguished name for IBM Security Identity Manager group that is a part of an ACI.</p> <p>ACI Role Business Unit Dn An LDAP distinguished name for a business unit that is associated with IBM Security Identity Manager group.</p> <p>ACI Parent An LDAP distinguished name for the parent container in which an ACI is defined.</p>

Role Audit namespace

The Role Audit namespace pertains to the audit history of the actions that are performed on the roles. You can generate the audit reports for the role entities.

Query subjects for Role Audit namespace

The following table lists the query subjects in the Role Audit namespace.

Query subject	Description
Role	Represents the role entity and its configuration attributes on which the audit actions are performed.
Role Audit	Represents the audit history of the role entities. You must use this query subject with the Role query subject.
Role Business Unit	Represents the business unit to which a role associated with the audit action belongs. You must use this query subject with the Role query subject.
Role Membership	Represents the person who is the member of a role and its configuration attributes. You must use this query subject with the Role query subject.
Role Owner	Represents an owner of a role that is associated with the audit action. The owner can be a user or role. You must use this query subject with the Role query subject.

Query items for Role Audit namespace

The following table lists the query items in the Role Audit namespace.

Query subject	Query items and their description
Role	Role Name The name of a role on which the audit actions are performed. Role Description The description of the role. Role Type The type of a role. The valid values are Static and Dynamic. Role Dn An LDAP distinguished name for the role. Role Container Dn An LDAP distinguished name for the container of the role.

Table 64. List of query items in the Role Audit namespace (continued)

Query subject	Query items and their description
<p>Role Audit</p>	<p>Audit Role Name The name of a role entity on which the audit action is performed.</p> <p>Audit Role Business Unit The business unit of the role.</p> <p>Audit Action The action that is performed on a role. For example, Add, Modify, Delete, and AddMember.</p> <p>Audit Comments The comments that are entered by the audit workflow approver. Note: Along with the audit comments, this query item might contain the operational data.</p> <p>Audit Initiator Name The name of a user who initiated the audit action.</p> <p>Audit Process Requestee Name The name of a user who is added to the role. This query item is applicable only to AddMember audit action.</p> <p>Audit Process Recertifier Name The name of a user who approved the audit action.</p> <p>Audit Operation Start Time The audit operation start date and time.</p> <p>Audit Process Submission Time The audit process submission date and time.</p> <p>Audit Process Schedule Time The date and time at which an event is scheduled for execution.</p> <p>Audit Process Completion Time The audit process completion date and time.</p> <p>Audit Process Subject The subject on which the audit action was performed. It applies to the cases where the defined workflow must complete before the audit action completion.</p> <p>Audit Process Subject Profile The profile type of an entity that is associated with the audit action. This query item contains the value only if the Audit Process Subject contain a value.</p> <p>Audit Process Subject Service The service to which an entity represented by the Audit Process Subject query item belongs.</p> <p>Audit Process Result Summary The result of a role audit process.</p> <p>Activity Result Summary The result of an activity within a role audit process.</p> <p>Audit Activity Name The name of the activity that corresponds to the audit process.</p> <p>Audit Activity Owner An owner who owns the activity. For example: Approve role membership or Add request.</p>
<p>Role Business Unit</p>	<p>Business Unit Name The name of a business unit to which the role belongs.</p> <p>Business Unit Supervisor A person who is the supervisor of a business unit to which the role belongs.</p> <p>Business Unit Dn An LDAP distinguished name for a business unit to which the role belongs.</p> <p>Business Unit Container DN An LDAP distinguished name for the parent organization of the business unit to which the role belongs.</p>

Table 64. List of query items in the Role Audit namespace (continued)

Query subject	Query items and their description
Role Membership	<p>Role Member First Name The given name of a role member.</p> <p>Role Member Last Name The surname of a role member.</p> <p>Role Member Supervisor The supervisor of a role member.</p> <p>Role Member Dn An LDAP distinguished name for a role member.</p> <p>Role Dn An LDAP distinguished name for a role.</p> <p>Role Member Business Unit Dn An LDAP distinguished name for the business unit to which a role member belongs.</p>
Role Owner	<p>Role Owner Name The name of an owner of the role.</p> <p>Role Owner Type Indicates whether the owner is a role or a user. The valid values are User and Role.</p> <p>Role Owner Business Unit The business unit to which the role owner belongs.</p> <p>Role Dn An LDAP distinguished name for a role.</p>

Role Configuration namespace

The Role Configuration namespace contains the query subjects and query items for configuring the roles.

Query subjects for Role Configuration namespace

The following table lists the query subjects in the Role Configuration namespace.

Table 65. Query subjects in the Role Configuration namespace

Query subject	Description
Role	Represents a role and some of its configuration attributes.
Role Owner	Represents an owner of a role that is associated with the audit action. The owner can be a user or role. You must use this query subject with the Role query subject.
Parent Roles	Represents the parent of a role. You must use this query subject with the Role query subject to obtain information about the parent of the role.
Role Assignment Attributes	Represents an assignment attributes for a role. You must use this query subject with the Role query subject to obtain information about the assignment attributes for the role.
Role Members	Represents the user members of a role. You must use this query subject with the Role query subject to obtain information about the members of the role.
Role ACI	Represents an ACI that is applicable on the roles. You must use this query subject with the Role query subject to obtain information about the roles that are managed by an ACI.
ACI Operations	Represents information about operations that are governed by an ACI. You must use this query subject with the Role ACI query subject to obtain information about an ACI associated with the role.
ACI Attribute Permissions	Represents information about the attributes and operations that can be performed on the attributes. You must use this query subject with the Role ACI query subject to obtain information about an ACI associated with a role.
Recertification Policy	Represents the recertification policy and some of its configuration attributes. You must use this query subject with the Role query subject to obtain information about the roles that are recertified by the recertification policy.
Recertification Policy Business Unit	Represents a business unit to which the recertification policy is applicable.

Table 65. Query subjects in the Role Configuration namespace (continued)

Query subject	Description
Provisioning Policy	Represents the provisioning policy and some of its configuration attributes. You must use this query subject with the Role query subject to obtain information about the roles who are member of a provisioning policy.
Shared Access Policy	Represents the shared access policy that provides entitlements for the credentials and credential pools. You must use this query subject with the Role query subject to obtain information about the role members of the shared access policy.
Separation of Duty Policy	Represents a separation of duty policy and some of its configuration attributes. You must use this query subject with the Role query subject to obtain information about the roles to which the policy applies.
Separation of Duty Rule	Represents the rule that is defined for a separation of duty policy. You must use this query subject with the Separation of Duty Policy and Role query subjects to obtain information about: <ul style="list-style-type: none"> • The rules that are defined for a separation of duty policy. • The roles that are covered by a separation of duty rule.

Query items for Role Configuration namespace

The following table lists the query items in the Role Configuration namespace.

Table 66. List of query items in the Role Configuration namespace

Query subject	Query items and their description
Role	<p>Role Name The name of a role.</p> <p>Role Description The description of a role.</p> <p>Role Type The type of a role. The valid values are Static and Dynamic.</p> <p>Role Access Enabled Represents whether an access for a role is enabled or not. True represents Enabled, and False represents Disabled.</p> <p>Role Common Access Enabled Represents whether a common access for the role is enabled or not. The valid values are True and False.</p> <p>Role Access Type The type of an access that is enabled for a role.</p> <p>Role Business Unit Name The name of a business unit to which the role belongs.</p> <p>Role Dn An LDAP distinguished name for the role.</p> <p>Role Business Unit Dn An LDAP distinguished name for the business unit of a role.</p> <p>Role Business Unit Container Dn An LDAP distinguished name for the parent organization of the business unit.</p> <p>Role Business Supervisor The supervisor of a user for the business unit.</p>
Role Owner	<p>Role Owner Name The name of an owner of the role.</p> <p>Role Owner Type Indicates whether the owner is a role or a user. The valid values are User and Role.</p> <p>Role Owner Business Unit The business unit to which the role owner belongs.</p> <p>Role Dn An LDAP distinguished name for a role.</p>

Table 66. List of query items in the Role Configuration namespace (continued)

Query subject	Query items and their description
Parent Roles	<p>Parent Role Name The name of the parent role.</p> <p>Parent Role Dn An LDAP distinguished name for the role.</p> <p>Parent Business Unit Dn An LDAP distinguished name for the business unit of the parent role.</p>
Role Assignment Attributes	<p>Attribute Name The name of an attribute.</p> <p>Role Dn An LDAP distinguished name for the role to which an attribute is assigned.</p>
Role Members	<p>Role Member First Name The given name of a role member.</p> <p>Role Member Last Name The surname of a role member.</p> <p>Role Member Attribute Name The name of the assignment attribute that is associated with a role member.</p> <p>Role Member Attribute Value An assignment attribute value that is associated with a role member.</p> <p>Role Member Dn An LDAP distinguished name for a role member.</p> <p>Role Member Business Unit Dn An LDAP distinguished name for the business unit of a role member.</p>
Role ACI	<p>Role ACI Name The name of an ACI that applies to a role.</p> <p>Role ACI Protection Category The type of a role that is protected by an ACI. The valid values are <code>Static Role</code> and <code>Dynamic Role</code>.</p> <p>Role ACI Scope The scope of an ACI. It determines whether an ACI applies to sub units of a business organization or not. The valid values and their meanings:</p> <ul style="list-style-type: none"> • <code>single</code> - The policy applies to a business unit and not its subunits. • <code>subtree</code> - The policy applies to the subunits of a business organization. <p>Role ACI Member Name The members who are governed by an ACI. The valid values are:</p> <ul style="list-style-type: none"> • All users in the system. • The supervisor of the business unit in which the role resides. • The owners of the role, The administrator of the domain in which the role resides. • The sponsor of the business partner organization in which the role resides. <p>Role ACI System Group Name Represents the name of the group whose members are governed by an ACI.</p> <p>Role ACI Business Unit Dn An LDAP distinguished name for a business unit.</p> <p>Role ACI System Group Dn An LDAP distinguished name for a system group.</p>
ACI Operations	<p>ACI Operation Name The name of an operation that is governed by an ACI.</p> <p>ACI Operation Permission The permission applicable on an ACI operation. The valid values are <code>grant</code>, <code>deny</code>, and <code>none</code>.</p> <p>ACI Business Unit Dn An LDAP distinguished name for the business unit to which an ACI applies.</p>

Table 66. List of query items in the Role Configuration namespace (continued)

Query subject	Query items and their description
<p>ACI Attribute Permissions</p>	<p>ACI Attribute Name The name of an LDAP attribute on which the permissions are controlled by an ACI.</p> <p>ACI Attribute Operation The name of an operation that an ACI governs.</p> <p>ACI Attribute Permission The permission applicable on an ACI operation. The valid values are <code>grant</code> and <code>deny</code>.</p> <p>ACI Business Unit Dn An LDAP distinguished name for a business unit to which an ACI applies.</p>
<p>Recertification Policy</p>	<p>Recertification Policy Name The name of the recertification policy.</p> <p>Recertification Policy Type The type of an entity that gets recertified by using this policy. The valid values are: <code>Account</code>, <code>Access</code>, and <code>Identity</code>.</p> <p>Recertification Policy Description Describes the policy as specified in the policy configuration.</p> <p>Recertification Policy Enabled Shows whether or not the policy is enabled.</p> <p>Recertification Policy Scheduling Mode The recertification scheduling modes. The valid values are <code>CALENDAR</code> and <code>ROLLING</code>.</p> <p>Recertification Policy Rolling Interval Represents the recertification period if the recertification policy scheduling mode is <code>ROLLING</code>. No value in this query item indicates that the scheduling is not in the <code>ROLLING</code> mode.</p> <p>Recertification Policy Reject Action An action that is taken if the recertification is rejected.</p> <p>Recertification Policy Timeout Period in Days The duration during which a recertifier must act.</p> <p>Recertification Policy Timeout Action The automatic action that must be taken if the recertification times out.</p> <p>Recertification Policy DN An LDAP distinguished name for the recertification policy.</p> <p>Recertification Policy Container DN An LDAP distinguished name for a business unit to which the recertification policy applies.</p> <p>Recertification Policy IsCustom Indicates whether the recertification policy is customized or not. It is defined in the workflow.</p> <p>Recertification Policy User Class The type of a user to which the recertification policy applies. The valid values are <code>All</code>, <code>Person</code>, and <code>Business Partner Person</code>.</p>
<p>Recertification Policy Business Unit</p>	<p>Business Unit Name The name of a business unit.</p> <p>Business Unit Supervisor The user supervisor of a business unit.</p> <p>Business Unit Dn An LDAP distinguished name for a business unit.</p> <p>Business Unit Container DN an LDAP distinguished name for the parent business unit.</p>

Table 66. List of query items in the Role Configuration namespace (continued)

Query subject	Query items and their description
<p>Provisioning Policy</p>	<p>Provisioning Policy Name The name of the provisioning policy.</p> <p>Provisioning Policy Business Unit Name The name of a business unit to which the provisioning policy applies.</p> <p>Provisioning Policy Dn An LDAP distinguished name for the provisioning policy.</p> <p>Provisioning Policy Business Unit Dn An LDAP distinguished name for the business unit to which the provisioning policy applies.</p> <p>Provisioning Policy Business Supervisor A user supervisor for the provisioning policy business unit.</p>
<p>Shared Access Policy</p>	<p>Shared Access Policy Name The name of a shared access policy.</p> <p>Shared Access Policy Description The description the shared access policy.</p> <p>Shared Access Policy Business Unit Name The name of a business unit to which the shared access policy applies.</p> <p>Shared Access Policy Scope The scope of a shared access policy in terms of business units the policy applies. 1 represents that the policy applies to the business unit only, and 2 indicates that the policy applies to the sub business units also.</p> <p>Shared Access Policy Status Represents whether a policy is enabled or not. 0 represents Enabled, and 1 represents Disabled.</p> <p>Shared Access Business Unit Supervisor A user supervisor for the shared access policy business unit.</p> <p>Shared Access Policy ID A unique numeric identifier that is assigned to the policy by IBM Security Identity Manager.</p> <p>Shared Access Policy Business Unit Dn An LDAP distinguished name for the business unit to which a shared access policy applies.</p>
<p>Separation of Duty Policy</p>	<p>Separation of Duty Policy Name The name of the separation of duty policy.</p> <p>Separation of Duty Policy Description The description of the separation of duty policy.</p> <p>Separation of Duty Policy Business Unit Name The name of the business unit to which the separation of duty policy applies.</p> <p>Separation of Duty Policy Enabled Represents whether the policy is enabled or not. True represents Enabled, and False represents Disabled.</p> <p>Separation of Duty Policy Owner Name The name of an owner of the separation of duty policy.</p> <p>Separation of Duty Policy Owner Type the type of an owner for the separation of duty policy. The valid values are Role and Person.</p> <p>Separation of Duty Policy Owner Business Unit Name The name of the business unit that applies to the policy owner.</p> <p>Separation of Duty Policy Id A unique numeric identifier that IBM Security Identity Manager assigns to the policy.</p> <p>Separation of Duty Policy Owner Dn An LDAP distinguished name for the policy owner.</p>

Table 66. List of query items in the Role Configuration namespace (continued)

Query subject	Query items and their description
Separation of Duty Rule	<p>Separation of Duty Rule Name The name of the separation of duty rule.</p> <p>Separation of Duty Rule Max Roles Allowed The maximum number of roles that are allowed in a rule.</p> <p>Separation of Duty Rule Version A numeric identifier for the current version of the rule that applies to a policy.</p> <p>Separation of Duty Rule Id A unique numeric identifier that IBM Security Identity Manager assigns to the rule.</p> <p>Separation of Duty Policy Id A unique numeric identifier that IBM Security Identity Manager assigns to the policy.</p> <p>Separation of Duty Role Id A unique numeric identifier that IBM Security Identity Manager assigns to the role.</p>

Separation of Duty Audit namespace

The Separation of Duty Audit namespace pertains to the audit history, exemption and violation of the separation of duty policy.

Query subjects for Separation of Duty Audit namespace

The following table lists the query subjects in the Separation of Duty Audit namespace.

Table 67. Query subjects in the Separation of Duty Audit namespace

Query subject	Description
Separation of Duty Policy	<p>Represents the separation of duty policy and the rules that are configured. You must use this query subject with the following query subjects to generate the violation and exemption reports:</p> <ul style="list-style-type: none"> • Separation of Duty Policy Violation and Exemption History. • Separation of Duty Policy Violation and Exemption Current Status. • Separation of Duty Policy Audit.
Separation of Duty Policy Role	<p>Represents the configuration attributes of a role. The role is a part of the rule that is associated with the separation of duty policy. You must use this query subject with the Separation of Duty Policy query subject.</p>
Separation of Duty Policy Violation and Exemption Current Status	<p>Provides information about the exemption and violation for a separation of duty policy. You must use this query subject with the Separation of Duty Policy query subject.</p>
Separation of Duty Policy Violation and Exemption History	<p>Represents the historical information about exemption and violation for a separation of duty policy. You must use this query subject with the Separation of Duty Policy query subject.</p>
Separation of Duty Policy Audit	<p>Represents the audit history for the separation of duty policy. The actions that are audited in this query subject are Add, Modify, Delete, Reconcile, and Revoke. You must use this query subject with the Separation of Duty Policy query subject to generate an audit history report.</p>
Separation of Duty Policy Role Conflict	<p>Provides information about:</p> <ul style="list-style-type: none"> • The roles that are involved in a violation. • The role on the person that is found to be in violation of the separation of duty policy rule. <p>You must use this query subject with the Separation of Duty Policy Violation and Exemption Current Status query subject to obtain more information about the violation that is occurred.</p>

Query items for Separation of Duty Audit namespace

The following table lists the query items in the Separation of Duty Audit namespace.

Query subject	Query items and their description
Separation of Duty Policy	<p>Separation of Duty Policy Name The name of the separation of duty policy.</p> <p>Separation of Duty Policy Description The description of the separation of duty policy.</p> <p>Separation of Duty Policy Business Unit Name The name of a business unit to which the separation of duty policy applies.</p> <p>Separation of Duty Policy Enabled Indicates whether or not the policy is enabled. The valid values are Enabled and Disabled.</p> <p>Separation of Duty Policy Rule Name The name of a rule that is associated with the separation of duty policy.</p> <p>Separation of Duty Policy Rule Max Roles Allowed The maximum number of the roles that can be a part of the separation of duty rule.</p> <p>Separation of Duty Policy Id A unique numeric identifier for the separation of duty policy.</p> <p>Separation of Duty Policy Dn An LDAP distinguished name for the separation of duty policy.</p> <p>Separation of Duty Rule Id A unique numeric identifier for the separation of duty rule that is associated with the separation of duty policy.</p>
Separation of Duty Policy Role	<p>Separation of Duty Policy Role Name The name of the role that is a part of the separation of duty rule.</p> <p>Separation of Duty Policy Role Description The description of the separation of duty policy role.</p> <p>Separation of Duty Policy Business Unit Name The name of the business unit to which the separation of duty policy role applies.</p> <p>Separation of Duty Policy Role Dn An LDAP distinguished name for the role that is a part of the separation of duty policy.</p> <p>Separation of Duty Policy Role Id A unique numeric identifier for the role that is a part of separation of duty policy.</p> <p>Separation of Duty Policy Rule Id A unique numeric identifier for the separation of duty rule that is associated with the separation of duty policy.</p>

Table 68. Query items in the Separation of Duty Audit namespace (continued)

Query subject	Query items and their description
<p>Separation of Duty Policy Violation and Exemption Current Status</p>	<p>Audit Status The status of the separation of duty policy violation or exemption. The possible values are:</p> <ul style="list-style-type: none"> • Violation - indicates that the violation occurred. • Approved - indicates that an approver approved the exempted violation. <p>Audit Person Name The name of a person to which the violation refers.</p> <p>Audit Person Business Unit The business unit to which a person involved in the violation belongs.</p> <p>Audit Approver Name The name of a person who exempted the violation.</p> <p>Audit Approver Business Unit The business unit of the user who exempted the violation.</p> <p>Audit Approver Comment The comment that is added by an approver during the violation exemption process.</p> <p>Audit Policy Rule Name The name of a rule that is associated with the separation of duty policy.</p> <p>Audit Policy Rule Max Roles Allowed The maximum number of the roles that can be a part of the separation of duty rule.</p> <p>Audit Policy Rule Version The separation of duty rule version.</p> <p>Audit Time Stamp The audit action occurrence time stamp.</p> <p>Audit Exemption Time Stamp The time stamp of the last violation occurred during separation of duty policy evaluation.</p> <p>Audit Violation Id A unique numeric identifier for the violation record.</p> <p>Audit Policy Global Id A unique identifier for the separation of duty policy.</p> <p>Audit Rule Global Id A unique identifier for the separation of duty policy rule.</p> <p>Audit Person Global Id A unique identifier for the person against whom the violation occurred.</p>

Table 68. Query items in the Separation of Duty Audit namespace (continued)

Query subject	Query items and their description
Separation of Duty Policy Violation and Exemption History	<p>Audit Status The status of the separation of duty policy violation or exemption. The possible values are:</p> <ul style="list-style-type: none"> • Violation - indicates that the violation occurred. • Approved - indicates that an approver approved the exempted violation. <p>Audit Person Name The name of a person to which the violation refers.</p> <p>Audit Person Business Unit The business unit to which a person involved in the violation belongs.</p> <p>Audit Approver Name The name of a person who exempted the violation.</p> <p>Audit Approver Business Unit The business unit of the user who exempted the violation.</p> <p>Audit Approver Comment The comment that is added by an approver during the violation exemption process.</p> <p>Audit Policy Rule Name The name of a rule that is associated with the separation of duty policy.</p> <p>Audit Policy Rule Max Roles Allowed The maximum number of the roles that can be a part of the separation of duty rule.</p> <p>Audit Policy Rule Version The separation of duty rule version.</p> <p>Audit Time Stamp The audit action occurrence time stamp.</p> <p>Audit Violation Id A unique numeric identifier for the violation record.</p> <p>Audit Policy Global Id A unique identifier for the separation of duty policy.</p> <p>Audit Rule Global Id A unique identifier for the separation of duty policy rule.</p> <p>Audit Person Global Id A unique identifier for the person against whom the violation occurred.</p>

Table 68. Query items in the Separation of Duty Audit namespace (continued)

Query subject	Query items and their description
<p>Separation of Duty Policy Audit</p>	<p>Audit Separation of Duty Policy Name The name of the separation of duty policy.</p> <p>Audit Separation of Duty Policy Business Unit The business unit of the separation of duty policy.</p> <p>Audit Action An action that is performed on the separation of duty policy. For example, Add, Modify, Delete, and Reconcile.</p> <p>Audit Comments The comments that are entered by the approver.</p> <p>Audit Process Subject The name of the separation of duty policy on which the audit action occurs.</p> <p>Audit Process Subject Profile The profile type of an entity that is associated with the audit action. This query item contains the value only if the Audit Process Subject contains a value.</p> <p>Audit Process Subject Service The service to which an entity represented by the Audit Process Subject query item belongs.</p> <p>Audit Process Recertifier Name The name of a user who approves the audit process workflow.</p> <p>Audit Process Requestee Name The entity upon which the audit action is performed.</p> <p>Audit Initiator Name The name of a user who initiates the audit action.</p> <p>Audit Activity Owner The name of a user who owns the audit activity.</p> <p>Audit Activity Name The name of the audit activity.</p> <p>Audit Operation Start Time The audit operation initiation date and time.</p> <p>Audit Process Submission Time The audit process submission date and time.</p> <p>Audit Process Schedule Time The date and time at which an event is scheduled for execution.</p> <p>Audit Process Completion Time The audit process completion date and time.</p> <p>Audit Activity Result Summary The result of an activity within the account audit process.</p> <p>Audit Process Result Summary The result of an account audit process.</p>

Table 68. Query items in the Separation of Duty Audit namespace (continued)

Query subject	Query items and their description
Separation of Duty Policy Role Conflict	<p>User Roles in Conflict The name of the role on the person that is found in violation of the separation of duty policy rule.</p> <p>User Roles in Conflict Role Dn An LDAP distinguished name for a role on the person that is found in violation of the separation of duty policy rule.</p> <p>User Roles in Conflict Business Unit Dn An LDAP distinguished name for the business unit of a role on the person that is found in violation of the separation of duty policy rule.</p> <p>User Roles in Conflict Owner Dn An LDAP distinguished name for an owner of a role. The referred role is the role that participates in the separation of duty policy. This query item might be empty if no owners are assigned to the role.</p> <p>Policy Roles in Conflict The name of the role as referenced in the separation of duty policy rule that is involved in the violation.</p> <p>Policy Roles in Conflict Role Dn An LDAP distinguished name for the role as referenced in the separation of duty policy rule that is involved in the violation.</p> <p>Policy Roles in Conflict Business Unit Dn An LDAP distinguished name for the business unit of a role as referenced in the separation of duty policy rule that is involved in the violation.</p> <p>Policy Roles in Conflict Owner Dn An LDAP distinguished name for an owner of a role. The referred role is the role that associates with a user. This query item might be empty if no owners are assigned to the role.</p> <p>Separation of Duty Policy Violation Id A unique numeric identifier for the separation of duty violation record.</p>

Separation of Duty Configuration namespace

The Separation of Duty Configuration namespace pertains to the configuration attributes of a separation of duty policy. It encompasses the business units, owner, and roles for the separation of duty policy. You can generate the separation of duty policy configuration reports.

Query subjects for Separation of Duty Configuration namespace

The following table lists the query subjects in the Separation of Duty Configuration namespace.

Table 69. Query subjects in the Separation of Duty Configuration namespace

Query subject	Description
Separation of Duty Policy	Represents the separation of duty policy and its configuration attributes. You must use this query subject with the Separation of Duty Rule query subject.
Separation of Duty Rule	Represents the separation of duty rule that is associated with the separation of duty policy.
Separation of Duty Policy Role	Represents the role that is a part of the separation of duty rule. You must use this query subject with the Separation of Duty Rule query subject.

Query items for Separation of Duty Configuration namespace

The following table lists the query items in the Separation of Duty Configuration namespace.

Query subject	Query items and their description
<p>Separation of Duty Policy</p>	<p>Separation of Duty Policy Name The name of the separation of duty policy.</p> <p>Separation of Duty Policy Description The description of the separation of duty policy.</p> <p>Separation of Duty Policy Enabled Indicates whether the policy is enabled or not. True represents Enabled, and False represents Disabled.</p> <p>Separation of Duty Policy Business Unit Name The name of a business unit to which the separation of duty policy applies.</p> <p>Separation of Duty Policy Owner Name the name of the policy owner. The owner can be:</p> <ul style="list-style-type: none"> • The single or multiple roles. • The single or multiple users. <p>Separation of Duty Policy Owner Type The type of an owner for the separation of duty policy. The valid values are Role and Person.</p> <p>Separation of Duty Policy Owner Business Unit Name The name of a business unit to which the policy owner belongs.</p> <p>Separation of Duty Policy Id A unique numeric identifier for the separation of duty policy.</p> <p>Separation of Duty Policy Owner Dn An LDAP distinguished name for an owner of the policy.</p>
<p>Separation of Duty Rule</p>	<p>Separation of Duty Policy Rule Name The name of a rule that is associated with the separation of duty policy.</p> <p>Separation of Duty Policy Rule Max Roles Allowed The maximum number of the roles that can be a part of the separation of duty rule.</p> <p>Separation of Duty Rule Id A unique numeric identifier for the separation of duty rule that is associated with the separation of duty policy.</p>
<p>Separation of Duty Policy Role</p>	<p>Separation of Duty Policy Role Name The name of the role that is a part of the separation of duty rule.</p> <p>Separation of Duty Policy Role Description Describes the separation of duty policy role.</p> <p>Separation of Duty Policy Business Unit Name The name of a business unit to which the separation of duty policy role applies.</p> <p>Separation of Duty Policy Role Dn An LDAP distinguished name for the role that is a part of the separation of duty policy.</p> <p>Separation of Duty Policy Role Id a unique numeric identifier for the role that is a part of separation of duty policy.</p> <p>Separation of Duty Policy Rule Id A unique numeric identifier for the separation of duty rule that is associated with the separation of duty policy.</p>

User Configuration namespace

The User Configuration namespace contains the query subjects and query items for configuring the user entity.

Query subjects for User Configuration namespace

The following table lists the query subjects in the User Configuration namespace.

Query subject	Description
Person	Represents a person entity and its configuration attributes.
Person Aliases	Provides information about the user aliases.
Person Manager	Provides information about the manager of a user.
Account	Represents an account entity and its configuration attributes. You must use this query subject with the Person query subject to obtain information about the accounts that are owned by the user.
Role	Represents the role entity and its configuration attributes. You must use this query subject with the Person query subject to obtain information about the role membership for a user.
Person ACI	Represents an ACI that is applicable to a user. You must use this query subject with the Person query subject to obtain information about an ACI applicable to the user.
ACI Operations	Represents the operations that an ACI governs. You must use this query subject with the Person ACI query subject to obtain information about an ACI associated with the user.
ACI Attribute Permissions	Represents the attributes and operations that can be performed on an attribute. You must use this query subject with the Person ACI query subject to obtain information about an ACI associated with the user.
ACI Members	Provides information about the members of an ACI. You must use this query subject with the Person ACI query subject to obtain information about the ACI members.
Supervised Business Unit	Represents the business unit entity that a user supervises and its configuration attribute. You must use this query subject with the Person query subject to obtain information about the business unit a user supervises.
Service Ownership	Represents the service entity that a user owns. You must use this query subject with the Person query subject to obtain information about the services that the user own.
Roles Ownership	Represents the role entity that a user owns. You must use this query subject with the Person query subject to obtain information about the roles that the user own.
Group Ownership	Represents the group entities that a user own. You must use this query subject with the Person query subject to obtain information about the groups that the user owns.
Credential Pool Ownership	Represents the credential pool that a user owns. You must use this query subject with the Person query subject to obtain information about the credential pool that the user owns.
Separation of Duty Policy Ownership	Represents the separation of duty policies that a user own. You must use this query subject with the Person query subject to obtain information about the separation of duty policies that the user own.
User	Represents all users of type <i>person</i> and <i>business partner person</i> . Use this query to get a consolidated view of all users that are defined in the organization. You can use this query subject with the Person and Business Partner Person query subjects to retrieve more specific details about the user.

Query items for User Configuration namespace

The following table lists the query items in the User Configuration namespace.

Query subject	Query items and their description
<p>Person</p>	<p>Person Full Name The full name of a user.</p> <p>Person Last Name The surname of a user.</p> <p>Person Preferred User ID Represents the name that a user might prefer during an account creation.</p> <p>Person Email An email address of a user.</p> <p>Person Status The status of the user entity. The valid values are Active and Inactive.</p> <p>Person Business Unit Name The name of the business unit to which a user belongs.</p> <p>Person Administrative Assistant Dn An LDAP distinguished name for the administrative assistant of a user.</p> <p>Person Dn An LDAP distinguished name for a user.</p> <p>Person Business Unit Dn An LDAP distinguished name for the business unit to which a user belongs.</p> <p>Person Business Unit Supervisor An LDAP distinguished name for the supervisor of the business unit to which a user belongs.</p>
<p>Person Aliases</p>	<p>Person Alias Name The name of a user alias.</p> <p>Person Dn An LDAP distinguished name for the user to which an alias belongs.</p>
<p>Person Manager</p>	<p>Person Full Name The full name of the manager.</p> <p>Person Last Name The surname of the manager.</p> <p>Person Status The status of the manager entity. The valid values are Active and Inactive.</p> <p>Person Dn An LDAP distinguished name for the manager.</p> <p>Person Business Unit Dn An LDAP distinguished name for the business unit to which a manager belongs.</p> <p>Person Supervisor The user supervisor of the manager.</p>

Table 72. List of query items in the User Configuration namespace (continued)

Query subject	Query items and their description
<p>Account</p>	<p>Account Name The name of an account.</p> <p>Account Status The status of an account. The valid values are Active and Inactive.</p> <p>Account Compliance The compliance status of an account. The valid values are Unknown, Compliant, Disallowed, and Non Compliant.</p> <p>Account Ownership Type The ownership type of an account. The valid values are Individual, System, Device, and Vendor.</p> <p>Account Last Access Date The last accessed date of an account.</p> <p>Account Service Name The name of the service on which an account is provisioned.</p> <p>Account Service Type The profile of the service on which an account is provisioned.</p> <p>Account Service Url A URL that connects to the service on which an account is provisioned.</p> <p>Account Service Business Unit Name An LDAP distinguished name for the business unit to which a service belongs.</p> <p>Account Dn An LDAP distinguished name for an account.</p> <p>Account Service Dn An LDAP distinguished name for the service on which an account is provisioned.</p> <p>Account Service Business Unit Dn An LDAP distinguished name for the business unit to which a service belongs.</p> <p>Account Service Owner Dn An LDAP distinguished name for a user who is the owner of the service.</p> <p>Account Service Business Unit Supervisor Dn An LDAP distinguished name for the supervisor of the business unit to which a service belongs.</p> <p>Account Owner Business Unit Dn An LDAP distinguished name for the business unit of a user who owns the account.</p>
<p>Role</p>	<p>Role Name The name of a role.</p> <p>Role Description The description of a role.</p> <p>Role Type The type of a role. The valid values are Static and Dynamic.</p> <p>Role Access Enabled Represents whether or not access for a role is enabled. True represents Enabled, and False represents Disabled.</p> <p>Role Common Access Enabled Represents whether or not common access for the role is enabled. The valid values are True and False.</p> <p>Role Access Type The type of an access that is enabled for a role.</p> <p>Role Dn An LDAP distinguished name for the role.</p> <p>Role Business Unit Dn An LDAP distinguished name for the business unit of a role.</p>

Table 72. List of query items in the User Configuration namespace (continued)

Query subject	Query items and their description
Person ACI	<p>ACI Name The name of the Access Control Item (ACI).</p> <p>ACI Protection Category The category of an entity that an ACI protects. The value of this item must be Person.</p> <p>ACI Target The type of the selected protection category that is associated with an ACI. The valid values are inetOrgPerson and erPersonItem.</p> <p>ACI scope The scope of an ACI. It determines whether an ACI is applicable to subunits of a business organization or not. The valid values and their meanings:</p> <ul style="list-style-type: none"> • single - The policy applies to a business unit and not its subunits. • subtree - The policy applies to the subunits of a business organization. <p>ACI Business Unit Dn An LDAP distinguished name for the business unit on which an ACI is defined.</p>
ACI Operations	<p>ACI Operation Name The name of an operation that an ACI governs.</p> <p>ACI Operation Permission The permission that applies to an ACI operation. The valid values are grant, deny, and none.</p> <p>ACI Business Unit Dn An LDAP distinguished name for the business unit.</p>
ACI Attribute Permissions	<p>ACI Attribute Name The name of an attribute for which an ACI controls the permissions.</p> <p>ACI Attribute Operation The name of an operation that can be run on an attribute. The valid values are r for read operation, w for write operation, and rw for read and write operations.</p> <p>ACI Attribute Permission The permission that applies to an ACI operation. The valid values are grant and deny.</p> <p>ACI Business Unit Dn An LDAP distinguished name for the business unit.</p>
ACI Members	<p>ACI Member Name The members that an ACI governs. The valid values are:</p> <ul style="list-style-type: none"> • All Users - All users in the system. • Profile Owner - The owner of the profile. • Manager - The manager of the profile owner. • Sponsor - The sponsor of the Business Partner organization in which the person resides. • Administrator - The administrator of the domain in which the person resides. • Service Owner - The owner of the service. • Access Owner - The owner of an access. <p>ACI System Group Name Represents the name of the group whose members are governed by an ACI.</p> <p>ACI Business Unit Dn An LDAP distinguished name for the business unit.</p> <p>ACI System Group Dn An LDAP distinguished name for the system group.</p>

Table 72. List of query items in the User Configuration namespace (continued)

Query subject	Query items and their description
Supervised Business Unit	<p>Business Unit Name The name of a business unit.</p> <p>Business Unit Supervisor A user who is the supervisor of a business unit.</p> <p>Business Unit Dn An LDAP distinguished name for the business unit to which a user belongs.</p> <p>Business Unit Container Dn An LDAP distinguished name for the parent business unit of an organization entity.</p>
Service Ownership	<p>Service Name The name of a service to which the accounts are provisioned.</p> <p>Service Dn An LDAP distinguished name for the service.</p> <p>Service Container Dn An LDAP distinguished name for the business unit of a service.</p> <p>Service Owner Dn An LDAP distinguished name for a user who owns the service.</p> <p>Service Url A URL that connects to the managed resource.</p> <p>Service Type The service profile type.</p>
Roles Ownership	<p>Role Name The name of a role.</p> <p>Role Description The description of a role.</p> <p>Role Type The type of a role. The valid values are <code>Static</code> and <code>Dynamic</code>.</p> <p>Role Access Enabled Represents whether an access for a role is enabled or not. <code>True</code> represents Enabled, and <code>False</code> represents Disabled.</p> <p>Role Common Access Enabled Represents whether or not common access for the role is enabled. The valid values are <code>True</code> and <code>False</code>.</p> <p>Role Access Type The type of an access that is enabled for a role.</p> <p>Role Dn An LDAP distinguished name for a role.</p> <p>Role Business Unit Dn An LDAP distinguished name for the business unit of a role.</p>

Table 72. List of query items in the User Configuration namespace (continued)

Query subject	Query items and their description
<p>Group Ownership</p>	<p>Group Name The name of a group for which an access is defined.</p> <p>Group Type The profile type of a group.</p> <p>Group Access Name The name of an access that is defined for a group.</p> <p>Group Access Type The type of an access that is defined for a group.</p> <p>Group Service Name The name of a service on which the group is provisioned.</p> <p>Group Service Type The profile type of a service on which the group is provisioned.</p> <p>Group Service Url A URL that connects to the service to which the group is provisioned.</p> <p>Group Service Business Unit Name The name of a business unit to which the service belongs.</p> <p>Group Dn An LDAP distinguished name for a group entity to which an access is defined.</p> <p>Group Service Dn An LDAP distinguished name for the service that is associated to a group.</p> <p>Group Service Business Unit Dn An LDAP distinguished name for the business unit to which a service belongs.</p> <p>Group Service Owner Dn An LDAP distinguished name for a user who owns the service.</p> <p>Group Service Business Unit Supervisor An LDAP distinguished name for the supervisor of a business unit to which a service belongs.</p>
<p>Credential Pool Ownership</p>	<p>Credential Pool Name The name of a credential pool.</p> <p>Credential Pool Service Dn An LDAP distinguished name for a service to which the group associated with a credential pool is provisioned.</p> <p>Credential Pool Business Unit Dn An LDAP distinguished name for the business unit of a credential pool.</p> <p>Credential Pool Dn An LDAP distinguished name for the credential pool.</p>
<p>Separation of Duty Policy Ownership</p>	<p>Separation of Duty Policy Name The name of the separation of duty policy.</p> <p>Separation of Duty Policy Description The description of the separation of duty policy.</p> <p>Separation of Duty Policy Enabled Indicates whether or not the policy is enabled. True represents Enabled, and False represents Disabled.</p> <p>Separation of Duty Policy Business Unit Name The name of a business unit to which the separation of duty policy applies.</p> <p>Separation of Duty Policy Id A unique numeric identifier for the separation of duty policy.</p>

Table 72. List of query items in the User Configuration namespace (continued)

Query subject	Query items and their description
User	<p>Full Name The full name of the user.</p> <p>Last Name The surname of the user.</p> <p>Type The profile type of the user, which is either <i>person</i> or <i>business partner person</i>.</p> <p>Status The status of the user, which is either <i>Active</i> and <i>Inactive</i>.</p> <p>Supervisor The supervisor of the user.</p> <p>Business Unit Name The name of the business unit to which a user belongs.</p> <p>Dn An LDAP distinguished name for a user.</p> <p>Business Unit Dn An LDAP distinguished name for the business unit to which a user belongs.</p>

Service Audit namespace

The Service Audit namespace pertains to the audit history of the actions that are performed on the services. You can generate the audit reports for the various types of services.

Query subjects for Service Audit namespace

The following table lists the query subjects in the Service Audit namespace.

Table 73. Query subjects in the Service Audit namespace

Query subject	Description
Service	<p>Represents the service and its configuration attributes on which the audit actions are performed.</p> <p>Note: You cannot see the deleted services by using this query subject.</p>
Service Audit	<p>Represents the audited actions applicable to the services. You must use this query subject with the Service query subject.</p> <p>Note: You can use this query subject alone to report any deletion of the previously existing services.</p>
Service Health	<p>Represents the status of a resource on which the service is created. You must use this query subject with the Service query subject.</p>
Service Provisioning Policy	<p>Represents the provisioning policies that are applied on the service. You must use this query subject with the Service query subject.</p>

Query items for Service Audit namespace

The following table lists the query items in the Service Audit namespace.

Query subject	Query items and their description
Service	<p>Service Name The name of a service.</p> <p>Service Type The type of a service. For example, PosixLinuxProfile.</p> <p>Service Description The description of the service that is entered during the service creation or modification.</p> <p>Service Business Unit Name The business unit to which a service belongs.</p> <p>Service Url The IP address of the resource on which the service is created.</p> <p>Service Tag A tag that logically groups the services. If a service is tagged during creation or modification, this query item represents the name of the tag.</p> <p>Service Owner First Name The given name of a user who is the service owner.</p> <p>Service Owner Last Name The surname of a user who is the service owner.</p> <p>Service Owner Business Unit Dn An LDAP distinguished name for a business unit to which the service owner belongs.</p> <p>Service Dn An LDAP distinguished name for a service.</p>

Table 74. List of query items in the Service Audit namespace (continued)

Query subject	Query items and their description
<p>Service Audit</p>	<p>Audit Service Name The name of a service on which the audit action is run.</p> <p>Audit Service Business Unit The business unit of a service.</p> <p>Audit Action Represents an action that is run on the service. The possible values are:</p> <ul style="list-style-type: none"> • Add. • Delete. • Modify. • EnforcePolicyForService. • UseGlobalSetting. • CorrectNonCompliant. • SuspendNonCompliant. • AlertNonCompliant. • MarkNonCompliant. <p>Audit Comments The comments that are entered by the audit workflow approver. Along with the audit comments, this query item might contain the operational data.</p> <p>Audit Initiator Name The name of a user who initiates the action on the service.</p> <p>Audit Process Requestee Name The entity upon which an audit action is run.</p> <p>Audit Operation Start Time The start date and time when the operation on the service started.</p> <p>Audit Process Submission Time The date and time of the audit process submission.</p> <p>Audit Process Schedule Time The date and time at which an event is scheduled for the execution.</p> <p>Audit Process Completion Time The date and time of the audit process completion.</p> <p>Audit Process Subject The subject on which the audit action is run. It applies to the cases where the defined workflow must complete before the audit action is complete.</p> <p>Audit Process Subject Profile The profile type of an entity that is associated with the audit action. This query item contains a value only if the Audit Process Subject contains the value.</p> <p>Audit Process Result Summary The result of the audit process on the service that is indicated with the values such as Success or Failed.</p>

Table 74. List of query items in the Service Audit namespace (continued)

Query subject	Query items and their description
Service Health	<p>Resource Dn An LDAP distinguished name for the service.</p> <p>Resource Status Indicates whether or not resource that is represented by the service is available. The valid values are Success and Failed.</p> <p>Resource Test Status Indicates whether or not resource that is represented by the service is connectable. The valid values are Success and Failed.</p> <p>Last Response Time The date and time of the last received response from the resource that is represented by the service.</p> <p>Lock Service Shows if a service is locked. For example, Service is locked for the reconciliation.</p> <p>Last Reconciliation Time The last date and time when the reconciliation of the service is attempted either by the system or through an explicit request of the reconciliation.</p> <p>Server The application server on which the service that pertains to a resource is created. The details are up to the level of a node on which the service is created.</p> <p>Restart Time The time from the last restart of a server.</p> <p>First Resource Fail Time The date and time when the resource fails for the first time. Use this information to analyze the resource failure situations.</p>
Service Provisioning Policy	<p>Provisioning Policy Name The name of a provisioning policy that applies to a service.</p> <p>Provisioning Policy Scope The scope in terms of a hierarchy of the business units to which the provisioning policy applies. The valid values and their meanings:</p> <ul style="list-style-type: none"> • Single - The policy applies to a business unit and not its subunits. • Subtree - The policy applies to the business unit and its subunits. <p>Provisioning Policy Is Enabled Represents whether the provisioning policy is enabled or not. True represents Enabled, and False represents Disabled.</p> <p>Provisioning Policy Dn An LDAP distinguished name for the provisioning policy.</p> <p>Provisioning Policy Business Unit Dn An LDAP distinguished name for the business unit to which the provisioning policy applies.</p>

Access Audit(Deprecated) namespace

The Access Audit(Deprecated) namespace pertains to the audit history of the actions that are performed on the access entities. The access audit is supported for the group, role, and service that is defined as an access.

Query subjects for Access Audit(Deprecated) namespace

The following table lists the query subjects in the Access Audit(Deprecated) namespace.

Query subject	Description
Access Audit	Represents the audit history of the access entity. You must use this query subject with the Access query subject.
Access	Represents the access entity on which the audit actions are performed. This query subject also contains the configuration attributes of an access.
Access Owner	Represents a user who owns the access.

Table 75. Query subjects in the Access Audit (Deprecated) namespace (continued)

Query subject	Description
Access Owner Business Unit	Represents the business unit to which an access owner belongs. You must use this query subject with the Access Owner query subject to obtain the configuration information about the business unit that is associated with an owner.
Access Service	Represents the service on which the access is provisioned. You must use this query subject with the Access query subject to obtain the configuration information about the access service.
Access Service Business Unit	Represents the business unit to which a service belongs. You must use this query subject with the Access Service query subject to obtain the configuration information about the business unit that is associated with the service.
Access Members	Provides information about the accounts that are the members of an access.
Access Member Owner	Provides information about the users who own the accounts that are members of an access.
Access Member Owner Business Unit	Represents the business unit to which the access member owner belongs.

Query items for Access Audit (Deprecated) namespace

The following table lists the query items in the Access Audit (Deprecated) namespace.

Query subject	Query items and their description
Access Audit	<p>Audit Access Name The name of an access on which the audit operation is run.</p> <p>Audit Access Service Name The name of a service for which the access is defined.</p> <p>Audit Action An action that is run on the access. The valid values are:</p> <ul style="list-style-type: none"> • Add. • Modify. • Delete. • AddMember. • RemoveMember. <p>Audit Initiator Name The name of a user who initiates the audit action. For the audit actions such as AddMember and RemoveMember, the initiator name represents the name of IBM Security Identity Manager account.</p> <p>Audit Account Name The name of an account for which the access is either requested or deleted. This query item applies to only AddMember and RemoveMember audit actions.</p> <p>Audit Process Requestee Name The name of a user whose account is added to the access. This query item applies to only AddMember and RemoveMember audit actions.</p> <p>Audit Process Recertifier Name The name of a user who approves the audit action.</p> <p>Audit Operation Start Time The audit operation start date and time.</p> <p>Audit Activity Owner IBM Security Identity Manager account user name that owns the activity. For example, a user who approves the request to add an account to the access.</p> <p>Audit Activity Name The name of the audit activity.</p> <p>Audit Activity Start Time The audit activity start date and time.</p> <p>Audit Activity Completion Time The audit activity completion date and time.</p> <p>Audit Process Submission Time The audit process submission date and time.</p> <p>Audit Process Schedule Time The date and time at which an event is scheduled for the execution.</p> <p>Audit Process Completion Time The audit process completion date and time.</p> <p>Audit Activity Result Summary The result of an activity within a role audit process.</p> <p>Audit Comments The comments that are entered by the audit workflow approver.</p> <p>Audit Process Result Summary The result of the access audit process.</p>

Table 76. List of query items in the Access Audit (Deprecated) namespace (continued)

Query subject	Query items and their description
Access	<p>Group Name The name of a group for which the access is defined.</p> <p>Group Type The profile type of a group.</p> <p>Group Access Name The name of an access that is defined for a group.</p> <p>Group Access Type The type of an access that is defined for a group.</p> <p>Group Supervisor The name of a user who is the supervisor of a group.</p> <p>Group Dn An LDAP distinguished name for a group to which the access is defined.</p> <p>Group Container Dn An LDAP distinguished name for the business unit that is associated with a group.</p> <p>Group Owner Dn An LDAP distinguished name for a group owner.</p> <p>Group Service Dn An LDAP distinguished name for the service that is associated with a group.</p> <p>Group Access Defined Specifies whether or not access is defined for a group. The possible values are True and False.</p> <p>Group Access Enabled Specifies whether or not access is enabled for a group. The possible values are True and False.</p> <p>Group Common Access Enabled Specifies whether or not common access is enabled for a group. The possible values are True and False.</p>
Access Owner	<p>Access Owner Full Name The given name of an account owner.</p> <p>Access Owner Last Name The surname of an account owner.</p> <p>Access Owner Status The status of a user. The valid values are Active and Inactive.</p> <p>Access Owner Dn An LDAP distinguished name for an account owner.</p> <p>Access Owner Business Unit Dn An LDAP distinguished name for the business unit to which an account owner belongs.</p> <p>Access Owner Manager Dn An LDAP distinguished name for the user supervisor of the account owner.</p>
Access Owner Business Unit	<p>Business Unit Name The name of a business unit.</p> <p>Business Unit Supervisor The business unit of a user who is the supervisor.</p> <p>Business Unit Dn An LDAP distinguished name for the business unit.</p> <p>Business Unit Container Dn An LDAP distinguished name for the parent business unit.</p>

Table 76. List of query items in the Access Audit (Deprecated) namespace (continued)

Query subject	Query items and their description
Access Service	<p>Service Name The name of a service to which the access belongs.</p> <p>Service Dn An LDAP distinguished name for a service to which the access belongs.</p> <p>Service Container Dn An LDAP distinguished name for a business unit of a service that is associated with the access.</p> <p>Service Owner Dn An LDAP distinguished name for a user owner of the service.</p> <p>Service URL A URL that connects to the managed resource.</p> <p>Service Type The service profile type.</p>
Access Service Business Unit	<p>Business Unit Name The name of a business unit.</p> <p>Business Unit Supervisor A user who is the supervisor of a business unit.</p> <p>Business Unit Dn An LDAP distinguished name for a business unit.</p> <p>Business Unit Container Dn An LDAP distinguished name for the parent business unit.</p>
Access Members	<p>Account Name The name of an account that is a member of an access.</p> <p>Account Ownership Type The type of the account ownership. The valid values are:</p> <ul style="list-style-type: none"> • Device. • Individual. • System. • Vendor. <p>Account Status The status of an account. The valid values are Active and Inactive.</p> <p>Account Compliance Indicates whether an account is compliant or not. The valid values are:</p> <ul style="list-style-type: none"> • Unknown. • Compliant. • Non Compliant. • Disallowed. <p>Account Last Access Date The last accessed date and time of an account.</p> <p>Account Dn An LDAP distinguished name for an account.</p> <p>Account Service Dn An LDAP distinguished name for a service to which the account belongs.</p>
Access Member Owner	<p>Person Full Name The full name of an account owner.</p> <p>Person Last Name The surname of an account owner.</p> <p>Person Dn An LDAP distinguished name for an account owner.</p> <p>Person Business Unit Dn An LDAP distinguished name for the business unit to which an account owner belongs.</p> <p>Person Supervisor A user who is the supervisor of an account owner.</p>

Table 76. List of query items in the Access Audit (Deprecated) namespace (continued)

Query subject	Query items and their description
Access Member Owner Business Unit	<p>Business Unit Name The name of a business unit to which the account owner belongs.</p> <p>Business Unit Supervisor A user who is the supervisor of a business unit.</p> <p>Business Unit Dn An LDAP distinguished name for a business unit.</p> <p>Business Unit Container Dn An LDAP distinguished name for the parent business unit of an organization entity.</p>

Access Audit namespace

Use the access audit model and reports to view the details about the accesses that are associated with a user.

The Access Audit namespace pertains to the audit history of the actions that are performed on the access entities in Identity Service Center. The access audit is supported for the group, role, and service that is defined as an access.

Note: If the account is on the service that is defined as an access, the audit details can be seen only in the Access Audit namespace.

Query subjects for Access Audit namespace

The table lists the query subjects in the Access Audit namespace.

Table 77. Query subjects in the Access Audit namespace

Query subject	Description
Access Audit	The audit history of the access entity. You must use this query subject with the Access query subject.
Access Audit Obligation Attributes	The obligation attributes of an access and their values. You must use this query subject with the Access Audit query subject.
Access	The access entity on which the audit actions are performed. This query subject also contains the configuration attributes of an access.
Access Owner	A user who owns the access.

Query items for Access Audit namespace

The table lists the query items in the Access Audit namespace.

Query subject	Query items and their description
Access Audit	<p>Audit Access Name The name of an access on which the audit operation is run.</p> <p>Audit Action An action that is run on the access. The valid values are Add, Edit, or Delete.</p> <p>Audit Comments The comments that are entered by the audit workflow approver.</p> <p>Audit Initiator Name The name of a user who initiates the audit action. For the audit actions such as Add, Edit, or Delete, the initiator name represents the name of IBM Security Identity Manager account.</p> <p>Audit Account ID An account identifier of a user for whom the access is requested.</p> <p>Audit Access Requestee Name The name of a user whose account is added to the access.</p> <p>Audit Access Approver Name The name of a user who approves the audit action.</p> <p>Audit Access Approver Account ID An account identifier of an audit approver.</p> <p>Audit Access Business Unit The name of an audit access business unit.</p> <p>Audit Workflow Process ID A unique identifier for a workflow process that is associated with the access request.</p> <p>Audit Operation Start Time The audit operation start date and time.</p> <p>Access Type Code The code for an audit entity type. The possible values are 1, 2, and 3. 1 represents service, 2 represents group, and 3 represents role.</p> <p>Audit Access Type The type of an access. For example, Application, Role, Email group, or Shared Folder.</p> <p>Audit Access Badge Text 1, Audit Access Badge Text 2, Audit Access Badge Text 3, Audit Access Badge Text 4, Audit Access Badge Text 5 The badge text that is defined for an access.</p> <p>Audit Access ID A unique identifier of an access on which the audit operation is run.</p>

Table 78. List of query items in the Access Audit namespace (continued)

Query subject	Query items and their description
<p>Access Audit (Continued)</p>	<p>Audit Access Request Justification The reason for the access request.</p> <p>Audit Activity Name The name of an audit activity.</p> <p>Audit Activity ID A unique identifier of an audit activity.</p> <p>Audit Activity Start Time The audit activity start date and time.</p> <p>Audit Activity Due Time The date and time when the audit activity is due for an approval.</p> <p>Audit Activity Escalation Time The escalation date and time of an audit activity.</p> <p>Audit Activity Completion Time The audit activity completion date and time.</p> <p>Audit Access Request Completion Time The date and time when an access request is completed.</p> <p>Audit Access Request Status The status of an access request. The possible values are Fulfilled, Not Fulfilled, Submitted, or Pending.</p> <p>Audit Activity Approval Status An approval status of an audit activity. For example, Approved, Rejected, or Pending.</p> <p>Audit Activity Approval Action The status of an action that is taken on the activity. For example, Completed or Escalated.</p> <p>Audit Action Code A code for the audit action. the possible values are ADD, CHANGE, or DELETE.</p> <p>Access Audit Obligation ID A unique obligation identifiers of an access. There can be multiple obligation identifiers that are separated by a comma.</p>
<p>Access Audit Obligation Attributes</p>	<p>Access ID A unique identifier of an access on which the audit operation is run.</p> <p>Access Audit Obligation ID A unique obligation identifier of an access.</p> <p>Access Account Attribute Name The attribute name of an account that belongs to the access.</p> <p>Access Account Attribute Previous Value The previous value of an account attribute that belongs to an access. If the attribute is edited for the first time, the previous value is empty or null.</p> <p>Access Account Attribute Modified Value The modified value of an account attribute that belongs to an access.</p>

Table 78. List of query items in the Access Audit namespace (continued)

Query subject	Query items and their description
<p>Access</p>	<p>Access Dn An LDAP distinguished name for an access.</p> <p>Access Name The name of an access.</p> <p>Access Type The type of an access. The possible values are Group, Role, or Service.</p> <p>Access Description The description of an access.</p> <p>Access Category A category of an access. For example, Application, Role, Email Group, or Shared Folder.</p> <p>Access Icon URL A URL that is defined for an access icon.</p> <p>Access Additional Information An additional information about the access.</p> <p>Access Enabled Specifies whether access is enabled. The possible values are True and False.</p> <p>Access Common Enabled Specifies whether common access is enabled. The possible values are True and False.</p>
<p>Access Owner</p>	<p>Access Dn A distinguished name of an access.</p> <p>Access Owner Dn A distinguished name for an access owner.</p> <p>Access Owner The name of an access owner.</p> <p>Access Owner Type The type of an access owner. For example, Person or Role.</p> <p>Access Owner Status The status of an access owner. For example, Active and Inactive. The access owner status is not applicable if an owner type is a role.</p> <p>Access Owner Manager Dn A distinguished name for a manager of an access owner.</p> <p>Access Owner Business Unit The business unit name of an access owner.</p> <p>Access Owner Business Unit Dn A distinguished name for a business unit of an access owner.</p>

Access Configuration namespace

Use the Access Configuration namespace to view access configuration and its business metadata for the access entities.

Query subjects for Access Configuration namespace

The following table lists the query subjects in the Access Configuration namespace.

Query subject	Description
Access	Represents an access that is defined in an organization. You can use this query subject with either of the following query subjects to obtain the business metadata for each access: <ul style="list-style-type: none">• Service Business Meta Data.• Group Business Meta Data.• Role Business Meta Data.
Service	Represents the services that are defined in an organization with its configuration attributes. You can use this query subject with either of the following query subjects to view the service that is defined as an access: <ul style="list-style-type: none">• Access.• Service Business Meta Data.
Service Business Meta Data	Represents the business metadata of the service that is defined as an access.
Group	Represents the groups that are defined in an organization with its configuration attributes. You can use this query subject with either of the following query subjects to view the groups that are defined as an access: <ul style="list-style-type: none">• Access.• Group Business Meta Data. Note: Group information is displayed if group access is set to enabled or common access enabled.
Group Access Owner	Represents a user who owns the group access. The query subject shows a unified view of a Person and Business Partner Person.
Group Business Meta Data	Represents the business metadata of the group that is defined as an access.
Role	Represents the role that is defined in an organization with its configuration attributes. Note: Role information is displayed if role access is set to enabled.
Role Business Meta Data	Represents the business metadata of the role that is defined as an access.
Business Partner Person	Represents the Business Partner person entity and its configuration attributes.
Person	Represents a person entity and its configuration attributes.
User	Represents all users of type <i>person</i> and <i>business partner person</i> . Use this query to get a consolidated view of all users that are defined in the organization. You can use this query subject with the Person and Business Partner Person query subjects to retrieve more specific details about the user

Query items for Access Configuration namespace

The following table lists the query items in the Access Configuration namespace.

Query subject	Query items and their description
Access	Access Name The name of the access that is defined in an organization. Access Category The category of the access application, email group, role, shared folder, or any other custom category that is defined. Access Dn An LDAP distinguished name for an access.

Table 80. List of query items in the Access Configuration namespace (continued)

Query subject	Query items and their description
Service	<p>Service Name The name of the service or resource that is defined in an organization.</p> <p>Service Type The type of a service. For example, PosixLinuxProfile.</p> <p>Service Dn An LDAP distinguished name for a service.</p> <p>Service Business Unit Dn An LDAP distinguished name for a business unit of a service.</p> <p>Service ID A unique identifier that represents the service.</p>
Service Business Meta Data	<p>Access ID A unique identifier that represents the business metadata for a service that is defined as an access.</p> <p>Access Description The description of a service that is defined as an access.</p> <p>Access Status Provides the state of access definitions. For example: access is enabled, or common access is enabled.</p> <p>Access Icon Url A uniform resource identifier (URL) string for the icon that represents an access.</p> <p>Access Additional Information Displays information about the access card by default. It is an extra information about the access item that an administrator can use.</p> <p>Access Badge Style Represents the class that applies the formatting to the badge text such as, font type, size, or color.</p> <p>Access Badge Text Provides the details about the badge that is defined for an access.</p> <p>Access Search Terms Displays the search string for a service defined as an access.</p>
Group	<p>Group Name The name of the group that is defined in an organization.</p> <p>Group Type The profile type of a group.</p> <p>Group Dn An LDAP distinguished name for a group.</p> <p>Group Business Unit Dn An LDAP distinguished name for the business unit of a group.</p> <p>Group Owner Dn An LDAP distinguished name of an owner that owns the group.</p> <p>Group Service Dn An LDAP distinguished name of a service to which the group belongs.</p>

Table 80. List of query items in the Access Configuration namespace (continued)

Query subject	Query items and their description
Group Business Meta Data	<p>Access Name The name of an access of a type as group.</p> <p>Access Description The description of a group that is defined as an access.</p> <p>Access Status Provides the state of access definitions. For example: access is enabled, or common access is enabled.</p> <p>Access Icon Url A uniform resource identifier (URL) string for the icon that represents an access.</p> <p>Access Additional Information Displays information about the access card by default. It is an extra information about the access item that an administrator can use.</p> <p>Access Badge Style Represents the class that applies the formatting to the badge text such as, font type, size, or color.</p> <p>Access Badge Text Provides the details about the badge that is defined for an access.</p> <p>Access ID A unique identifier that represents the business metadata for a group that is defined as an access.</p> <p>Access Search Terms Displays the search string for a group defined as an access.</p>
Group Access Owner	<p>Full Name The full name of the user.</p> <p>Last Name The surname of the user.</p> <p>Type The profile type of the user, which is either <i>person</i> or <i>business partner person</i>.</p> <p>Status The status of the user, which is either <i>Active</i> and <i>Inactive</i>.</p> <p>Supervisor The supervisor of the user</p> <p>Business Unit Name The name of the business unit to which a user belongs.</p> <p>Dn An LDAP distinguished name for a user.</p> <p>Business Unit Dn An LDAP distinguished name for the business unit to which a user belongs.</p>
Role	<p>Role Name The name of a role.</p> <p>Role Type The type of a role. The valid values are <i>Static</i> and <i>Dynamic</i>.</p> <p>Role Dn An LDAP distinguished name for a role.</p> <p>Role Business Unit Dn An LDAP distinguished name for the business unit of a role.</p> <p>Role Supervisor The supervisor of a user for the business unit of a role.</p> <p>Role Owner Dn An LDAP distinguished name for the role owner.</p>

Table 80. List of query items in the Access Configuration namespace (continued)

Query subject	Query items and their description
Role Business Meta Data	<p>Access Name The name of an access of a type as role.</p> <p>Access Description The description of a role that is defined as an access.</p> <p>Access Status Provides the state of access definitions. For example: access is enabled, or common access is enabled.</p> <p>Access Icon Url A uniform resource identifier (URL) string for the icon that represents an access.</p> <p>Access Additional Information Displays information about the access card by default. It is an extra information about the access item that an administrator can use.</p> <p>Access Badge Style Represents the class that applies the formatting to the badge text such as, font type, size, or color.</p> <p>Access Badge Text Provides the details about the badge that is defined for an access.</p> <p>Access ID A unique identifier that represents the business metadata for a role that is defined as an access.</p> <p>Access Search Terms Displays the search string for a role defined as an access.</p>
Business Partner Person	<p>Business Partner Person Full Name The full name of a user.</p> <p>Business Partner Person Last Name The surname of a user.</p> <p>Business Partner Person Supervisor An LDAP distinguished name for the supervisor of a user.</p> <p>Business Partner Person Status The status of a user entity. The valid values are <i>Active</i> and <i>Inactive</i>.</p> <p>Business Partner Person Dn An LDAP distinguished name for a user.</p> <p>Business Partner Person Business Unit Dn An LDAP distinguished name for the business unit to which a user belongs.</p> <p>Business Partner Person Parent The name of the parent business partner person.</p>
User	<p>Full Name The full name of the user.</p> <p>Last Name The surname of the user.</p> <p>Type The profile type of the user, which is either <i>person</i> or <i>business partner person</i>.</p> <p>Status The status of the user, which is either <i>Active</i> and <i>Inactive</i>.</p> <p>Supervisor The supervisor of the user</p> <p>Business Unit Name The name of the business unit to which a user belongs.</p> <p>Dn An LDAP distinguished name for a user.</p> <p>Business Unit Dn An LDAP distinguished name for the business unit to which a user belongs.</p>

References

Reference information is organized to help you locate particular facts quickly, such as the mapping attributes, entities, or scenario to configure the report model.

Mapping the attributes and entities

You must map the following attributes to the entities to work with the query items for the IBM Security Identity Manager Cognos report models.

Note: After you map the schema by using IBM Security Identity Manager administration console, it might take some time to reflect the updated data in the Cognos report. You must run a successful data synchronization after mapping the attributes. You must restart IBM Cognos Analytics server to reflect the updated schema in the report.

Namespace	Entity	Attribute Name
Account Audit	Business partner person	Status
Account Configuration	Organizational Role	<ul style="list-style-type: none"> Access Name Object profile name
	Identity policy	<ul style="list-style-type: none"> Policy Name Policy Target Enabled Scope UserClass
	Password policy	<ul style="list-style-type: none"> Policy Name Policy Target Enabled Scope
	Account	Account Ownership Type
	Business partner person	Status
Role Configuration	Organizational Role	<ul style="list-style-type: none"> Access Name Access Options Object profile name Owner
Provisioning Policy Config	Provisioning policy	<ul style="list-style-type: none"> Enabled Entitlement Ownership Type Priority Scope
	Business partner person	<ul style="list-style-type: none"> Full name Last name Parent DN Sponsor
Recertification Audit	Account	Account Ownership Type
Recertification Config	Account	Account Ownership Type
	Group	<ul style="list-style-type: none"> Access description Group description Group name
	Recertification policy	Scope
User Audit	Business partner person	Status

Table 81. Mapping the attributes and entities (continued)

Namespace	Entity	Attribute Name
User Configuration	Account	Account Ownership Type
	Person	<ul style="list-style-type: none"> • Administrative Assistant • Preferred user ID • E-mail address • Aliases
	Organizational Role	<ul style="list-style-type: none"> • Access Name • Access Options • Object profile name • Owner
	Business partner person	<ul style="list-style-type: none"> • Organizational roles • Status
Service Audit	Service	Tag
	Provisioning policy	<ul style="list-style-type: none"> • Enabled • Priority • Scope
Access Audit	Group	<ul style="list-style-type: none"> • Access Options • Group name
	Organizational Role	<ul style="list-style-type: none"> • Access Name • Object profile name
Access Configuration	Business partner person	<ul style="list-style-type: none"> • Full Name • Last Name • Organizational Unit Name • Organizational roles • Status
	Person	<ul style="list-style-type: none"> • Organizational roles

Report model configuration by using IBM Cognos components

To customize reports, you might be required to configure the report model. The following table provides a list of the basic tasks for configuring any IBM Cognos report model. It also provides information about the user guide for some IBM Cognos components.

Table 82. Basic tasks to configure report model

Tasks	Access the IBM Cognos Analytics documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html
Framework Manager user guide.	See the IBM Cognos Framework Manager documentation at https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.ug_fm.doc/ug_fm.pdf
Import the metadata from the relational database.	Search for Importing metadata from relational databases.
Create a relationship.	Search for Creating relationships.
Modify a relationship.	Search for Modifying a relationship.
Create a complex expression for a relationship.	Search for Creating complex expressions for a relationship.
Create a data source query subject.	Search for Data source query subjects.
Create a model query subject.	Search for Model query subjects.

Table 82. Basic tasks to configure report model (continued)

Tasks	Access the IBM Cognos Analytics documentation at http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html
Update query subjects.	Search for Updating query subjects .
Create or modify a package.	Search for Creating or modifying packages .
Publish a package.	Search for Publishing packages .

Migration of Tivoli Common Reporting reports to IBM Cognos reports

You can use the reference of the following link to convert Tivoli Common Reporting reports to IBM Cognos reports.

The following link provides information about converting the Business Intelligence and Reporting Tools (BIRT) reports to IBM Cognos reports. You can obtain the reference by using the following link to convert Tivoli Common Reporting reports to IBM Cognos reports. See http://www.ibm.com/support/knowledgecenter/SSH2DF_2.1.1/ttcr_converting_birt_to_cognos.html.

Scenarios

See the possible scenarios that can be used to customize the IBM Security Identity Manager Cognos report model.

Adding custom tables

The scenario describes the steps to add or import custom tables in IBM Security Identity Manager Cognos model.

Before you begin

- Install and configure IBM Cognos Analytics server.
- Install IBM Framework Manager.
- Map the user and its required attributes through schema mapper in IBM Security Identity Manager Console and run the data synchronization.

About this task

You can define the custom types or objects in IBM Security Identity Manager. By default, IBM Security Identity Manager provides the objects `Person` and `Business Partner Person` for a `User` entity. You can further define your own object classes that can be used as the custom person or custom Business Partner person types. For example, `JKPerson`.

Consider that a custom user `JKPerson` defined in IBM Security Identity Manager. With this customization in IBM Security Identity Manager, there are two profiles or types of a user. The `Person` is a type that is provided by default and a new customized person `JKPerson`.

Procedure

1. Extract the `ISIMReportingModel_6.0.0.6.zip` to the local disk.
2. Create a project in IBM Cognos Framework Manager and open `.cpf` file for the model customization.

Note: Open an existing project if any customization is already done in IBM Security Identity Manager metadata model.
3. Navigate to the **Database Layer**.
4. Select the **Database Layer**.
5. Right click, and then select **Run Metadata Wizard**.
6. Select `ISIM` as a data source from the list that is defined in IBM Cognos, and then click **Next**.
7. Select the objects that you want to import, and then click **Next**.
For example, `JKPerson`, `JKPerson_CN`, or `JKPerson_SN`.

8. On **Generate Relationships** panel, clear the **Use primary and foreign keys** check box.
9. Click **Import**.

Results

JKPerson, JKPerson_CN, or JKPerson_SN are added to the database layer in metadata model. Similarly, you can import the other required tables that you want.

Creating a relationship with the existing tables

The scenario describes the steps to create a relationship with any existing custom table.

Before you begin

- Install and configure IBM Cognos Analytics server.
- Install IBM Framework Manager.
- Map the user and its required attributes through schema mapper in IBM Security Identity Manager Console and run the data synchronization.

About this task

IBM Security Identity Manager Cognos report model is divided into two basic namespaces: audit and configuration. Audit namespace provides the tables or query subjects that helps to generate the audit reports. Configuration namespace provides the configuration information that helps to generate configuration reports.

You can define the custom types or objects in IBM Security Identity Manager. By default, IBM Security Identity Manager provides the objects `Person` and `Business Partner Person` for a `User` entity. You can further define your own object classes that can be used as the custom person or custom `Business Partner` person types. For example, `JKPerson`.

The `JKPerson` is of a type `User`. Therefore, navigate to the `User` configuration namespace to merge the `JKPerson`.

Procedure

1. Extract the `ISIMReportingModel_6.0.0.6.zip` to the local disk.
2. Create a project in IBM Cognos Framework Manager and open `.cpf` file for the model customization.
Note: Open an existing project if any customization is already done in IBM Security Identity Manager metadata model.
3. Navigate to the **Database Layer**.
4. Hold the **Ctrl** key, and select the `JKPerson` and `JKPerson_CN` tables.
5. Right click, and then select **Create > Relationship**.
6. Set the **Cardinality**, and then click **OK**.
7. Create a relationship between the `JKPerson` and `JKPerson_SN` tables
8. A common entity such as `User` lists all types of the users.
For example, `Person`, `Business Partner Person`, or `JKPerson`.

To create a common entity, pick the common attributes in them. Assuming that the `cn`, `sn`, `businessunit dn`, and `dn` are the attributes that are must, create the `JKPerson Must Attributes` query subject that contains the attributes that are must. Rename an individual item to some business names. For example, `CN` to `Full Name`, `SN` to `Last Name`.

Introduce one more data item as `Type`. The `Type` attribute indicates the type of a user such as `JKPerson`.

- a) Navigate to the **Database Layer**.
- b) Select the **Database Layer**.
- c) Right click, and then select **Create > Query subject**.

- d) Select the type as a Model query subject.
 - e) Provide the name to the query subject.
For example, JKPerson Must Attributes.
 - f) Click **OK**.
The **Query Subject Definition** window is displayed.
 - g) Navigate to the **Database Layer**.
 - h) Add JKPerson DN, Business Unit Dn from the JKPerson query subject.
 - i) Add JKPerson_CN from the JKPerson_CN and JKPerson_SN from the JKPerson_SN.
 - j) Add a Type data item to indicate the type of a user.
 - 1) Click **Add** link.
 - 2) Provide the **Type** as a name to the item.
 - 3) In the expression definition, add the JKPerson.
 - 4) Click **OK**.
9. Edit the union definition for the User query subject and include newly added JKPerson Must Attributes query subject.
10. Select User, right click, and test the results.
11. Optional: Create a shortcut of User and use it in the namespace.
For example, User Configuration.
- a) Select a User from the database layer.
 - b) Right click, and select **Create > Shortcut**.
 - c) Drag the shortcut to User Configuration namespace.
 - d) Rename the shortcut query to JKPerson or some business name and use it as per the requirement.

Results

The relationship is created with the existing tables.

Adding custom attributes to an existing query subject

The static report does not show an email address. You can configure the report model to add custom attributes such as, an email address. The scenario describes how to configure model so that you can view or drag the email addresses of the users in the reports.

Before you begin

- Install and configure IBM Cognos Analytics server.
- Install IBM Framework Manager.

Procedure

1. Add the E-mail property to the ISIM database schema.
 - a) In the IBM Security Identity Manager console, select **Reports > Schema Mapping**.
 - b) From the **Entities** list, select **Person** entity.
 - c) From the unmapped attribute list, select **E-mail address**.
 - d) Click **Add**.
2. Run the data synchronization tool.
 - a) Select **Reports > Data Synchronization**.
 - b) Click **Run Synchronization Now**.
3. Add the information about email address in the ISIMReportingPackage_6.0.0.6.zip.
 - a) Open the Framework Manager.

- b) Extract the ISIMReportingModel_6.0.0.6.zip to the local disk.
 - c) Open the .cpf file in the ISIMReportingModel_6.0.0.6 folder.
 - d) Right click the IBM Identity Security Manager (ISIM) namespace and select **Run Metadata Wizard**.
 - e) From the **Metadata Wizard** window, select **Data Source** and click **Next**.
 - f) Select **ISIM** and click **Next**.
 - You must use the data source name as **ISIM**.
 - g) Select the ITIMUSER object and click **Tables**.
 - h) Select the PERSON_MAIL table and click **Next**.
 - i) Clear the **Use primary and foreign keys** check box.
 - j) Click **Import**.
 - k) Click **Finish**.
4. Create a relationship between the PERSON and PERSON_MAIL table.
 - a) Hold the Ctrl key and select the PERSON and PERSON_MAIL tables.
 - b) Right click and select **Create > Relationship**.
 - c) Set the **Cardinality** of the following items:
 - PERSON table to 1..1
 - PERSON_MAIL table to 0..1
 - d) Click **OK**.
 5. Publish the modified model.
 - a) In the Framework Manager console, expand **Packages**.
 - b) Right click the metadata model and click **Publish Packages**.
 - c) Click **Next** twice.
 - d) Click **Publish**.
 - e) If the package was published previously, a message prompts for the confirmation. Click **Yes**.
 - f) Click **Finish**.

Results

You can view the email addresses in the reports.

Troubleshooting report problems

The following section describes solutions for the IBM Security Identity Manager Cognos report problems.

Problems and their solutions

Unable to view the IBM Security Identity Manager Cognos drill through reports in Microsoft Internet Explorer version 10

If you are using the Microsoft Internet Explorer version 10 browser, the IBM Security Identity Manager Cognos drill through reports might not work.

Solution

Complete the following steps:

1. Enable the compatibility view.
 - a. In the Microsoft Internet Explorer 10 menu, go to **Tools**.
 - b. Select **Compatibility View**.
2. Add the IBM Cognos website to the trusted sites list.
3. In the Microsoft Internet Explorer 10 menu, go to **Tools > Internet Options**.
4. On the **Security** tab, click the **Trusted sites** icon.

5. Click **Sites**.
6. In the **Add this website to the zone** box, add the IBM Cognos website address.
7. Click **Add**.
8. Click **Close**.

IBM Cognos audit history report does not show the audit of an account that is provisioned on the managed resource

IBM Cognos audit history for an account does not show the audit of the account that is provisioned on the managed resource when "Default Account Request Workflow" is configured with the entitlements that are associated with the provisioning policy.

Solution

To generate the audit history reports for the accounts with the default workflow, clear the **Approval Start Date** and **Approval End Date** check boxes, and then run the report.

IBM Security Identity Manager Cognos report execution fails on Oracle data source

During the report generation on Oracle data source, if you select more than 1000 filter values on the prompt page, the report execution fails.

Solution

1. Open the report in IBM Cognos Report Studio.
2. Open the prompt page and edit the property **Rows Per Page** for all input widgets.
3. Set the value to less than or equal to 1000.

The scope for the default provisioning policy is shown as blank on Oracle database.

When you generate the customized IBM Cognos report that includes provisioning policy scope in it, the scope for the default provisioning policy is shown as blank. This issue is specific to Oracle database.

Solution

If the scope for the default provisioning policy is shown as blank on Oracle database, then, interpret the scope of a provisioning policy as Subtree.

No data is displayed in the IBM Security Identity Manager Cognos audit history report

Account audit is not supported for an account that is added and does not have a defined workflow. To audit the accounts for an audit history report, the default workflow or custom workflow must be attached to the provisioning policy that is created.

Long filter values are not shown completely on the prompt pages

Follow the technote link <http://www-01.ibm.com/support/docview.wss?uid=swg21341018> to resolve this issue. The information in the technote also applies to IBM Cognos Analytics version 11.0.13.

Known limitations

The Prompt Page Summary table in the IBM Cognos Report shows "--" as the parameter value when more than 1000 filters per prompt is selected.

IBM Cognos Reports provide the option for multiple selection. You can select more than one value for each parameter in the prompt page. When you select several values to filter the report, text overflow can occur and '--' is displayed instead in the Prompt Page Summary table.

Solution

Avoid selecting too many values for each parameter in the prompt page.

IBM Cognos Reports do not display the actual values of custom labels that are defined in the Custom Labels properties file

IBM Security Identity Manager supports the use of custom labels. You can specify these labels in the CustomLabels_<locale>.properties file. Custom labels are defined in a key-value pair format. This key can be used to set custom access types, access badges, and others.

For example:

- *Custom access badge label:* \$OPDData

- *Custom access badge label value: Critical*

You can view the access catalog information or entitlements from the following IBM Security Identity Manager reports:

- Access Definition Report
- User Access Report

These reports list all access that is defined in the IBM Security Identity Manager console. When you define an access badge in the IBM Security Identity Manager console, the value can be:

- Derived from the CustomLabels_<locale>.properties file. For example: \$OPDData OR
- A regular string value. For example: "Sensitive data"

For custom labels, these reports display the key for the respective label. For example: \$OPDData. You must see the CustomLabels_<locale>.properties file to get the actual value of the custom label.

Disabled access is not displayed in the User Access Report

The access that is defined on groups and roles cannot be displayed in the User Access Report if the access is disabled.

User entitlements are not displayed in Legacy Administrator console reports and in BIRT reports

Both the Legacy Administrator console reports and BIRT reports do not show the entitlements that are granted to an individual when the provisioning policy membership is set to "All Other Users". To resolve the problem, use Cognos-based entitlements granted to an individual report to get the entitlement details.

Audit of the disconnected credentials in the IBM Cognos shared access history report

In IBM Security Identity Manager, a user can disconnect the shared access credentials in the credential vault. After the credentials are disconnected, the credentials in the vault do not have a connection with an account.

IBM Cognos shared access history report does not include the check-out and check-in history of the credentials that are not connected to an account. The shared access history report does not show the disconnected credentials for check-out and check-in audit action.

IBM Cognos entitlements report shows the provisioning policy data that is in the draft state

The IBM Cognos entitlements report shows the entitlements that are granted to an individual. It lists all the users and the items for which they are entitled. The report also shows the provisioning policy information that includes the policies that are saved in the draft state.

Cannot truncate the length of the text in the pie charts

An option or a property that can be set to truncate the length of the text is not available for the pie charts. You cannot truncate the length of the text in the pie charts.

Duplicate entries of the account add operation are observed when you run the account audit report

Duplicate entries of the account add operation are observed if the provisioning policy is configured with the default workflow and an extra custom workflow is created in IBM Security Identity Manager Console under **Configure System > Manage Operations**.

Solution

Remove the default workflow that is defined in the provisioning policy. Therefore, only the custom workflow that is defined would be effective, which would be captured in the account audit report.

Custom workflows that are defined in IBM Security Identity Manager are not supported for the following type of actions on an account

Only the default workflows are supported for the following actions on an account.

- Restore
- Suspend

Audit of the custom access type is not supported in the access audit history report

Any custom access type that is defined as access for a role, service, or group cannot be audited in the access audit history report.

IBM Security Identity Manager console reports

The section provides information about IBM Security Identity Manager console reports.

Types of reports

View descriptions of the reports that you can generate for IBM Security Identity Manager.

Requests

Account Operations

A report that lists all account requests. Allows filtering by account operation, service, and other fields.

Account Operations Performed by an Individual

A report that lists account requests made by a specific user. Allows filtering by the user who made the request in addition to other fields.

Approvals and Rejections

A report that lists request approval activities that were approved or rejected. Allows filtering by activity approver, service, and other fields.

Operation Report

A report that lists all operations submitted in the system. Allows filtering by requestee, operations, and the request start date and end date.

Pending Approvals

A report that lists the request activities submitted but not yet approved. Allows filtering by service, activity status, and other fields.

Rejected Report

A report that lists all rejected requests. Allows filtering by requestee and the request start date and end date.

User Report

A report that lists all requests, shows the set of operations that were requested, who the operations were requested for, and who requested them. Allows filtering by requestor, requestee, and the request start date and end date.

User and Accounts

Account Report

A report that lists accounts for a business unit. Allows filtering by service and business unit.

Accounts/Access Pending Recertification Report

A report that lists all pending recertifications for access definitions and accounts. Allows filtering by account or access owner, service type, and service.

Individual Access

A report that lists user access definitions selected by individual account owner, business unit, access, or service. Allows filtering by a user that owns accesses, business unit of the user, access defined in the system, and service where access is supported.

Individual Accounts

A report that lists the accounts and their owners. Allows filtering by user.

Individual Accounts by Role

A report that lists accounts owned by users of a specific role that is a member of provisioning policy. Allows filtering by role and business unit.

Recertification Change History Report

A report that lists the recertification history of accounts and user accesses. Allows filtering by account or access owner, recertification response, start date and end date, and other fields.

Suspended Individuals

A report that lists all individuals that are suspended. Allows filtering by date.

Services

Reconciliation Statistics

A report that lists the activities that occurred during the last completed reconciliation of a service, regardless of when the report data was synchronized. Remote services provide reconciliation statistics during a reconciliation. This report contains data from the last service reconciliation. Data synchronization is not a report prerequisite. Allows filtering by service.

Services

A report that lists services currently defined in the system. Allows filtering by service type, service, owner and business unit.

Summary of Accounts on Service

A report that lists the accounts on a specified service. Allows filtering by service and account status.

Audit and Security

Access Control Information (ACIs)

A report that lists all access control items in the system. Allows filtering by access control item name, protection category, object type, scope, and business unit.

Access Report

A report that lists all access definitions in the system. Allows filtering by access type, access entitlement, service type, service, and administration owner of an access definition.

Audit Events

A report that lists all audit events. Allows filtering by audit event category, action, initiator, start date, and end date.

Dormant Accounts

A report that lists the accounts that have not been used recently. An account that does not have last access information is not considered dormant, including new accounts where the last access date is blank. These types of accounts are not displayed in a dormant report. Allows filtering by service and dormant period.

Entitlements Granted to an Individual

A report that lists all users with the provisioning policies for which they are entitled. Allows filtering by user.

Note: This report shows direct entitlements and not inherited entitlements.

Non-Compliant Accounts

A report that lists all accounts that are noncompliant. Allows filtering by service and the reason for noncompliance.

Orphan Accounts

A report that lists all accounts that do not have an owner. Allows filtering by service and account status.

Policies

A report that lists target and memberships of the provisioning policies in the system. Allows filtering by policy name.

Policies Governing a Role

A report that lists all provisioning policies for a specified organization role. Allows filtering by role name.

Recertification Policies Report

A report that lists all recertification policies. Allows filtering by policy target type, service type, service, access type, and access.

Suspended Accounts

A report that lists the accounts that are suspended. Allows filtering by user, account, service, and date.

Generating reports

You can generate reports based on requests, user and accounts, services, or audit and security.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Reports of subsets of information can help you discover trends that can help you identify ways to improve your business process.

To generate a report, select the type of report you want to generate, and specify the criteria of the report. The criteria you specify depends on the type of report and controls the scope and quantity of the report entries.

To generate a custom report, you must first create the report schema that specifies what entities and attributes can be made available for the custom report.

Generating requests reports

Generate the reports that provide workflow process data.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To run a report, complete these steps:

Procedure

1. Click **Reports > Requests Reports**.
2. Select the report that you want to generate.
3. Provide filtering criteria by completing the fields on the report page, and then click **OK**.

Results

The report is displayed in the format that you specified.

What to do next

Select another reporting task, or click **Close**.

Generating user and accounts reports

Generate the reports that provide user and accounts data.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To run a report, complete these steps:

Procedure

1. Click **Reports > User and Accounts Reports**.
2. Select the report that you want to generate.
3. Provide filtering criteria by completing the fields on the report page, and then click **OK**.

Results

The report is displayed in the format that you specified.

What to do next

Select another reporting task, or click **Close**.

Generating services reports

Generate the reports that provide service data.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To run a report, complete these steps:

Procedure

1. Click **Reports > Services**.
2. Select the report that you want to generate.
3. Provide filtering criteria by completing the fields on the report page, and then click **OK**.

Results

The report is displayed in the format that you specified.

What to do next

Select another reporting task, or click **Close**.

Generating audit and security reports

Generate the reports that provide audit and security data.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To run a report, complete these steps:

Procedure

1. Click **Reports > Audit and Security Reports**.
2. Select the report that you want to generate.
3. Provide filtering criteria by completing the fields on the report page, and then click **OK**.

Results

The report is displayed in the format that you specified.

What to do next

Select another reporting task, or click **Close**.

Regular expression notation usage for searching

Regular expression notation is a group of symbols and characters that make up a syntax that is used as a template to match patterns of text.

Note: The Report task in the console supports only the wildcard (*) as a regular expression character. If you select the **Search** function in the console while you are doing a report-related task, you can specify only the wildcard as a regular expression character.

If a regular-expression field displays an asterisk (*) as the default character, that character is interpreted as a wildcard character that indicates that all string values apply. No filtering is done to reduce the number of string values that apply. IBM Security Identity Manager supports the set of regular expression characters from Java (regex4j).

Regular expressions are commonly used on UNIX platforms and in the PERL 5 language. A free online tutorial, *Using regular expressions*, is available on the following IBM developerWorks® website:

<http://www.ibm.com/developerworks/java/>

Type `regular` expression in the **Search for** field when the website is displayed, and then select **Using regular expressions** from the list of topics. You must register with developerWorks to take the tutorial.

Report customization

Use the **Design Report** task to create report templates. Add them to a table that contains a selection of report templates that you can modify or delete.

When you, as an administrator, create a custom report, you must also manually create report ACIs and entity ACIs for that custom report. The ACIs allow users that are not administrators, such as auditors, to run the custom report and to view data in the custom report.

Report templates can apply to one of the following categories. The category determines where the reporting link is displayed in the task portfolio.

- Requests
- User and Accounts
- Services
- Audit and Security
- Custom

Report templates

All reports, including standard reports and custom reports, are generated with report templates. A *report template* defines the layout of a report and the filter criteria that determines the contents of the report. When you select a report to run, you are selecting the report template used to generate the report.

IBM Security Identity Manager provides a large set of standard report templates that are designed to help you manage system resources and monitor the status of various activities and accounts. You can keep the standard report templates in their original form to generate reports. You can also examine them to determine how to design custom report templates, or modify the standard report templates to meet the needs of your organization. You modify standard report templates with the **Design Report** task in the console.

Custom reports are generated with report templates that you design. Use either the built-in report designer or a third-party report designer.

When you use the Design Report task, you can determine which report designer was used to create the report template. Use the **Report Type** column in the reports table. **Designer** identifies report templates that were created with IBM Security Identity Manager Design Report task. You can modify these report templates with Design Report task.

Creating custom report templates

Use the IBM Security Identity Manager report designer to create custom report templates.

Before you begin

Run the data synchronization process before you create a custom report template. See [“Data synchronization for reports”](#) on page 895.

Procedure

To create a custom report template, complete these steps:

1. From the left navigation pane, select **Reports > Design Report** to open the Custom Report Template page.
2. Click **Create** to open the General page.
3. In the **Report name** field, type a unique name for the report.
4. Optional: To specify the generation date and time of the report, select the **Include generated date and time** check box.
5. Optional: To specify the user name who generated the report, select the **Include generated by user information** check box.
6. Optional: To include page numbers in the report, select the **Show paging information (Page n of m)** check box.
7. Optional: Select a style sheet from the list. The default style sheet is Standard.
8. Optional: Retain the default value of the report category in the **Report Category** list. The default value is Custom.
9. Click **Contents** and then click **Add** to open the Report Column Details page.

Important: You must add at least one column to create the report.

10. Complete the following steps on this page:

- a) From the **Apply Case** list, select an appropriate option.
- b) From the **Entity** list, select an appropriate option. For example, select **Role Assignment Attributes**.
- c) From the **Attribute** list, select one of the options for adding it as a column in the report. For example, select **Attribute Name**.

Note: Attribute list options are mapped with the entity that you selected earlier.

- d) In the **Column width** field, type the size of the column. The default value is 5.
- e) In the **Sort** section, complete these steps:
 - Select one of these options: **None**, **Ascending**, or **Descending**.
 - From the **Sort order** list, select an appropriate option. For example, **2**.
- f) Click **OK** to add the column in the report.

11. Click the **Filter** tab, and then add or remove rows and columns for the report according to your requirements. For example, you can add a row in the report for a list of roles that have assignment attributes. To do so, complete these steps under the **Add a New Filter Row** area:

- a) From the **Entity** list, select **Organizational Role**.
- b) From the **Attribute** list, select **DN**.
- c) From the **Operator** list, select **Equals**.
- d) From the **Entity** list, select **Role Assignment Attributes**.

- e) From the **Attribute** list, select **Role Distinguished Name**.
 - f) From the **Condition** list, select one of these options:
 - None: Indicates that no more filter condition can be added to the report.
 - AND: Generates results only if all the specified filter conditions meet.
 - OR: Generates results if either of the specified filter conditions meet.
12. Optional: Click **Preview** to open a new browser window that contains a preview of the report.
13. Click **OK** to create the custom report.

Results

A message is displayed, which indicates that you created the custom report template.

What to do next

Generate the custom report that you created either in a PDF or a CSV format. See [“Generating custom reports”](#) on page 875.

Modifying custom report templates

Use the report designer to modify custom reports that you created.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To modify a custom report template, complete these steps:

Procedure

1. Click **Reports > Design Report**.

The **Custom Report Template** page is displayed, which contains a table that lists the standard report templates. The table might consist of multiple pages.
2. On the **Custom Report Template** page, click the name of the report that you want to modify.

The **General** tab of the Design Report notebook is displayed.
3. On the **General** tab, modify the fields as wanted, and then click the **Contents** tab.

The **Contents** tab of the Design Report notebook is displayed.
4. Optional: On the **Contents** tab, add attributes to the report column as follows:
 - a) Click **Add** to add an attribute as a column of data in the report.

The **Report Column Details** page is displayed.
 - b) On the **Report Column Details** page, complete the fields as wanted, and then click **OK**.

The new attribute is displayed in the **Report Column** of the attribute table that is within the **Contents** tab.
5. Optional: On the **Contents** tab, remove attributes from the report column as follows:
 - a) Select the check box next to the attribute that you want to remove.

Selecting the check box at the top of this column selects all attributes.
 - b) Click **Remove**.

The table on the **Contents** tab is refreshed, and the attribute is removed.
6. Click the **Filter** tab.

The filter for the report template is displayed.
7. On the **Filter** tab, select the row in the list box to view the filter details.

Filters cannot be modified for out-of-box reports. Only the filters of custom-designed report can be modified.

8. Click **Preview** to open a new browser window that contains a preview of the report, or click **OK** to save the report template.

Results

A message is displayed, indicating that you successfully updated the report template.

What to do next

To view the updated report template within the custom report table, click **Return to the Report Design Page**. You can also select another reporting task, or click **Close**.

Deleting custom report templates

Use the report designer to delete custom report templates that you no longer need.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To delete a custom report template, complete these steps:

Procedure

1. Click **Reports > Design Report**.

The **Custom Report Template** page is displayed, which contains a table that lists the standard report templates. The table might consist of multiple pages.

2. On the **Custom Report Template** page, select the check box next to the report template that you want to delete.

Selecting the check box at the top of this column selects all report templates.

3. Click **Delete**.

A confirmation page is displayed.

4. On the **Confirm** page, click **Delete** to delete the selected report template, or click **Cancel**.

Results

A message is displayed, indicating that you successfully deleted the report template.

What to do next

To view the custom report table, click **Return to the Report Design Page**. You can also select another reporting task, or click **Close**.

Generating custom reports

Generate the custom reports that are designed with the Design Report task.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Custom reports can be located within any of the report categories and not necessarily only in Custom Reports.

To generate a custom report from the Custom Reports category, complete these steps:

Procedure

1. Click **Reports > Custom Reports**.
2. Click the name of the report that you want to generate.
3. Provide filtering criteria by completing the fields on the report page, and then click **OK**.

Results

The report is displayed in the format that you specified.

What to do next

Select another reporting task, or click **Close**.

Shared access objects for custom reports

You can generate custom reports by using the shared access objects in IBM Security Identity Manager. Use the shared access entities, such as credential, credential pool, credential lease, and shared access policy to generate the custom reports.

For more information about shared access entities and their corresponding attributes, see *Database and Directory Server Schema Reference > Database tables reference > Shared access tables* in the *IBM Security Identity Manager* product documentation.

Example: Creating custom report to view all shared access credentials checked out

This topic provides detailed instructions to create custom reports to view all the shared access credentials that are currently checked out with examples.

Before you begin

Run the data synchronization process before you create a custom report to view all the shared credentials that are currently checked out. See [“Data synchronization for reports”](#) on page 895.

Procedure

To create a custom report to view all the shared access credentials that are currently checked out, complete these steps:

1. From the left navigation pane, select **Reports > Design Report** to open the Custom Report Template page.
2. Click **Create** to open the General page.
3. In the **Report name** field, type a unique name for the report.
4. Optional: To specify the generation date and time of the report, select the **Include generated date and time** check box.
5. Optional: To specify the user name who generated the report, select the **Include generated by user information** check box.
6. Optional: To include page numbers in the report, select the **Show paging information (Page n of m)** check box.
7. Optional: Select a style sheet from the list. The default style sheet is Standard.
8. Optional: Retain the default value of the report category in the **Report Category** list. The default value is Custom.
9. Click **Contents** and then click **Add** to open the Report Column Details page.

Important: You must add at least one column to create the report.

10. Complete the following steps on this page:

- a) From the **Entity** and **Attribute** lists, select appropriate options. For example, to create a custom report for viewing all the credentials that are checked out, you can map the following entities and attributes.

<i>Table 83. Entities and Attributes</i>		
Entity	Attribute	Mapping displayed on the Contents page
Credential	Name	Credential.Name
Credential lease	Credential Checkout Expiration Time	Credential lease.Credential Checkout Expiration Time
Credential lease	Credential Checkout Time	Credential lease.Credential Checkout Time

Note: You can select the entities and attributes based on your requirements.

- b) In the **Column width** field, type the size of the column. The default value is 5.
 - c) Click **OK** to add the column in the report.
11. Click the **Filter** tab to specify the data that must be displayed in the report. To do so, apply the filter conditions in the **Add a New Filter Row** area:
- a) Add rows with these filter conditions. Click **Add Row** after you finish adding every row.

<i>Table 84. Filter conditions</i>						
Row	Entity	Attribute	Operator	Entity	Attribute	Condition
1	Credential	Name	Like	_USERINPUT_	-	AND
2	Credential	Service name	Like	_USERINPUT_	-	AND
3	Credential lease	Credential DN	Equals	Credential	DN	AND
4	Credential lease	Credential Lessee	Equals	Person	DN	AND
5	Service	Service Name	Like	_USERINPUT_	-	NONE

Note: You can apply filter conditions based on your requirements. For information about entities, attributes, operators, and conditions, see the Security Identity Manager online help for the Filter page.

- b) Optional: Click **Preview** to open a new browser window that contains a preview of the report.
 - c) Click **OK** after you apply all the filter conditions.
12. On the Success page, in the **Other Tasks** area, click **Run Custom Report**.
13. On the Options page, click the report whose data you want to view.
14. Optional: If you selected the **_USERINPUT_** entity in the filters that you specified earlier, narrow down the search scope of the report. For example:
- a) In the **Credential Name Like** field, specify * to show all the credential names.
 - b) In the **Service Service Name Like** field, specify Win* to show all the services whose service name begins with Win.
15. Select the format of the report. You can select either PDF or CSV format.
16. Click **OK** to generate the report.

Results

A report is generated in a new window that shows all the shared access credentials that are currently checked out.

Example: Creating check in audit report

This topic provides detailed instructions to create a report that displays audit information for the checked in credentials.

Before you begin

Run the data synchronization process before you create a check in audit report. See [“Data synchronization for reports”](#) on page 895.

Procedure

To create a report that displays audit information for the checked in credentials, complete these steps:

1. From the left navigation pane, select **Reports > Design Report** to open the Custom Report Template page.
2. Click **Create** to open the General page.
3. In the **Report name** field, type a unique name for the report.
4. Optional: To specify the generation date and time of the report, select the **Include generated date and time** check box.
5. Optional: To specify the user name who generated the report, select the **Include generated by user information** check box.
6. Optional: To include page numbers in the report, select the **Show paging information (Page n of m)** check box.
7. Optional: Select a style sheet from the list. The default style sheet is Standard.
8. Optional: Retain the default value of the report category in the **Report Category** list. The default value is Custom.
9. Click **Contents** and then click **Add** to open the Report Column Details page.

Important: You must add at least one column to create the report.

10. Complete the following steps on this page:

- a) From the **Entity** and **Attribute** lists, select appropriate options. For example, to create a report that displays audit information for the checked in credentials, you can map the following entities and attributes.

Entity	Attribute	Mapping displayed on the Contents page
Audit Event	Entity Name	Audit Event.Entity Name
Audit Event	Initiator Name	Audit Event.Initiator Name
Audit Event	Timestamp	Audit Event.Timestamp

Note: You can select the entities and attributes based on your requirements.

- b) In the **Column width** field, type the size of the column. The default value is 5.
 - c) Click **OK** to add the column in the report.
11. Click the **Filter** tab to specify the data that must be displayed in the report. To do so, apply the filter conditions in the **Add a New Filter Row** area:
 - a) Add rows with these filter conditions. Click **Add Row** after you finish adding every row.

Table 86. Filter conditions

Row	Entity	Attribute	Operator	Entity	Attribute	Condition
1	Audit Event	Action	Like	_USERINPUT_	-	AND
2	Audit Event	Entity Name	Like	_USERINPUT_	-	AND
3	Audit Event	Initiator Name	Like	_USERINPUT_	-	AND
4	Audit Event	Timestamp	Like	_USERINPUT_	-	NONE

Note: You can apply filter conditions based on your requirements. For information about entities, attributes, operators, and conditions, see the Security Identity Manager online help for the Filter page.

- b) Optional: Click **Preview** to open a new browser window that contains a preview of the report.
 - c) Click **OK** after you apply all the filter conditions.
12. On the Success page, in the **Other Tasks** area, click **Run Custom Report**.
 13. On the Options page, click the report whose data you want to view.
 14. Optional: If you selected the **_USERINPUT_** entity in the filters that you specified earlier, narrow down the search scope of the report. For example,
 - a) In the **Audit Event Action Like** field, select **Check in** from the list to view audit information for the checked in credentials.
 - b) In the **Audit Event Entity Name Like** field, specify * to show all the entity names.
 - c) In the **Audit Event Initiator Name Like** field, specify * to show all the initiator names.
 - d) In the **Audit Event Timestamp Like** field, specify the date for which you want to view the audit information for the checked in credentials.
 15. Select the format of the report. You can select either PDF or CSV format.
 16. Click **OK** to generate the report.

Results

A report is generated in a new window that shows audit information for the checked in credentials.

Example: Creating role and shared access entitlement report

This topic provides detailed instructions to create role and shared access entitlement report by using examples. The report provides you information about roles and groups by using which the entitlement is defined and other entitlement details.

Before you begin

Run the data synchronization process before you create role and shared access entitlement report. See [“Data synchronization for reports”](#) on page 895.

Procedure

To create role and shared access entitlement report, complete these steps:

1. From the left navigation pane, select **Reports > Design Report** to open the Custom Report Template page.
2. Click **Create** to open the General page.
3. In the **Report name** field, type a unique name for the report.
4. Optional: To specify the generation date and time of the report, select the **Include generated date and time** check box.
5. Optional: To specify the user name who generated the report, select the **Include generated by user information** check box.

6. Optional: To include page numbers in the report, select the **Show paging information (Page n of m)** check box.
7. Optional: Select a style sheet from the list. The default style sheet is Standard.
8. Optional: Retain the default value of the report category in the **Report Category** list. The default value is Custom.
9. Click **Contents** and then click **Add** to open the Report Column Details page.

Important: You must add at least one column to create the report.

10. Complete the following steps on this page:

- a) From the **Entity** and **Attribute** lists, select appropriate options. For example, to create role and shared access entitlement report, you can map the following entities and attributes.

Table 87. Entities and attributes

Entity	Attribute	Mapping displayed on the Contents page
Group	Group ID	Group.Group ID
Organizational Container	Name	Organizational Container.Name
Organizational Role	Name	Organizational Role.Name
Shared Access Policy Entitlement View	Entitlement Name	Shared Access Policy Entitlement View.Entitlement Name
Shared Access Policy Entitlement View	Entitlement Service Name	Shared Access Policy Entitlement View.Entitlement Service Name
Shared Access Policy Entitlement View	Entitlement Target Name	Shared Access Policy Entitlement View.Entitlement Target Name
Shared Access Policy Entitlement View	Entitlement Type	Shared Access Policy Entitlement View.Entitlement Type

Note: You can select the entities and attributes based on your requirements.

- b) In the **Column width** field, type the size of the column. The default value is 5.
 - c) Click **OK** to add the column in the report.
11. Click the **Filter** tab to specify the data that must be displayed in the report. To do so, apply the filter conditions in the **Add a New Filter Row** area:
- a) Add rows with these filter conditions. Click **Add Row** after you finish adding every row.

Table 88. Filter conditions

Row	Entity	Attribute	Operator	Entity	Attribute	Condition
1	Shared Access Policy Entitlement View	Shared Access Policy DN	Equals	Shared Access Policy	DN	AND
2	Shared Access Policy	Parent DN	Equals	Organizational Container	DN	AND

Table 88. Filter conditions (continued)

Row	Entity	Attribute	Operator	Entity	Attribute	Condition
3	Shared Access Policy Entitlement View	Entitlement Target DN	Equals	Credential Pool	DN	AND
4	Credential Pool	Groups	Equals	Group	DN	AND
5	Organizational Role	Name	Like	_USERINPUT_	-	NONE

Note: You can apply filter conditions based on your requirements. For information about entities, attributes, operators, and conditions, see the Security Identity Manager online help for the Filter page.

- b) Optional: Click **Preview** to open a new browser window that contains a preview of the report.
 - c) Click **OK** after you apply all the filter conditions.
12. On the Success page, under the **Other Tasks** area, click **Run Custom Report**.
 13. On the Options page, click the report whose data you want to view.
 14. Optional: If you selected the **_USERINPUT_** entity in the filters that you specified earlier, narrow down the search scope of the report. For example, in the **Organization Role Name Like** field, specify * to show all the organizational roles.
 15. Select the format of the report. You can select either PDF or CSV format.
 16. Click **OK** to generate the report.

Results

A report is generated in a new window that shows role and shared access entitlement details.

Creating role custom report templates

Use the IBM Security Identity Manager report designer to create role custom report templates by using the role assignment attributes.

Before you begin

Run the data synchronization process before you create a custom report template. See [“Data synchronization for reports”](#) on page 895.

Procedure

To create a role custom report template, complete these steps:

1. From the left navigation pane, select **Reports > Design Report** to open the Custom Report Template page.
2. Click **Create** to open the General page.
3. In the **Report name** field, type a unique name for the report.
4. Optional: To specify the generation date and time of the report, select the **Include generated date and time** check box.
5. Optional: To specify the user name who generated the report, select the **Include generated by user information** check box.
6. Optional: To include page numbers in the report, select the **Show paging information (Page n of m)** check box.
7. Optional: Select a style sheet from the list. The default style sheet is Standard.
8. Optional: Retain the default value of the report category in the **Report Category** list. The default value is Custom.

9. Click **Contents** and then click **Add** to open the Report Column Details page.

Important: You must add at least one column to create the report.

10. Complete the following steps on this page:

- a) From the **Entity** list, select an appropriate option. For example, select **Role Assignment Attributes**.
- b) From the **Attribute** list, select one of the options for adding it as a column in the report. For example, select **Attribute Name**.

Note: Attribute list options are mapped with the entity that you selected earlier.

- c) In the **Column width** field, type the size of the column. The default value is 5.
 - d) Click **OK** to add the column in the report.
11. Click the **Filter** tab, and then add or remove rows and columns for the report according to your requirements. For example, you can add a row in the report for a list of roles that have assignment attributes. To do so, complete these steps under the **Add a New Filter Row** area:
- a) From the **Entity** list, select **Organizational Role**.
 - b) From the **Attribute** list, select **DN**.
 - c) From the **Operator** list, select **Equals**.
 - d) From the **Entity** list, select **Role Assignment Attributes**.
 - e) From the **Attribute** list, select **Role Distinguished Name**.
 - f) From the **Condition** list, select one of these options:
 - None: Indicates that no more filter condition can be added to the report.
 - AND: Generates results only if all the specified filter conditions meet.
 - OR: Generates results if either of the specified filter conditions meet.
12. Optional: Click **Preview** to open a new browser window that contains a preview of the report.
13. Click **OK** to create the role custom report.

Results

A message is displayed, which indicates that you created the role custom report template.

What to do next

Generate the role custom report that you created either in a PDF or a CSV format. See [“Generating custom reports”](#) on page 875.

Report schema mapping

A *report schema* specifies which entities and attributes can be included in reports. Before an entity and its associated attributes can be specified as reporting criteria and included in custom report data, a report schema must be defined.

Schemas are installed for all of the standard reports during product installation. The administrator does not define schemas for standard reports.

By default, entities and attributes are not included in custom reports. The administrator must define a schema for each custom report template that is created, including designer reports. To create a report schema, you must run the Design Schema task in the console.

Note: Map only the entities and attributes for which you want to generate custom reports. These mappings directly affect the performance of IBM Security Identity Manager. The impact occurs because all of the data from the directory server is copied to the database each time a data synchronization is done.

By defining the schema, you select directory entities that are staged as tables in the IBM Security Identity Managers database. Defining the schema involves mapping attributes. After mapping the entities and attributes, you must synchronize the data to make the data available for reporting.

Mapping attributes

To create a custom report schema, create an attribute mapping that specifies the entities and entity attributes that can be included in a report.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

The type of data that can be included in a custom report is determined by the report schema. You do not create report schemas for standard reports because those schemas are already defined. The attributes for a particular entity can be unmapped if all the reports with that entity and attribute are deleted.

To map the attributes for an entity, complete these steps:

Procedure

1. Click **Report > Schema Mapping**.

The **Select Entity Attributes** page is displayed.

2. On the **Select Entity Attributes** page, select an entity from the list of objects.

Both mapped and unmapped attributes for the selected entity are displayed. If they are being used by standard reports, some of the attributes can be mapped by default.

3. Select one or more attributes from the **Unmapped attributes** list, and then click **Add**.

- To select multiple attributes at the same time, press the Ctrl key and click each attribute that you want to map.
- To select continuous, multiple attributes at the same time, press the Shift key and click each attribute that you want to map.

The attribute is moved to the **Mapped attributes** list.

4. Click **OK** to save the report schema and close the Select Entity Attributes page.

Results

A message is displayed, indicating that you successfully updated the schema mapping for the entity that you selected.

What to do next

Select another reporting task, or click **Close**.

Unmapping attributes

You can unmap previously mapped attributes so that they are no longer available for reporting.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Only attributes that are not being used in any reports can be unmapped. The attributes that you unmap are made unavailable for reporting as soon as you save your changes. You do not have to run the data synchronization task for the changes to take effect.

To unmap the attributes for an entity, complete these steps:

Procedure

1. Click **Report > Schema Mapping**.

The Select Entity Attributes page is displayed.

2. On the Select Entity Attributes page, select an entity from the list of objects.

Both mapped and unmapped attributes for the selected entity are displayed. If they are being used by standard reports, some of the attributes can be mapped by default.

3. Select one or more attributes from the **Mapped attributes** list, and then click **Remove**.

- To select multiple attributes at the same time, press the Ctrl key and click each attribute that you want to unmap.
- To select continuous, multiple attributes at the same time, press the Shift key and click each attribute that you want to unmap.

The attribute is moved to the **Unmapped attributes** list.

4. Click **OK** to save the report schema and close the Select Entity Attributes page.

Results

A message is displayed, indicating that you successfully updated the schema mapping for the entity that you selected.

What to do next

Select another reporting task, or click **Close**.

User input values

Determine which user input values to specify when you run standard reports.

User input values describe:

- Fields in standard reports for which you can specify values when you run the reports.
- Types of values that you can specify for each field.
- Default values used for each field if you do not specify a value.

Report field name	Values that can be specified	Default value used if no input is specified
Access Name	Name of an access or a string expression that contains one or more wildcards	Any
Access Type	Access type from list	Any
Account Operation	Any of the values displayed in the list	Any
ACI Context	Name of an entity type or the value "any," which is specified with the asterisk (*)	*, indicating any value
ACI Name	Name of a policy or a sting expression that contains one or more wildcards	*, indicating any value
ACI Object Type	Name of an object associated with the entity type, or the value "any"	Any
ACI Scope	Any, single, or sub tree	Any, single, sub tree

Table 89. User input values (continued)

Report field name	Values that can be specified	Default value used if no input is specified
Approval Activity	Name of an activity or a sting expression that contains one or more wildcards	*, indicating any value
Approver	Person (A person search is started to get a value.)	Any
Approver (Pending Approvals)	Person	Any
Organization Unit	Business unit	Any
Dormant Period	Integer	14 (days)
End date	Date in the format set for your locality	Current [®] date and time
Operations	Any of the values displayed in the list	Any
Person	Person	Any
Person - Suspended before	Date in the format set for your locality	Current date and time
Provisioning Policy Name	Name of a policy or a sting expression that contains one or more wildcards	*, indicating any value
Recertification Policy Target Type	Recertification policy target type from list	Any
Recertification Response	Recertification response type from list	Any
Requestee	Person	Any. For nonadministrative users, the default value is the owner of a user that is logged on.
Role	Role	Any
Root Process	Any of the values displayed in the list	Any
Service	Service	Any
Service owner	Person	Any
Service Type	Service type from the list	Any
Start Date	Date in the format set for your locality	30 days before current date and time
Status (Account)	Any, Active, or Inactive	Any
Status (Account Operation)	Any, Success, Warning, Failure, or Pending	Any
Status (Pending Approvals)	Any, Escalated, or Locked	Any
Submitted by	Person	Any

Table 89. User input values (continued)

Report field name	Values that can be specified	Default value used if no input is specified
Suspended Before (Accounts and Individuals)	Date in the format set for your locality	Current date and time
User ID	Specific user ID or a sting expression that contains one or more wildcards	*, indicating any user ID

User input filters

Determine which filters to specify when you design custom reports that allow user input.

User input filters include:

- User input filters that you can specify for each type of standard report.
- Corresponding filter that is defined in each report template to enable user input for built-in designer reports.

Use the filters as guidelines to create user input filters for custom reports.

You can specify one or more filter values for a single report, depending on which user input filters are available for the report. If you specify multiple values, IBM Security Identity Manager determines the *entity.attribute* to which each value applies by the position and type of each value. For example, when you run an account report, you can specify a service name and an organization unit name in a field, such as

Provide User Input.

Table 90. User input filters

Report name	User input	Default value	Report designer filter
Access Control Item	ACI Name	Any	ACI.name = _USERINPUT_
	ACI Context	Any	ACI.category = _USERINPUT_
	Object Type	Any	ACI.Target = _USERINPUT_
	ACI Scope	Any	ACI.scope = _USERINPUT_
	Organization Unit	Any	Organizational Container.DN = _USERINPUT_
Access Report	Access Type	Any	Access.Type = _USERINPUT_
	Access	Any	Access.DN = _USERINPUT_
	Service Type	Any	Service.servicetype = _USERINPUT_
	Service	Any	Service.DN = _USERINPUT_
	Owner	Any	Person.DN = _USERINPUT_
Account	Service	Any	Service.DN = _USERINPUT_
	Organization Unit	Any	Organizational Container.DN = _USERINPUT_
Account/Access Pending Recertification Report	Account/Access Owner	Any	Process.Requestee = _USERINPUT_
	Service Type	Any	Service.Servicetype = _USERINPUT_

Table 90. User input filters (continued)

Report name	User input	Default value	Report designer filter
Account Operations	Root Process	Any	Process.Type = _USERINPUT_
	Account Operation	Any	Activity.Type = _USERINPUT_
	Start Date	30 days before current date	Process.Completed > _USERINPUT_ AND Process.Completed < _USERINPUT_
	End Date	Current date	
	Service Type	Any	Service.servicetype = _USERINPUT_
	Service	Any	Service.DN = _USERINPUT_
	User ID	Any	Activity.Subject = _USERINPUT_
	Status	Any	Activity.Result_Summary = _USERINPUT_ (Any)
Account Operations Performed by an Individual	Submitted by	Any	Process.REQUESTER = _USERINPUT_
	Account Operation	Any	Activity.Type = USERINPUT_
	Start Date	30 days before current date	Process.Completed > _USERINPUT_ AND Process.Completed < _USERINPUT_
	End Date	Current date	
	Service Type	Any	Service.servicetype = _USERINPUT_
	Service	Any	Service.DN = _USERINPUT_
	User ID	*	Activity.Subject = _USERINPUT_
	Status	Any	Activity.Result_Summary = _USERINPUT_
Approvals and Rejections	Approver	Any	Person.DN like _USERINPUT_ AND PERSON.CN = PROCESSLOG.REQUESTOR
	Start Date	30 days before current date	Process.Completed > _USERINPUT_ AND Process.Completed < _USERINPUT_
	End Date	Current date	
	Service Type	Any	Service.servicetype = _USERINPUT_
	Service	Any	Service.DN = _USERINPUT_
	User ID	*	Process.Subject = _USERINPUT_
	Status	*	PROCESS.RESULT_SUMMARY like _USERINPUT_
	Approval Activity		ACTIVITY_DEFINITION_ID like _USERINPUT_
Dormant Accounts	Service	Any	Service.DN = _USERINPUT_
	Dormant Period	14	Last Accessed Date = _USERINPUT_

Table 90. User input filters (continued)

Report name	User input	Default value	Report designer filter
Individual Access	Account Owner	Any	Person.DN = _USERINPUT_
	Organization Unit	Any	OrganizationalContainer.DN = _USERINPUT
	Access	Any	Access.DN = _USERINPUT_
	Service	Any	Service.DN = _USERINPUT_
Individual Accounts	Person	Any	Person.DN = _USERINPUT_
	Organization Unit	Any	OrganizationalContainer.DN = _USERINPUT_
Individual Accounts by Role	Role	None (no role specified)	Organization Role.DN = _USERINPUT_
	Organization Unit	Any	OrganizationalContainer.DN = _USERINPUT_
Non-Compliant Accounts	Service	Any	Service.DN = _USERINPUT_
	Reason	Any	Account.eraccountcompliance = _USERINPUT_
Operation	Requester	Any	Process.REQUESTER = _USERINPUT_
	Requestee	Any	Process.REQUESTEE = _USERINPUT_
	Operations	AccountAdd (as specified in the properties file)	Process.Type = _USERINPUT
	Start Date	30 days before the current date	Process.Completed > _USERINPUT_ AND Process.Completed < _USERINPUT_
	End Date	Current date	
Orphan Accounts	Service	Any	Service.DN = _USERINPUT_
	Account Status	Any	Account.eraccountstatus = _USERINPUT_
Pending Approvals	Approver	Any	Person.DN = _USERINPUT_
	Start Date	30 days before current date	Workitem.Created > _USERINPUT_ AND Workitem.Created < _USERINPUT_
	Service Type	Any	Service.Servicetype = _USERINPUT_
	Service	Any	Service.DN = _USERINPUT_
	User ID	*	Process.Subject = _USERINPUT_
	Status	Any	Pending_Approval. Result_Summary = _USERINPUT_
	Approval Activity Name	*	Activity.Name = _USERINPUT_
Policies Governing a Role	Role	Any	Organization Role.DN = _USERINPUT_

Table 90. User input filters (continued)

Report name	User input	Default value	Report designer filter
Policy	Provisioning Policy Name	Any	ProvisioningPolicy. Policy Name = _USERINPUT_
Recertification Change History Report	Service	Any	Recertificationlog. Service = _USERINPUT_
	Access Type	Any	Recertificationlog. Access_Type = _USERINPUT_
	Account/Access Owner	Any	Recertificationlog. Account_Owner = _USERINPUT_
	Recertification Response	Any	Recertificationlog. Recert_Result = _USERINPUT_
	Show Last Recertification Only	Yes/No	
	Start Date	30 days before current date	Recertificationlog. Completed > _USERINPUT_ AND Recertificationlog. Completed < _USERINPUT_
	End Date	Current date	
Recertification Policy Report	Recertification Policy Target Type	Any	RecertificationPolicy. GROUPDN LIKE '_USERINPUT_'
	Service Type	Any	RecertificationPolicy. SERVICETYPE = _USERINPUT_
	Service	Any	RecertificationPolicy. SERVICEDN = _USERINPUT_
	Access Type	Any	RecertificationPolicy. ACCESSTYPE = _USERINPUT_
	Access	Any	RecertificationPolicy. ACCESSDN = _USERINPUT_
Reconciliation Statistics	Service	None (input required)	Service.DN = _USERINPUT_
Rejected	Requester	Any	Process.REQUESTER = _USERINPUT_ (Any)
	Requestee	Any	Process.REQUESTEE = _USERINPUT_ (Any)
	Start Date	30 days before the current date	Process.Completed > _USERINPUT_ AND Process.Completed < _USERINPUT_
	End Date	Current date	
Services	Service Type	Any	Service.servicetype = _USERINPUT_
	Service	Any	Service.DN = _USERINPUT_
	Owner	Any	Person.DN = _USERINPUT_
	Organization Unit	Any	Organizational Container.DN = _USERINPUT_

<i>Table 90. User input filters (continued)</i>			
Report name	User input	Default value	Report designer filter
Services Granted to an Individual	Person	Any	Person.DN = _USERINPUT_
Summary of Accounts on Service	Service	Any	Service.DN = _USERINPUT_
	Account Status	Any (as specified in the properties file)	Account.Account Status = _USERINPUT_
Suspended Accounts	Account	Any	Account.DN = _USERINPUT_
	Person	Any	Person.DN = _USERINPUT_
	Service Type	Any	Service.servicetype = _USERINPUT_
	Service	Any	Service.DN = _USERINPUT_
	Suspended Date	Current date	Process.Completed < _USERINPUT_
Suspended Individuals	Person	Any	Person.DN = _USERINPUT_
	Organization Unit	Any	Organizational Container.DN = _USERINPUT_
	Suspended Before	Current date	Process.Completed < _USERINPUT_
User	Requester	Any	Process.REQUESTER = _USERINPUT_ (Any)
	Requestee	Any	Process.REQUESTEE = _USERINPUT_ (Any)
	Start Date	30 days before the current date	Process.Completed > _USERINPUT_ AND Process.Completed < _USERINPUT_
	End Date	Current date	

Filter conditions for custom reports

Filter conditions are logical expressions that are parsed as a JOIN condition to determine what information to include in a report when it is generated.

You can create a simple filter condition with one operator:

```
Account.Service Equals Service.DN
```

You can also create complex filters with multiple conditions:

```
ACI.DN = ACI Principals.DN
```

```
AND ACI.Name = ACI Principals.Name
```

```
AND ACI.Target = ACI Principals.Target
```

Example: Creating filter conditions for accounts

This example report lists users with accounts of type ITIMService.

Assume that you specified the following entities, attributes, and filters to create the report template:

- **Report columns:** Account.Userid, ITIM.ServiceName
- **Filters:** None

Because no JOIN filter is specified, if there are two users:

- User1 with ITIMService1 and ITIMService2
- User2 with ITIMService3

The result is:

User1	ITIMService1
User1	ITIMService2
User1	ITIMService3
User2	ITIMService1
User2	ITIMService2
User2	ITIMService3

This result is the Cartesian product of the two tables; it does not display the wanted results. To yield the appropriate result set, specify the appropriate JOIN condition to indicate the relationships between these two tables. The JOIN condition in this case is:

```
Account.Service = ITIM.DN
```

If you specify this filter, the result is:

User1	ITIMService1
User1	ITIMService2
User2	ITIMService3

Example: Creating filter conditions for persons and organization roles

This report shows persons associated with an organization role.

Assume that you specified the following entities, attributes, and filters in the console to create the report template:

- **Report columns:** Person.FullName, OrganizationRole.Name
- **Filter:** OrganizationRole.Name = '_USERINPUT_'

Assume that there are two users:

- Person1 with Role1
- Person2 with Role2

If you enter Role1 as user input when you run the report, the result is:

Person1	Role1
Person2	Role1

For this report to generate the correct results, specify the following filter:

```
Person.OrganizationRoles = OrganizationRole.DN  
AND OrganizationRole.Name = '_USERINPUT_'
```

Now, if you enter Role1 as user input when you run the report, the result would be:

Person1	Role1
---------	-------

The specified filter condition works because the Organization Roles attribute of the Person contains the value of the DN of the role to which a user belongs. Also note that Organization Role is a multi-valued attribute; that is, a person can have multiple roles in an organization.

Example: Creating filter conditions for persons and accounts

This report shows accounts associated with persons defined to IBM Security Identity Manager.

Assume that you specified the following entities, attributes, and filters in the console to create the report template:

- **Report column:** Person.FullName, Account.AccountStatus
- **Filters:** None

This report returns the Cartesian product of the Person and Account table entries. To yield the correct result, the JOIN condition that specifies the relationship between the Person and Account tables is:

```
Account.owner = Person.DN
```

Sample JOIN conditions for designing reports

Review examples of filters that you can use to design custom reports.

The Filters column contains the exact JOIN condition that yields accurate and meaningful results.

Note: The Serial No. column is included only for referencing by support personnel.

Serial No.	Entities	Filters
1	Person, Account	Person.DN = Account.owner
2	Person, Organization Role	Person.Organization Roles = Organization Role.DN
3	Person, Organizational Unit	Person.ParentDN = Organizational Unit.DN OR Organizational Unit. Supervisor = Person.DN
4	Account, Service	Account.Service = Service.DN
5	Location, Person	Location.Supervisor = Person.DN
6	Business Partner, Organization, Person	Business Partner Organization.Sponsor = Person.DN
7	Business Partner Person, Organization Role	Business Partner Person.Organization Roles = Organization Role.DN
8	Organization, Location	Organization.DN = Location.Parent DN
9	Organization, Organizational Unit Organization, Business Partner Organization	Organization.DN = Organizational Unit.ParentDN
		Organization.DN = Business Partner
		Organization.ParentDN
10	Organizational Unit, Location	Organizational Unit.Parent DN = Location.DN OR Location.Parent DN = Organizational Unit.DN

11	Organizational Unit, Business Partner Organization	Organizational Unit.Parent DN = Business Partner Organization DN OR Business Partner Organization.Parent DN = Organizational Unit.DN
12	Location, Business Partner Organization	Location.Parent DN = Business Partner Organization.DN OR Business Partner Organization.Parent DN = Location.DN
13	Service, Person	Service.Account Owner = Person.DN
14	SQL2000Account, Service	SQL2000Account.Service = Service.DN
15	ITIMAccount, ITIM Service	ITIMAccount.Service = ITIM.DN
16	Entitlement, Service	Service.DN = Entitlement.Service Target Name
17	Provisioning Policy, Entitlement	ProvisioningPolicy.DN = Entitlement.DN
18	ACI, ACI Principals	ACI.DN = ACI Principals.DN AND ACI.Name = ACI Principals.Name AND ACI.Target = ACI Principals.Target
19	ACI, ACI Permission ClassRight	ACI.DN = ACI Permission ClassRight.DN AND ACI.Name = ACI Permission ClassRight.Name AND ACI.Target = ACI Permission ClassRight.Target
20	ACI, ACI Permission AttributeRight	ACI.DN = ACI Permission AttributeRight.DN AND ACI.Name = ACI Permission AttributeRight.Name AND ACI.Target = ACI Permission AttributeRight.Target
21	ACI, ACI Role DNs	ACI.DN = ACI Role DNs.DN AND ACI.Name = ACI Role DNs.Name AND ACI.Target = ACI Role DNs.Target
22	ACI, Organizational Unit	ACI.DN = Organizational Unit.DN

Customizing the report banner

You can add a customized banner to your IBM Security Identity Manager reports.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Use this task to produce reports that display the logo of your organization in the header.

To add a customized banner, complete these tasks:

Procedure

1. Create your custom banner as a Graphic Interchange Format (GIF) file, with `logo.gif` as the file name.
2. Place the `logo.gif` file in the `ISIM_HOME/data/adhocreport/logo` directory.
3. Ensure that the `logo.gif` file provides read permission that allows the web application server to access the file.
4. To validate that the customized banner is used, generate and view a report. If the customized banner is not displayed, restart your browser.

Custom report configuration files

You can modify properties files to change settings that are related to custom reports and to add user-defined functions to the custom reports tasks.

adhocreporting.properties

This file contains configuration properties related to the custom reporting tasks.

DatabaseFunctions.conf

You can specify user-defined database functions when designing custom report templates. For example, to retrieve an attribute from a table column in the staged data, IBM Security Identity Manager provides two functions, `upper` and `lower`. Use these functions to specify that the data is returned for display in uppercase or lowercase letters. To make available user-defined functions, add the functions to this file.

Data synchronization

IBM Security Identity Manager stores most of its operational data in an LDAP directory. Examples of operational data include information about the people and accounts that are managed by IBM Security Identity Manager, the policies that are defined in IBM Security Identity Manager, and other information.

IBM Security Identity Manager provides the ability for users to run reports about this operational data. For example:

- As an auditor, you might want to run a report that lists all of the people who are in violation of a corporate policy.
- As an administrator, you might want to run a report that lists all of the accounts that are inactive for the last six months.
- As a manager, you might want to run a report that lists all of the accounts that are owned by people in your department.

The reporting architecture requires that data reside in a database. The IBM Security Identity Manager data synchronization feature copies the operational data from the LDAP directory to a database, making it available to be included in reports.

Running data synchronization

Data synchronization can be run in the following ways:

Full data synchronization

This approach synchronizes all of the operational data. That is, the full data synchronization process starts by deleting all of the data it previously copied into the database. Then, it copies all of the operational data from the LDAP directory to the database. The full data synchronization can be run in the following ways:

On demand

As an administrator, you can log in to IBM Security Identity Manager, and run the full data synchronization process.

On a recurring schedule

As an administrator, you can configure IBM Security Identity Manager to automatically run the full data synchronization process on a specified recurring schedule. For example, you can configure IBM Security Identity Manager to run the full data synchronization process at these times:

- Every Sunday night at midnight.
- The 15th day of every month.

Incremental data synchronization

This approach synchronizes only the operational data that changed since the last time the data was synchronized. Unlike the full data synchronization, the incremental data synchronization does not delete all of the data it previously copied into the database. Rather, it updates the database to reflect the changes that occurred in the LDAP directory since the last time the data was synchronized. Incremental data synchronization requires enabling the LDAP change log feature.

Report Data Synchronization Utility

This approach is identical to the full data synchronization. The only difference is that it can be run from a computer that is not part of the deployed IBM Security Identity Manager environment. That is, the first two approaches must be run on a computer in which IBM Security Identity Manager is installed. The Report Data Synchronization Utility can be run on any computer, provided the computer meets the hardware and software requirements of the utility.

Data synchronization for reports

Manage schedules for data synchronization, or initiate a data synchronization activity immediately. You can also refresh the synchronization status.

When you initiate a data synchronization activity, the following actions occur:

- Directory server data is staged for report processing
- Mapping updates that are made with the Schema Mapping task are made available to the Design Report task
- Data and ACI information is synchronized between the directory server and the database
- All separation of duty policies defined in the system are evaluated for violations

Data synchronization schedules that you add are run as a background process at the scheduled time.

In general, schedule the data synchronization task when system load is low.

You can initiate a data synchronization activity immediately, or you can schedule a task to run at a specified time or at regular intervals.

You can view the status of the most recent data synchronization.

You can add or modify data synchronization schedules at any time.

You do not need to do a data synchronization task when you modify a report. However, if you change the report schema, reporting ACIs, or the entity data, you must do a data synchronization for the changes to take effect. For example, you might add a person to the system and want the name of that person to occur in a report.

The entities and attributes that you map with the Schema Mapping task are made available for the Design Report task only after data is synchronized.

Synchronizing data immediately

You can initiate an immediate data synchronization activity.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To initiate a data synchronization activity immediately, complete these steps:

Procedure

1. Click **Reports > Data Synchronization**.
2. On the **Data Synchronization** page, click **Run Synchronization Now**.
A confirmation page is displayed.
3. On the **Confirm** page, click **Run Synchronization Now** to run the synchronization, or click **Cancel**.

Results

A message is displayed, indicating that you successfully initiated a data synchronization activity.

What to do next

To view the results of the synchronization, click **Return to the Data Synchronization page**. You can also select another reporting task, or click **Close**.

Creating a data synchronization schedule

You can create a schedule for synchronizing data.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To create a data synchronization schedule, complete these steps:

Procedure

1. Click **Reports > Data Synchronization**.
2. On the **Data Synchronization** page, click **Create**.
The **Synchronization Schedule** page is displayed.
3. Select a schedule interval to synchronize data on the system.
The fields displayed depend on the scheduling option that you select.
4. Complete any remaining fields as wanted, and then click **OK** to save the new schedule.

Results

A message is displayed, indicating that you successfully added the new synchronization schedule.

What to do next

Select another reporting task, or click **Close**.

Modifying a data synchronization schedule

You can modify an existing schedule for synchronizing data.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

A data synchronization schedule must exist.

About this task

To modify a data synchronization schedule, complete these steps:

Procedure

1. Click **Reports > Data Synchronization**.
2. On the **Data Synchronization** page, click the schedule that you want to modify.
The **Synchronization Schedule** page is displayed.
3. Select a schedule interval to synchronize data on the system.
The fields displayed depend on the scheduling option that you select.
4. Complete any remaining fields as wanted, and then click **OK** to save the modified schedule.

Results

A message is displayed, indicating that you successfully updated an existing synchronization schedule.

What to do next

Select another reporting task, or click **Close**.

Deleting a data synchronization schedule

You can delete one or more schedules for data synchronization.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

A data synchronization schedule must exist.

About this task

To delete a data synchronization schedule, complete these steps:

Procedure

1. Click **Reports > Data Synchronization**.
2. On the **Data Synchronization** page, select the check box next to the synchronization schedule that you want to delete. Selecting the check box at the top of this column selects all synchronization schedules.
3. Click **Delete**
A confirmation page is displayed.

4. On the **Confirm** page, click **Delete** to delete the selected synchronization schedule, or click **Cancel**.

Results

A message is displayed, indicating that you successfully removed the synchronization schedule.

What to do next

Select another reporting task, or click **Close**.

Incremental data synchronizer overview

The Incremental Data Synchronizer is a separately installed utility that provides fast synchronization of data and access control items. Synchronization occurs between the directory server that IBM Security Identity Manager uses and the IBM Security Identity Manager database.

In addition, the Incremental Data Synchronizer can be configured to enforce changes in the schema entities and attribute mappings that are used in custom report templates.

The Incremental Data Synchronizer synchronizes staged reporting data (entities and attributes) and corresponding access control item information for the data. Additionally, it can propagate schema changes. The Incremental Data Synchronizer does the following operations:

1. Changelog synchronization:
 - a. Obtain the changelogs from the directory server.
 - b. Analyze the effective operation and attribute values of each modified entry.
 - c. Update the access control item information, if necessary.
 - d. Update all available entry attributes in the staged tables with the changes recorded in the directory changelog.
2. Schema enforcement:
 - a. Determine any changes made to the report schema.
 - b. Map or unmap entities, if necessary.
 - c. Map or unmap entity attributes, if necessary.
 - d. Add or remove the access control item information of the newly mapped and unmapped attributes.

A fully configured Incremental Data Synchronizer does the same functions as the built-in data synchronizer. However, it manages incremental changes to the data and does the synchronization task only on the changed data. By propagating only the changes since the last synchronization task was done, the Incremental Data Synchronizer can update the staged reporting data quickly.

You install and configure the Incremental Data Synchronizer after installing IBM Security Identity Manager. Incremental data synchronization is not a prerequisite for custom reports unless your environment requires a fast synchronization of data and access control item definitions.

The more often you run the Incremental Data Synchronizer, the less likely you are to have errors in the data. You are less likely to have errors in the access permissions to the report data. The accuracy of the custom reporting process is enhanced.

For information about the Incremental Data Synchronizer, search for **Incremental Data Synchronizer** in the IBM Security Identity Manager documentation.

Directory Server changelog

The Incremental Data Synchronizer uses a mechanism known as changelog, a feature provided by the directory server.

The changelog is a history of changes maintained by the directory. Directory servers supported by IBM Security Identity Manager can be configured to record data changes under a directory node called:

```
cn=changelog
```

The Incremental Data Synchronizer fetches change entries stored under the `cn=changelog` directory. The Incremental Data Synchronizer picks up the data and access control item change entries needed to synchronize with the staged database tables.

To enable changelog for the specific directory server used by IBM Security Identity Manager, see the appropriate documentation provided by the vendor of that directory server.

Note: Enabling the IBM Security Identity Manager Server changelog can reduce directory update performance by 10 to 15 percent.

Starting the incremental data synchronizer

Start the IBM Security Identity Manager Server and synchronize the data with the Synchronize Data task in the IBM Security Identity Manager console *before* you start the Incremental Data Synchronizer.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

You can start the Incremental Data Synchronizer by using the command-line interface.

You can run the Incremental Data Synchronizer immediately or schedule its execution. However, *you must run the Incremental Data Synchronizer interactively the first time you use it*. During the initial session, you can specify the time intervals for running the utility in the future. You can set the changelog synchronization and schema enforcement features independently as required.

Procedure

Start the Incremental Data Synchronizer command line tool.

See "incr_data_synch command" in the *IBM Security Identity Manager Reference Guide* .

Fine-tuning the Incremental Data Synchronizer

You can tune the performance of the Incremental Data Synchronizer by modifying properties in the `adhocreporting.properties` configuration file.

The following three properties can be modified in combination to produce efficient operation of the synchronization process:

- **changeLogFetchSize**
- **maximumChangeLogsToSynchronize**
- **changeLogsToAnalyzeBeforeSynchronization**

For more information, see the *IBM Security Identity Manager Performance and Tuning Guide*.

Utility for external report data synchronization

The report data synchronization utility is a separately installed utility that synchronizes data and access control items between the directory server and the IBM Security Identity Manager virtual appliance database. The synchronized data is used for running the reports.

You must install, configure, and run the utility on a different computer other than the IBM Security Identity Manager virtual appliance computer. The utility installed on a different computer does not require the installation of the Application server, a directory server, or a database.

The utility for external report data synchronization is used for remote or non-IBM Security Identity Manager virtual appliance purposes. From the Appliance Dashboard on the IBM Security Identity Manager virtual appliance console, click **Configure > Advanced Configuration > Custom File Management**. From the **All Files** tab, go to `directories/utilities` and download the `itim_report_data_sync_utility.zip` file and extract it.

Running the report data synchronization utility

After you configure the utility, you can start the synchronization process.

Before you begin

- Configure IBM Security Identity Manager report data synchronization utility.
- Access the folder in which you extracted the utility.

About this task

To run the report data synchronization utility, complete these steps:

Procedure

1. Run one of the following commands:

Microsoft Windows platforms

```
SyncData.cmd [-JAVA_HOME java_home_value]
```

For example, `SyncData.cmd -JAVA_HOME "C:\Program Files\IBM\Java60"`

UNIX or Linux platforms

```
./SyncData.sh [-JAVA_HOME java_home_value]
```

For example, `./SyncData.sh -JAVA_HOME /opt/IBM/Java60`

where, `-JAVA_HOME` is an optional argument that specifies the location of the Java runtime environment. See [Table 91 on page 900](#) for specifying the location of the Java runtime environment.

If the <code>-JAVA_HOME</code> argument is	IBM Security Identity Manager
<ul style="list-style-type: none">• Specified	Uses the corresponding Java runtime environment.
<ul style="list-style-type: none">• Not specified, and• The <code>-JAVA_HOME</code> operating system environment variable contains a value.	Uses the Java runtime environment corresponding to the <code>-JAVA_HOME</code> operating system environment variable.
<ul style="list-style-type: none">• Not specified, and• The <code>-JAVA_HOME</code> operating system environment variable either does not exist or does not contain a value.	Reports a failure for the report data synchronization utility.

2. If you encounter any problem while running the report data synchronization utility, see the `SyncData.log` file. This log file is created in the directory where you extracted the utility.

What to do next

- See [“Report data synchronization utility errors and their workarounds” on page 900](#).

Report data synchronization utility errors and their workarounds

The following topic describes how to troubleshoot the IBM Security Identity Manager report data synchronization utility errors.

The report data synchronization utility completes the data synchronization operation successfully, but with the following exception.

The following exception might get registered into the trace file:

```
Class com.ibm.websphere.cache.DistributedMap NOT FOUND
```

It might happen because the synchronization time exceeds the cache refresh timeout interval specified by the `enrole.profile.timeout` property. This exception does not affect the success of the data synchronization. You can ignore this exception message.

Workaround:

Increase the timeout interval value for the property `enrole.profile.timeout` in the `enRole.properties` property file.

The report data synchronization utility completes with a failure with log entries and indicates that the data synchronization cannot run because data synchronization is already running.

Follow the steps to end the data synchronization operation process and rerun the data synchronization utility. For more information about how to end the data synchronization operation, see <http://www.ibm.com/support/docview.wss?uid=swg21303678>.

The report data synchronization utility completes with a failure with log entries and indicates that the data synchronization failed with an `OutOfMemoryError` message.

`OutOfMemoryError` can occur if the Java virtual machine heap is too small.

Workaround:

Increase the Java virtual machine heap size by creating an operating system environment variable:

Microsoft Windows operating systems

```
set IBM_JAVA_OPTIONS=-Xms1024m -Xmx2048m
```

UNIX or Linux operating systems

```
export IBM_JAVA_OPTIONS='-Xms1024m -Xmx2048m'
```

where:

- Xms1024m specifies initial heap size of 1024 mb
- Xmx2048m specifies maximum heap size of 2048 mb

Note: The numbers mentioned in the instructions are examples only. The exact numbers that are required might vary.

Access control items (ACI) for reports

Access control item (ACI) definitions govern the availability of reports for all users. The report ACIs grant or deny a group of users the ability to run reports.

A IBM Security Identity Manager administrator can access all reports. In addition, there are default ACIs for the Manager, Service Owner, and Auditor groups. For example, service owners and managers can search for all persons that they can access. Managers can see direct reports, and service owners can see people on services controlled by ACIs. Auditors can run all reports and see all data. No report access is available for users or members of the Help Desk group, unless an administrator creates an ACI definition that grants access to a group of which the user is a member. ACI definitions must be defined for both standard and custom reports.

An administrator can create an ACI definition at any time. After an ACI definition is added, the system immediately applies the ACI. The new ACI affect users who are logged in to the system and not currently viewing the list of available reports. Those users currently viewing the list of reports are not affected.

Users can view only activities that are specific to their group, either as submitters of the requests or as persons for whom the requests are submitted. For example, managers can view reports for requests that they initiated or for requests that are made for them. Employees that are not in supervisory or managerial roles can view only reports for requests that are made for them because they cannot initiate requests. Auditors can see requests generated by other users.

Report ACIs are applicable in only one organization. Therefore, for non-administrative users of secondary organizations to be able to run reports, report ACIs must also be created in those secondary organizations.

ACI object filters used for reporting

Object filters defined in ACIs are used by the reporting engine to stage data and ACI information in the database.

The reporting engine requires object filters that meet these conventions:

- The supported filters for LDAP to SQL conversion are a subset of filters mentioned in RFC 2254 for LDAP Filter Specification.
- Matching rules, soundex filters, and approximation operators are not supported.
- In regular expressions, only the * (asterisk) wildcard character is supported.
- Only the following special characters are allowed in LDAP filters:
 - \$ (dollar sign)
 - @ (at sign)
 - _ (underscore)
 - * (asterisk)
 - ? (question mark)
 - / (forward slash)
 - \ (backward slash)
 - . (period)
 - : (colon)
 - space
 - tab
- The following characters are not supported in LDAP filters. If you use these characters in an object filter, the reporting engine does not consider the characters for ACI information staging:
 - { open curly brace
 - } close curly brace
 - [open box bracket
 -] close box bracket
 - % (percent sign)
 - & (ampersand)
 - , (comma)
- As specified within RFC 2254, these special characters can be used as normal characters in attribute values:
 - \2a to use * as a normal character, not as a wildcard
 - \28 to use (as a left parenthesis character
 - \29 to use) as a right parenthesis character
 - \5c to use \ as a backslash character

Chapter 12. Policy administration

For your organization, you can manage policies, which are sets of organizational rules and logic.

IBM Security Identity Manager supports the following types of policies:

- Adoption policies
- Identity policies
- Password policies
- Provisioning policies
- Recertification policies
- Separation of duty policies
- Service selection policies

Note: The installation of IBM Security Identity Manager creates default data such as default provisioning and default identity policies. Do not delete the default data. When you upgrade IBM Security Identity Manager by applying a fix pack, the **ldapUpgrade** tool restores the default data if the entries are not found in the directory server. This action can affect any customized policies that you created. You can modify the default entries or disable the default policies, but do not delete the default data.

Adoption policies

During reconciliation, an *adoption policy* determines the owner of an account. An account without any owner is an *orphan account*.

An adoption policy can apply to more than one service of the same service type. An adoption policy applies only to service types that represent adapters and manual services, not service types that represent identity feeds.

An adoption policy matches the attributes for an account on a managed resource to the attributes for a Security Identity Manager user.

An adoption policy applies to the following circumstances:

- To either the entire system, as a global adoption policy, or to a specific type of managed resource, as a service-specific adoption policy. The service-specific adoption policy takes precedence over the global adoption policy.
- To more than one service.
- Only to service types that represent adapters and manual services, not service types that represent identity feeds.

Note: You cannot define service instances of different types on the same adoption policy. Account ownership assigned by adoption policies is always of the INDIVIDUAL account ownership type.

JavaScript can define adoption policies. These policies use all standard JavaScript functions and programming constructs, such as loops and conditional branches. The policies also use functions that are designed specifically for creating adoption policies. Specific JavaScript functions that return a person can retrieve personal attribute values to evaluate account owners.

Global adoption policies are defined for a service type or all service types. Global adoption policies apply to all service instances if no adoption policy is defined for the specific service. The default global adoption policy assigns an account to a user if the account user ID attribute matches the Security Identity Manager user UID attribute.

Creating an adoption policy

An administrator can create an adoption policy to use when reconciling accounts for one or more services. For example, you might create a policy that determines account ownership by attempting to match the family name of a user with the account user ID.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you can create an adoption policy, you must create one or more services to associate with the policy. If you try to create an adoption policy with a service that is already the target of an adoption policy, an error message is displayed.

About this task

To create a global adoption policy (for a specific service type), you must navigate to **Configure System > Global Adoption policies**.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Adoption Policies**.
2. On the **Work With Adoption Policies** page, in the **Adoption Policies** table, click **Create**.
3. On the **Manage Adoption Policies** page, on the **General** page, type a name for your adoption policy.
4. Click the **Services** page, and then add one or more specific services to associate with the policy. To add one or more services:
 - a) Click **Add**.
 - b) On the **Services** page, type your search criteria, and then click **Search**.
 - c) In the **Services** table, select one or more services.
 - d) Click **OK**.
5. On the **Manage Adoption Policies** page, click the **Rule** page, and then specify the attributes that the adoption policy uses to match accounts to users.

If you want to define matches, click **Add a match field** to select the account and user attributes that must match during reconciliation. The user attribute list provides a few common attribute combinations when defining the match. Such a combination might be the first letter of a given name plus the family name. The combination might be the given name plus the first letter of the family name. If your adoption policy is more complex, you can choose the more advanced path by selecting **Provide a Script**. If you defined matches, the associated scripts are populated for you in the script definition field.

Important: If you want to provide a script, the IBM Security Identity Manager Server does not verify that the JavaScript is correct. Verify that the JavaScript is correctly coded before using it to define the adoption policy.

6. Click **OK** to save the changes.
7. On the **Success** page, click **Close**. On the **Work With Adoption Policies** page, you can search to see the new adoption policy displayed in the table. The table controls can be used to change or delete the policy.

JavaScript examples for writing adoption policies

An administrator of IBM Security Identity Manager, and can use JavaScript examples to write adoption policies.

Example 1

The following example shows a simple script that matches the account user ID to the alias field of the person.

```
var ps = new PersonSearch();
return ps.searchByFilter("", "(eraliases="+subject.eruid[0]+")", 2);
```

Example 2

This example is a more complicated sample you can use for orphan adoption. This script uses the following three strategies to deduce an owner for an account:

1. Locate a single person with an `eraliases` entry that matches the account **eruid** field.
2. If this action yields multiple matches and the new entry has a **cn** field, check the matching list for one with a **cn** field that matches the account **cn** field.
3. If no matches are obtained in the first step, check for a matching account (the same `eruid`) in the master service, such as a Windows Active Directory Service. If this account has an owner, use that person. If all three strategies fail, return null, which causes an orphan.

Note: Log messages are written to the message log with the script category.

```
var entryUid = subject.eruid[0];
Enrole.log("script", "Starting script for eruid=" + entryUid);
/* change the following value to the name of the master service: */
/* var masterServiceName = "Master AD Service";
*/
var masterServiceName = "NT4 (local)";
/* change the following value to the service profile name of the master service:
   This change is required only if the profile of master service and profile of the
   service for which the adoption policy is defined are different */
/* var serviceNameOfMasterService = "ADProfile";
*/
var scriptResult = null;
var personsearch = new PersonSearch();
var filter = "(eraliases=" + entryUid + ")";
var psResult = personsearch.searchByFilter("", filter, 2);
if (psResult.length == 1) {
    /* found one person with matching alias */
    Enrole.log("script", "single match for eraliases=" + entryUid);
    scriptResult = psResult;
}
else if (psResult.length > 1) {
    /* more than one person matched alias.
     * if the account has a "cn" attribute value, see if this matches
     the "cn" of one of them
     */
    Enrole.log("script", "multiple matches for eraliases=" + entryUid);
    var entryCn = subject.cn;
    if (typeof entryCn != "undefined") {
        Enrole.log("script", "checking cn=" + entryCn[0]);
        for (idx=0; idx<psResult.length; ++idx) {
            var cn1 = psResult[idx].getProperty("cn");
            if (cn1.length != 0 && cn1[0] == entryCn[0]) {
                /* we found a match for the cn */
                scriptResult = psResult[idx];
                break;
            }
        }
    }
    else {
        Enrole.log("script", "cn field not defined for eruid=" + entryUid);
    }
}
else {
    /* no person matched specified alias.
     See if there is a matching account uid in the company Active Directory */
    var acctSearch = new AccountSearch();
```

```

    /* Method acctSearch.searchByIdAndService(entryUid, masterServiceName) is used
    if the profile of the master service is same as the profile of the service
    for which the adoption policy is defined.
    If the profile of master service and the profile of the service for which the
    adoption policy is defined are different then the profile name of the master
    service is passed to the searchByIdAndService() method as follows-
    var asResult = acctSearch.searchByIdAndService(entryUid, masterServiceName,
    serviceProfileNameOfMasterService); */
var asResult = acctSearch.searchByIdAndService(entryUid, masterServiceName);
if (asResult != null && asResult.length == 1) {
    /* found a matching AD account -- use this accounts owner,
if it is not an orphan */
    var owner = asResult[0].getProperty("owner");
    if (owner.length == 1) {
        var owner_dn = owner[0];
        Enrole.log("script", "single match for service " + masterServiceName + " uid="
+ entryUid + ", returning person with dn=" + owner_dn);
        scriptResult = new Person(owner_dn);
    }
    else {
        Enrole.log("script", "service " + masterServiceName + " uid="
+ entryUid + " is an orphan");
    }
}
else {
    Enrole.log("script", "No match or more than one match for uid=" + entryUid
+ " on master service " + masterServiceName);
}
}
return scriptResult;
/* end of script */

```

Example 3

The following example checks to see whether the name of a person, the gecos field in Linux, matches their full name in IBM Security Identity Manager, , and .

```

/*
 * OrphanAdoption JavaScript
 */

if (subject["gecos"] == null) {
    return null;
} else {
    var buf = "|";

    for (i = 0; i < subject["gecos"].length; i++) {
        buf += "(cn=" + subject["gecos"][i] + ")";
    }

    buf += ")";

    var ps = new PersonSearch();
    /* Have to use sub-tree search type (2) */
    return ps.searchByFilter("Person", buf, 2);
}

```

Example 4

This example uses the new JavaScript API ExtendedPerson to adopt a "root" account as a "System" account and adopt other accounts as "Individual" accounts.

```

/*
 * OrphanAdoption JavaScript
 */

if ((subject["eruid"]==null)){
    return null;
} else if (subject["eruid"]!=null){
    var buff='|';
    for (i=0;i<subject["eruid"].length;i++){
        buff+='(uid='+subject["eruid"][i]+' )';
    }
    buff+=')';

    var ps = new PersonSearch();

```

```

var searchResult = ps.searchByFilter("",buff, 2);
if (searchResult!=null && searchResult.length==1) {
    var person = searchResult[0];

    // If it is a "root" account, adopt it as a "System" account;
    // otherwise, adopt it as an "Individual" account by default.
    if (subject.eruid[0] == "root") {
        return new ExtendedPerson(person, "System");
    } else {
        return person;
    }
} else if (searchResult!=null && searchResult.length>1) {
    return searchResult;
} else {
    return null;
}
}

```

Changing an adoption policy

An administrator can change an adoption policy for specific services. For example, you might change an adoption policy to associate the policy with additional instances of a service type.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

The effect of changes to an adoption policy can be seen when the next reconciliation is run. Changing an existing adoption policy does not affect existing accounts of the specific service or service type. Changes do not affect accounts that are already adopted. Only new and existing orphan accounts are adopted, based on the new policy.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Adoption Policies**.

Note: To change a global adoption policy for a specific service type, you must navigate to **Configure System > Global Adoption policies**.

2. On the **Work With Adoption Policies** page, type information about the adoption policy or service in the **Search information** field.
You can type an asterisk (*) as a wildcard.
3. Select a filter in the **Search by** field, and then click **Search**.
4. In the **Adoption Policies** table, locate and select the adoption policy that you want to change, and then click **Change**.
5. On the **Manage Adoption Policies** page, modify the information on the General, Service, and Rule pages.
6. Click **OK** to save the changes.
7. On the **Success** page, click **Close**.

Deleting an adoption policy

An administrator can delete an adoption policy for specific services.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Deleting an existing adoption policy does not affect existing accounts of the specific service or service type.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Adoption Policies**.
2. On the **Work With Adoption Policies** page, type information about the adoption policy or service in the **Search information** field.
You can type an asterisk (*) as a wildcard.
3. Select a filter in the **Search by** field, and then click **Search**.
4. In the **Adoption Policies** table, locate and select an adoption policy that you want to delete, and then click **Delete**.
5. On the **Confirmation** page, review the adoption policy to delete, and then click **Delete**.
6. On the **Success** page, click **Close**.

Attribute matching

An adoption policy matches the attributes for an account on a managed resource to the attributes for an IBM Security Identity Manager user. If the match occurs, the account is assigned to the user so that the user owns the account. For example, the user can change the IBM Security Identity Manager account password. Otherwise, the account is identified as an orphan.

The default global adoption policy assigns an account to a user if the account user ID attribute matches the IBM Security Identity Manager user UID attribute.

Matching can use either single or multi-valued attributes. Matching occurs if the string value is identical to one of the following attributes:

- A single account attribute and a single user attribute
- Either a single attribute or any multi-valued attribute for either the account attribute or the user attribute

Account reconciliation and orphan accounts

Reconciliation uses an adoption policy to determine the owner of an account, or to identify the account as an orphan.

An adoption policy does not alter the ownership of accounts that are already owned within IBM Security Identity Manager.

Reconciliation uses either a global or a service-specific adoption policy. Reconciliation determines whether the user ID attribute for an account on a managed resource matches an alias attribute for a IBM Security Identity Manager user. If no match occurs, the account is identified as an orphan. Later, an administrator can manually assign orphan accounts to owners.

By default, during reconciliation, the global adoption policy is evaluated to determine the owner of an account by matching the account UID to the user UID.

Adoption policies can be defined at a global level, for a service type, or for a particular service instance. If more (or fewer) than one person is evaluated as the owner of the account, the account is orphaned.

Identity policies

An *identity policy* defines the characteristics of a user ID used when requesting a new account. An administrator defines the targets and the rule that is used to generate user IDs automatically for the services to which the rule is applied. The user ID can be based on attributes of the user for whom the account is being created.

An identity policy generates a default user ID used when requesting a new account. An administrator defines the rule to generate the user ID and specifies the service targets that apply.

Identity policies can be defined for the following targets:

All services

The same policy is used for all services.

Types of services

The policy is used for generating user IDs for services of the specified type.

Service instances

The policy is used for generating user IDs for the specified services.

Note: The default identity policy is used to generate the user ID when creating users, when the system is configured to provision Security Identity Manager accounts automatically to users.

A basic approach requires no scripting. You can define basic rules for an identity policy. Basic rules can specify which attributes to use, how many characters are used from each attribute, and what case to use when creating a user ID.

An advanced approach involves scripting, and you can use it to define more complex and customized rules. Security Identity Manager provides a default script you can modify. See the example section for an illustration of the advanced approach, which includes use of JavaScript.

To set a character limit, an identity policy rule defines the number of characters to use from a first and second attribute to form the user ID. Forming the user ID from the attributes has the following conditions:

- If the number of characters in the attribute is greater than the specified character limit, only the character limit is used.
- If the number of characters in the attribute is less than or equal to the specified character limit, the entire value of the attribute is used.
- If a second attribute is not specified, only the first attribute is used.
- If a duplicate user ID exists when Security Identity Manager creates a user ID, the process appends an integer to the new user ID to create a unique user ID.

An identity policy rule determines whether case modification occurs in forming a user ID. You can set the following conditions:

- Lowercase (default)
- Existing case
- Uppercase

If the identity policy generates a user ID with a null value, Security Identity Manager attempts to form a user ID. Security Identity Manager uses the first letter of the user's given name, concatenated with the value of the user's family name, retaining the existing case.

Name and **Business unit** are required fields when you are creating an identity policy. **Business unit** is populated with your organization name if you are authorized to create identity policies at the organization level. If you do not have that authority, the **Business unit** field is blank. You must search for a business unit where you have the authority to create an identity policy.

Identities

An *identity* is the subset of profile data that uniquely represents a person in one or more repositories, and includes additional information related to the person.

For example, an identity might be represented by a unique combination of the given, family, and full names of a person, and an employee number. The data might also contain additional information such as a telephone number, the office number, and an email address.

Identity policy script example (advanced approach)

Identity policies can be defined dynamically through the use of JavaScript (the advanced approach). Policies can also be defined with the basic method (which does not require any JavaScript). JavaScript can use all standard functions and programming constructs, including loops and conditional branches.

The values of personal attributes can be retrieved with the IBM Security Identity Manager specific JavaScript functions. The context of the script is a user (person) for whom the identity is being generated. A JavaScript object that represents the person within the IBM Security Identity Manager data model named `subject` represents this context.

The following example illustrates the advanced mode of creating user IDs with the `uid` attribute (or given name, if the `uid` attribute is empty) for an individual. The script also checks whether the user ID is already used. If the user ID is already in use, the script adds a number to the end of the user ID, making it unique.

```
function createIdentity() {
    var EXISTING_CASE = 0;
    var UPPER_CASE = 1;
    var LOWER_CASE = 2;
    var tf = false;
    var identity = "";
    var baseidentity = "";
    var counter = 0;
    var locale = subject.getProperty("erlocale");
    var fAttrKey = "uid";
    var sAttrKey = "";
    var idx1 = 0;
    var idx2 = 0;
    var fCase = 2;
    var sCase = 2;
    if ((locale != null) && (locale.length > 0)) {
        locale = locale[0];
    }
    if (locale == null || locale.length == 0)
        locale = "";
    var firstAttribute = "";
    var secondAttribute = "";
    if (((fAttrKey != null) && (fAttrKey.length > 0)) || ((sAttrKey != null)
    && (sAttrKey.length > 0))) {
        if ((fAttrKey != null) && (fAttrKey.length > 0)) {
            firstAttribute = subject.getProperty(fAttrKey);
            if (((firstAttribute != null) && (firstAttribute.length > 0)))
                firstAttribute = firstAttribute[0];
            if (firstAttribute == null || firstAttribute.length == 0)
                firstAttribute = "";
            else {
                firstAttribute = IdentityPolicy.resolveAttribute(fAttrKey,
                firstAttribute);
                if ((idx1 > firstAttribute.length) || (idx1 == 0))
                    idx1 = firstAttribute.length;
                firstAttribute = firstAttribute.substring(0, idx1);
            }
            if (fCase == UPPER_CASE)
                firstAttribute = firstAttribute.toUpperCase(locale);
            else if (fCase == LOWER_CASE)
                firstAttribute = firstAttribute.toLowerCase(locale);
        }
        if ((sAttrKey != null) && (sAttrKey.length > 0)) {
            secondAttribute = subject.getProperty(sAttrKey);
            if (((secondAttribute != null) && (secondAttribute.length > 0)))
                secondAttribute = secondAttribute[0];
            if (secondAttribute == null || secondAttribute.length == 0)
                secondAttribute = "";
            else {
                secondAttribute = IdentityPolicy.resolveAttribute(sAttrKey,
                secondAttribute);
                if ((idx2 > secondAttribute.length) || (idx2 == 0))
                    idx2 = secondAttribute.length;
                secondAttribute = secondAttribute.substring(0, idx2);
            }
            if (sCase == UPPER_CASE)
                secondAttribute = secondAttribute.toUpperCase(locale);
            else if (sCase == LOWER_CASE)
                secondAttribute = secondAttribute.toLowerCase(locale);
        }
        baseidentity = firstAttribute + secondAttribute;
    }
    if ((baseidentity == null) || (baseidentity.length == 0)) {
```

```

var givenname = subject.getProperty("givenname");
if (((givenname != null) && (givenname.length > 0)))
    givenname = givenname[0];
if (givenname == null || givenname.length == 0)
    givenname = "";
else
    givenname = givenname.substring(0, 1);
baseidentity = givenname + subject.getProperty("sn")[0];
}
tf = IdentityPolicy.userIDExists(baseidentity, false, false);
if (!tf) {
    return baseidentity;
}
while (tf) {
    counter+=1;
    identity = baseidentity + counter;
    tf = IdentityPolicy.userIDExists(identity, false, false);
}
return identity;
}
return createIdentity();

```

Creating an identity policy

An administrator can create an identity policy for use by all service types, specific service types, or specific service instances. For example, you can create an identity policy that specifies that a user ID is constructed from the family name of a user and a department number.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

IBM Security Identity Manager offers two approaches, basic and advanced, for creating an identity policy. Decide which approach you want to use.

Note: If an identity policy is intended to specify a service instance as a target, that service instance must exist.

You can use the **Manage Identity Policies** notebook to create an identity policy. Identity policies do not change user IDs for accounts that exist. Rather, they are used when creating new accounts through Security Identity Manager.

Note: When you are defining a new identity policy, services that are already the target of an identity policy are listed. However, the services are not selectable from the services table on the **Add Targets** page. An error message is generated during the save operation if a target service type is already being used in another identity policy.

To create an identity policy, complete these steps:

Procedure

1. From the navigation tree, select **Manage Policies > Manage Identity Policies**.
2. On the **Work With Identity Policies** page, in the **Identity Policies** table, click **Create**.
3. On the **Manage Identity Policies** page, on the **General** page, type a name and select a business unit for your identity policy.

Note: On the General Page, you can optionally specify a caption to provide additional information about the policy and a description of its purpose. You can specify keywords to reference the identity policy and a status. The status value is enabled to use the policy and make it active, or disabled to make the policy inactive. You can also specify a user type to which the identity policy applies. You can specify the extent to which the identity policy applies to a business unit or to a business unit and subunits.

4. Click the **Targets** page. Add one or more services or service types to which the identity policy applies, or specify that the policy applies to all service types:
 - To specify that the identity policy applies to all service types, select **All service types**.
 - To specify that the identity policy applies to specific service instances:
 - a. Click **Add**.
 - b. On the **Add Targets** page, specify your search criteria, and then click **Search**.
 - c. In the **Services** table, select a service.

Note: If you select the box at the top of the column, all services are targeted. To apply all service *types*, select **All Service Types**. If you select **All Service Types**, you cannot add specific service types or instances. If you want to apply the policy to selected service types or instances, ensure that **All Service Types** is not selected.
 - d. Click **OK**.
 - To specify that the identity policy applies to a specific service type:
 - a. Click **Add**.
 - b. Select a Target type of Service type.
 - c. Select the service type to which you would like the identity policy to apply.
 - d. Click **OK**.

The script field is populated with the default identity policy for the Person user type.

5. On the **Manage Identity Policies** page, click the **Rule** page to specify the schema attributes that the identity policy uses to create a user ID.
 - To use a basic input mode that applies a rule with schema attributes, select **Simple - define rule** and provide the following details:
 - A first attribute, its character limit, and its type of case (existing, upper, or lower)
 - (Optionally) a second attribute, its character limit, and its type of case (existing, upper, or lower)

A blank value for character limit means no limit, and the entire attribute is used. If a duplicate user ID exists at the time an account is requested, an integer is appended to the user ID and incremented until a unique user ID is determined.
 - For the identity policy that uses JavaScript code, select **Advanced - define script**. The script field is populated with the default identity policy for the Person user type.
6. Click **OK** to save the changes.
7. On the **Success** page, click **Close**.

Changing an identity policy

An administrator can change an identity policy to meet your organizational requirements for user IDs. For example, you might change an identity policy to use the office number of a user when a new user ID is created.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Changes to the identity policy affect only new accounts; old accounts are not affected by these changes.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Identity Policies**.

2. On the **Work with Identity Policies** page, type information about the identity policy, service, or business unit in the **Search information** field, or use an empty value. Select a filter in the **Search by** field and click **Search**.
3. In the **Identity Policies** table, locate and select an identity policy, and click **Change**.
4. On the **Manage Identity Policies** page, modify the information on the General, Targets, and Rule pages. The business unit designation cannot be changed for an identity policy that is already created.
5. Click **OK** to save the changes.
6. On the **Success** page, click **Close**.

Deleting an identity policy

An administrator can delete an identity policy that is not needed to manage user IDs. Deleting an identity policy causes the services that are using the identity policy to use another identity policy. For example, the services use the default identity policy that applies to all services.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

If an applicable identity policy is not defined and the identity policy of a service is deleted, the **user ID** field on the corresponding account form is blank.

To delete an identity policy, complete these steps:

Procedure

1. From the navigation tree, select **Manage Policies > Manage Identity Policies**.
2. On the **Work With Identity Policies** page, type information about the identity policy, service, or business unit in the **Search information** field, or use an empty value. Select a filter in the **Search by** field, and click **Search**.
3. In the **Identity Policies** table, locate and select an identity policy, and then click **Delete**.
4. On the **Confirm** page, review the identity policy to delete, and then click **Delete**.
5. On the **Success** page, click **Close**.

Password policies

A *password policy* defines the password strength rules that are used to determine whether a new password is valid.

A *password strength rule* is a rule to which a password must conform. For example, password strength rules might specify that the minimum number of characters of a password must be 5. The rule might also specify that the maximum number of characters must be 10.

A password policy sets the rules that passwords for a service must meet, such as length and type of characters allowed and disallowed. Additionally, the password policy might specify that an entry is disallowed if the term is in a dictionary of unwanted terms. To select this choice in the user interface, you must first load a `dictionary.ldif` file into the IBM Security Identity Manager.

You can specify the following standards and other rules for passwords:

- Minimum and maximum length
- Character restrictions
- Frequency of password reuse
- Disallowed user names or user IDs

- Specify a minimum password age

Note:

- If password synchronization is enabled, the administrator must ensure that password policies do not have any conflicting password strength rules. When password synchronization is enabled, Security Identity Manager combines policies for all accounts that are owned by the user to determine the password to be used. If conflicts between password policies occur, the password might not be set.

You might need to coordinate the password strength rules for the services. The first password strength rule might specify a minimum number of eight characters. Another password strength rule might specify a maximum number of *six* characters for a password. You must resolve such conflicts to enable a user to log on successfully.

- Some sites with a service such as AIX might require longer passwords for users who have root authority. You might set a value for the minimum length of a password that is shorter than the default password on the AIX server. The shorter value might cause some users with root authority to enter a password that is shorter than required, causing authentication failure.

Creating a password policy

An administrator can create a password policy for use with one or more services. For example, you might create a password policy that specifies a rule that a character can be repeated no more than three times in a password.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you create a password policy, create one or more service instances to associate with the password policy. If your policy uses a dictionary of unwanted terms, create and import the dictionary file also.

About this task

If a password policy exists for all services, other policies can still be added. However, only a single password policy can be specified for each service type or each instance of a service type. A password policy might exist for a service type. Additionally, password policies might exist for different instances of that service type. The more specific password policy overrides all others (for example, a password policy for a Windows service instance overrides a password policy for the Windows service).

Procedure

1. From the navigation tree, select **Manage Policies > Manage Password Policies**.
2. On the **Select Password Policies** page, in the **Password Policies** table, click **Create**.
3. On the **Manage Password Policies** page, on the **General** page, type a name and select a business unit for your password policy.
Optionally, you can add information about the scope of the policy, its status, keywords, a caption, and a description for the password policy.
4. Click the **Targets** page, and then choose to add all service types or choose one or more specific services to associate with the policy.
To add one or more services, complete these steps:
 - a) Click **Add**.
 - b) On the **Add Targets** page, type your search criteria, and then click **Search**.
 - c) In the **Services** table, select one or more services.
 - d) Click **OK**.

Note: Service type can also be selected as target for password policy by selecting the target type as Service Type.

5. On the **Manage Password Policies** page, click the **Rules** page. Specify the settings for the password rules that you want to use to determine whether a password entry is valid.

Note: If password synchronization is enabled, ensure that password policies do not have any conflicts. When password synchronization is enabled, IBM Security Identity Manager combines policies for all accounts that are owned by the user to determine the password to be used. If conflicts between password policies occur, the password might not be set.

6. Click **OK** to save the changes.
7. On the **Success** page, click **Close**.

Adding targets to a password policy

An administrator can add targets to an existing password policy.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Password Policies**.
2. On the **Select Password Policies** page, type information about the password policy, service, or business unit in the **Search information** field.
You can also use an asterisk (*) as a wildcard.
3. Select a filter in the **Search by** field, and click **Search**.
4. In the Password Policies table, locate and select a policy, and then click **Change**.
5. Click the **Targets** page, and either add all service types or select one or more specific services to associate with the policy.

To add one or more specific services:

- a) Click **Add**.
- b) On the **Add Targets** page, type your search criteria, and then click **Search**.
- c) In the **Services** table, select one or more services.
- d) Click **OK**.

Note: A specific Service type can also be selected as a target for password policy by selecting the target type as Service Type.

6. Click **OK** to save the changes.
7. On the **Success** page, click **Close**.

Creating a password policy rule

As an administrator, you can create a rule for an existing password policy. For example, you might create a rule that specifies the minimum number of numeric characters for a password.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Password Policies**.
2. On the **Select Password Policies** page, type information about the password policy, service, or business unit in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and click **Search**.
3. In the **Password Policies** table, locate and select a policy, and then click **Change**.
4. On the **Manage Password Policies** page, click the **Rules** page. Specify the settings for the password rules that you want to use to determine whether a password entry is valid.

Note: If password synchronization is enabled, ensure that password policies do not have any conflicts. When password synchronization is enabled, IBM Security Identity Manager combines policies for all accounts that are owned by the user to determine the password to be used. If conflicts between password policies occur, the password might not be set.

5. Click **OK** to save the changes.
6. On the **Success** page, click **Close**.

Changing a password policy

An administrator can change a password policy to meet the requirements of your organization for passwords. For example, you might change a password policy to set the minimum and maximum characters that are required for the password.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Changes to the password policy affect only new accounts. Old accounts are not affected by these changes.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Password Policies**.
2. On the **Select Password Policies** page, type information about the password policy, service, or business unit in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and click **Search**.
3. In the **Password Policies** table, locate and select a policy, and then click **Change**.
4. On the **Manage Password Policies** page, modify the information on the **General**, **Targets**, and **Rules** pages.

Note: If password synchronization is enabled, ensure that password policies do not have any conflicts. When password synchronization is enabled, IBM Security Identity Manager combines policies for all accounts that are owned by the user to determine the password to be used. If conflicts between password policies occur, the password might not be set.

5. Click **OK** to save the changes.
6. On the **Success** page, click **Close**.

Changing targets for a password policy

An administrator can change targets for an existing password policy.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Password Policies**.
2. On the **Select Password Policies** page, type information about the password policy, service, or business unit in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and click **Search**.
3. In the **Password Policies** table, locate and select a policy, and then click **Change**.
4. Click the **Targets** page. Add or remove all service types or choose to change one or more specific services that are associated with the policy. To change one or more specific services:
 - a) Click **Add**.
 - b) On the **Add Targets** page, type your search criteria, and then click **Search**.
 - c) In the **Services** table, select or clear one or more services.
 - d) Click **OK**.
5. Click **OK** to save the changes.
6. On the **Success** page, click **Close**.

Changing a password policy rule

An administrator can change a password policy rule. For example, you might change or remove the settings for an existing rule.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To change a password policy rule, complete these steps:

Procedure

1. From the navigation tree, select **Manage Policies > Manage Password Policies**.
2. On the **Select Password Policies** page, type information about the password policy, service, or business unit in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and click **Search**.

Note: If the search for password policies is done by Service, the default Service Owner ACIs limit the search to the password policies in Services that belong to the Service Owner. However, these default ACIs do not limit the search by password policy name. The default ACIs can be modified, or new ACIs can be created to change the search scope for the Service Owner.
3. In the **Password Policies** table, locate and select a policy, and then click **Change**.
4. On the **Manage Password Policies** page, click the **Rules** page. Change or remove the settings for the password rules that you want to use to determine whether a password entry is valid.

Note: If password synchronization is enabled, ensure that password policies do not have any conflicts. When password synchronization is enabled, IBM Security Identity Manager combines policies for all

accounts owned by the user to determine the password to be used. If conflicts between password policies occur, the password might not be set.

5. Click **OK** to save the changes.
6. On the **Success** page, click **Close**.

Deleting a password policy

An administrator can delete a password policy that is no longer needed to control password entries.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Deleting a password policy causes the services that are using the password policy to use another password policy, such as the default password policy.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Password Policies**.
2. On the **Select Password Policies** page, type information about the password policy, service, or business unit in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and click **Search**.
3. In the **Password Policies** table, locate and select a policy, and then click **Delete**.
4. Click **OK** to save the changes.
5. In the **Success** page, click **Close**.

Customized password rules

You can use IBM Security Identity Manager server to add customized logic for generating passwords. To add the logic you can use a customized rule, a customized generator, or a combination of both.

Adding customized logic for password rules with a customized rule

A customized password rule is used for validating both new passwords that are generated by IBM Security Identity Manager Server and existing passwords.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. Create a class by implementing *com.ibm.passwordrules.Rule interface*.
2. Register the class in `passwordrules.properties` by entering a line like the following one:

```
password.rule.com.ibm.tivoli.itim.CustomPasswordRule1=true
```

The value of this expression determines the type of interface widget that is used to create a customized rule when you define a password policy. The following values are valid:

- A value of `true` means that the instantiated rule object requires a parameter. The widget is a text box. If any value is entered, a customized rule is used. If the value is optional, typing in any printing character marks the rule for use.

- A value of `false` means that the rule does not require parameters. If the box is selected, a customized rule is used.

If more than one parameter value is required, a user-defined delimiter might separate individual values. Alternatively, the value might contain a structure that is represented by a user-defined XML document.

3. Optional: Add a label for the customized rule name.

The key for the value is the fully qualified name of the customized class. The specified value is displayed on all screens that show the password rules

```
password.rule.com.ibm.tivoli.itim.CustomPasswordRule1=Use Complexity Level 1.
```

In this example, the required prefix is followed by the fully qualified name of the customized rule class. Both parts constitute the entire property key for any customized rule.

Note: If the customized label is not defined in `CustomLabels.properties`, the fully qualified name of the customized Java class is displayed on the interface forms.

Adding a customized password generator

You can add a customized password generator for creating passwords with the IBM Security Identity Manager Server.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. Create a customized password generator class that implements the `com.ibm.passwordrules.PasswordGenerator` interface.
2. Register the customized password generator class. The customized password generator might be used by adding a line to the `passwordrules.properties` file.
For example:

```
generator.ibm.tivoli.itim.CustomGenerator
```

In this example, `generator` is the required prefix followed by the fully qualified name of the password generator class. Both parts constitute the entire property key of a customized generator. Initialization parameters can be passed to the customized generator by specifying a value for the property, as in the following example:

```
generator.ibm.tivoli.itim.CustomGenerator=value1?value2
```

This value must be defined in a format that is expected by the `initialize()` method of the generator. If the author of a customized generator class chooses not to do any initialization, the property value is ignored by the `initialize` method of the generator class.

Note: Any password generator, including the built-in one, has a global scope, and is the only one that generates passwords for accounts of all service types.

Customized logic using customized rules and a customized generator

You can use a combination of a customized rule and a customized generator to add customized logic for generating passwords.

Using standard password rules might not always be helpful or even wanted at all. You might prefer a single customized password rule to generate compliant passwords. You might use a standard set of password rules to define password policies. When you want to avoid standard rules, that preference must be known to the IBM Security Identity Manager administrator.

Mixing customized rules with a customized generator might have unforeseen implications. For example, a customized password generator implementation might be sufficient to generate valid passwords, and thus a password policy might not be required at all.

Using a customized rule might preclude the authors of password policies from using some or even all standard password rules that might be incompatible with the customized rule. However, to achieve the wanted effect, authors of customized rules or generators might decide to use a combination of both. Such an approach might be more flexible, because different parameters can be passed to individual rule definitions in password policies for different service types.

Joining rules

Any class that implements a Rule interface is expected to provide logic in its `join()` method. This logic joins parameters of two rules of the same type defined for two or more accounts of different service types. If such joins are difficult or even impossible to do, parameters of one of the two similar rules can be chosen by code. The Framework does not provide any mechanism for resolving join conflicts. The author of customized rule classes resolves such conflicts by imposing a preferred mechanism in the `join()` method itself.

Constraining the password generator

For customized password generators, which are based on an iterative algorithm, limiting the possible number of attempts during which the password might be generated is a way of ensuring that the maximum limit of iterations is not exceeded before a valid password is produced. A *valid password* is one that complies with all the rules defined for it in a password policy. Each rule class implements the `constrain()` method that tells the generator how to generate the password.

Authors of customized rule classes might choose not to implement the `constrain()` method. These authors must test the process of generating the expected password. They must test with a combination of rules, including the customized rules, which are expected to be used in production environment. The test must produce an acceptable, large number of consecutive passwords are generated without triggering the `IterationsExceededException`. If the test is successful, the mechanism is acceptable, and can be used in the production environment. Some customized password generators (for example, those generators based on a dictionary) might not require constraints at all. In such cases, `constraint()` methods although always called, do not affect the way passwords are generated.

Note: The maximum limit of iterations is hardcoded 20,000.

Internationalization

Parameter values passed to the customized generator might include Unicode characters. If the `passwordrules.properties` file contains any Unicode characters, save it in Unicode format. IBM Security Identity Manager automatically detects the format when the file is read. A file that contains Unicode characters must be viewed and edited with a text editor that can display these characters.

Alternatively, use the hex-encoded format to insert the Unicode characters into the file: `\uXXXX` or `0xXXXX`. This method makes it possible to view and edit the file in text format, but the generator class must interpret these character encodings. The `StandardGenerator` class in the password rules framework can generate passwords using Unicode characters to the extent supported by the Java virtual machine used with the IBM Security Identity Manager server.

The default character set used by the `StandardGenerator` class is uppercase and lowercase letters from the Latin alphabet. They correspond to Unicode ranges `0x0041-0x005a` and `0x0061-0x007a`, and most special characters such as `#`, `$`, and `%` that are in the ASCII set. You can extend or replace this character set by defining a parameter value for the standard generator class in the `passwordrules.properties` file. For example:

```
generator.com.access360.passwordrules.standard.StandardGenerator=  
\0x0041,0x005a \0x0061,0x007a \0x0104,0x0107 \0x0118,0x0119 \0x00d3 \0x00f3  
\0x0141,0x0144 \0x015a,0x015b \0x0179,0x017c
```

The first two ranges are the standard Latin letters. The others are from Extended Latin I and II Unicode sets. Customized rule parameter values added to password policy definitions might also be required to accept Unicode characters. Again, the two ways of specifying the Unicode values and ranges of values apply here as well. XML is used to save all rules within a password policy to the LDAP directory. The interface always displays the customized rule parameters exactly as they were entered.

Configuration of minimum password age rule

An administrator can configure a minimum password age rule to limit how frequently users can change the password on their account. This rule is provided in the password policy. By default, the rule is disabled.

The following points describe the limitations, scenarios, and configuration information about the minimum password age rule.

- The rule accepts only integer values. A user with permissions to define or edit a password policy can specify the minimum period, in hours, for a password change. A user cannot change the password on that account again within the specified period.
- IBM Security Identity Manager interprets the specified integer value for the rule in hours. Security Identity Manager does not evaluate the rule when a user specifies a negative value, 0, or no value. In other words, users can change the password on their accounts immediately.
- Security Identity Manager can evaluate the rule only in these conditions:
 - When users try to change the password on any of the accounts owned by them.
 - When the previous password change on those accounts was successfully run by the same users (owners of the accounts).

In other words, Security Identity Manager does not evaluate the rule if users other than owners of the accounts made the previous account password change. For example, help desk or system administrators.

- Security Identity Manager does not evaluate the rule when users change the password on accounts that are not owned by them. For example, Security Identity Manager does not evaluate the rule when help desk or system administrators change the password on some other user accounts. Security Identity Manager does not evaluate the rule if the password change is initiated by the system. For example, a password change initiated by the lifecycle rule or an automatic provisioning request workflow.
- Security Identity Manager maintains this information in IBM Security Directory Server:
 - Users who ran the last password change on each account object.
 - Time when the password change was run on each account object.

For some reasons, if this information is corrupted or these attributes are wiped off from the account object, then Security Identity Manager does not evaluate the rule correctly.

- Security Identity Manager stores the password change information only when the password change is initiated by using one of these resources:
 - IBM Security Identity Manager console
 - IBM Security Identity Manager Self Service or the Identity Service Center user interface
 - IBM Security Identity Manager APIs

Therefore, any information about password changes done directly on the resource or by using some other tool is not used to evaluate the rule.

Adding a customized minimum password age rule

An administrator can add a customized minimum password age rule to limit users from changing the password on their account. For example, you might want to specify the minimum time, in hours, for a password change on your account before you can change it again.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Ensure that IBM Security Identity Manager is installed.

About this task

Run the following procedure to configure and enable this rule in your environment.

If you are on a clustered environment, then repeat the following procedure on each node of the cluster. The procedure configures and enables this rule in your environment.

Note: By default, this rule is disabled.

Procedure

1. Stop WebSphere Application Server.
2. Change to the directory where the `passwordrules.properties` file is located.
For example: `$ISIM_HOME/data`.
3. Uncomment the following property in `passwordrules.properties` files to enable the new rule:

```
password.rule.com.ibm.passwordrules.standard.MinAgeConstraint=true
```

The "Minimum Password Age" label is added in the `$ISIM_HOME/data/CustomLabels.properties` file.

Note: `ISIM_HOME` is the directory where Security Identity Manager is installed.

4. Optional: Complete these steps if a language pack is installed, or if the `com.ibm.passwordrules.standard.MinAgeConstraint` key is not assigned a label in the `CustomLabels_nn.properties` file:
 - a) Edit the appropriate `$ISIM_HOME/data/CustomLabels_nn.properties` file if a language pack is installed.
`nn` is a two letter language code. For example, `en` for English.
 - b) Add the following line at the end of the file with appropriate messages for that language. Add the line after you replace the text on the right of the equals "=" sign.
For example:

```
com.ibm.passwordrules.standard.MinAgeConstraint  
=Minimum Password Age
```

Do not change the English text on the left of the equals "=" sign.

5. Change to the directory where the `tmsMessages.properties` file is located.
For example: `$ISIM_HOME/data`.
6. Back up the `tmsMessages.properties` file.
7. Using any text editor, open the `tmsMessages.properties` file.
8. Add the following message at the end of the `tmsMessages.properties` file.
For example:

```
com.ibm.passwordrules.MinAgeConstraint.MIN_AGE_VIOLATED  
=Attempting to set the password within minimum age of password.
```

If you violate the rule, this message displays on the IBM Security Identity Manager Console.

9. Save the `tmsMessages.properties` file and close the editor.

Note: Repeat Steps 5, 6, 7, 8, and 9 to edit the `tmsMessages_nn.properties` file for the language packs that you installed.

10. Start WebSphere Application Server.

Results

The **Rule** tab on the **Manage Password Policies** page displays the **Minimum Password Age** rule.

What to do next

Specify appropriate values for the minimum password age.

Provisioning policies

A *provisioning policy* grants access to many types of managed resources, such as IBM Security Identity Manager Server, Windows servers, and Solaris servers.

Each provisioning policy consists of the following components:

- General Information
- Membership
- Entitlements

A provisioning policy must target one or more service instances, service types, or a service selection policy. System administrators can use provisioning policy parameters to define attribute values that are required and values that are optional.

A provisioning policy defines the accounts and access that are authorized to users or automatically provisioned for users by the user's role. When account and access are authorized to a user by a provisioning policy, they can be requested by the user. A provisioning policy can be used to support role-based provisioning, in which accounts and access are automatically provisioned to a user, based on the user's roles.

Provisioning policies are important to support security compliance. Security Identity Manager evaluates all account and access requests based on the provisioning policy to identify accounts and access that are not authorized and take appropriate actions to handle noncompliant account and access. Based on the enforcement configuration on the service, Security Identity Manager can either mark the account or access as noncompliant. Security Identity Manager can also suspend the account, alert the administrator to revoke disallowed privilege, or automatically correct the account or access and make it compliant. A provisioning policy provides a key part of the framework for the automation of identity lifecycle management.

Security Identity Manager provides APIs that interface to information about provisioning policies defined in Security Identity Manager, and interface to the access granted to an individual task. These APIs can be used effectively to generate audit data.

When two or more provisioning policies are applied to the same user, a *join directive* defines how to handle attribute values from different policies. To work with policy joins or customize them, go to the navigation tree and select **Configure System > Configure Policy Join Behaviors**.

Provisioning policies can be mapped to services of a distinct portion or level of the organizational hierarchy. The business unit to which the provisioning policy belongs determines the services the policy governs. The scope of the provisioning policy indicates whether to cover services in the same level of the business unit or the subtree of the business unit. An entitlement in the provisioning policy support different types of service targets. Target types include all services, services of same type, services defined by service selection policy, or a specific service instance. In all cases, the services must be within the specified scope of the business unit where the policy is defined. A service selection policy enables service selection base on person attributes.

Policy enforcement

Policy enforcement is the manner in which IBM Security Identity Manager allows or disallows accounts that violate provisioning policies.

When a provisioning policy, person, account data, or dynamic role is changed, an account that was originally compliant with a provisioning policy can become noncompliant.

If a role is a member of another organizational role in a provisioning policy, then that role member also inherits the permissions of provisioning policy.

When a policy enforcement action is set to `Global`, the policy enforcement for any service is defined by the global or default configuration setting.

You can set the policy enforcement action as **Mark**, **Suspend**, **Correct**, **Alert**, or **Use Global Enforcement Action: Mark**. For more information, see *Policy enforcement actions* in [“Policy enforcement”](#) on page 737.

Provisioning policy parameter enforcement rules

The parameter enforcement types specify the rule for the system to evaluate the validity of an account attribute value.

An account that contains an invalid value is considered a noncompliant account. The role of the policy enforcement settings (**Mark**, **Suspend**, **Correct**, and **Alert**) is to specify the action the system does when the account becomes noncompliant. A **Correct** policy enforcement setting causes the system to take corrective action for the noncompliant account. Actions, include adding mandatory values to the account and removing invalid values from the account.

Use the following key to determine the enforcement type:

- M** Mandatory
- A** Allowed
- D** Default
- E** Excluded

A mandatory value is added if it is missing from an account. Default attributes are used only during account creation. Afterward, they can be used. Excluded attribute values are removed only if they are not granted in another policy.

Some adapters such as the Oracle eBS adapter support complex group attribute requests. Support for these requests requires the installation of a service profile-specific handler. For more information about handlers, see your specific adapter guide. For accesses that are related to such complex group values, typically the default subattribute values are obtained from the handler plug-in. However, if the provisioning policy for the service has a mandatory enforcement on the group attribute, that value is used instead.

The following table lists the set of valid and mandatory parameter values.

ALLOWED				ACTIONS	
M	A	D	E	Account creation	Account validation (reconciliation)
				No action.	All valid values.
X				Mandatory attributes are set.	Mandatory attributes are set to the defined value, and all other values are not valid.
	X			No action.	All defined attributes are valid, and all others are not valid.

Table 92. System attribute enforcement rules (continued)

ALLOWED				ACTIONS	
M	A	D	E	Account creation	Account validation (reconciliation)
		X		Default attributes are set.	Default attributes defined are defaulted on account creation, and all other values are also valid.
			X	No action.	Excluded attribute values are removed (all other values can be present or set on the attribute). The valid values are equal to {M + A + D + not(E)}. If a value is not contained in the set of valid values, it is removed. Note: Excluded adds values by negation to the allowed set. It does not remove values from the allowed set.
X	X			Mandatory attributes are set.	Mandatory attributes are set to the defined value. Valid values can be present or set on the attribute.
X	X	X		Mandatory and default attributes are set.	Mandatory attributes are set to the defined value. Optional and default values can be present or set on the attribute.
X	X	X	X	Mandatory and default attributes are set.	Mandatory attributes are set to the defined value. Excluded attribute values are removed. Optional and default values can be present or set on the attribute.
X		X		Mandatory and default attributes are set.	Mandatory attributes are set to a defined value. Default values can be present or set on the attribute.
X		X	X	Mandatory and default attributes are set.	Mandatory attributes are set to a defined value. Default values can be present or set on the attribute. Excluded attribute values are removed.
X			X	Mandatory attributes are set.	Mandatory attributes are set to defined values. Excluded attribute values are removed (all other values can be present or set on the attribute).
X	X		X	Mandatory attributes are set.	Mandatory attributes are set to defined values. Optional attributes are valid, and must be one of the defined values if a value is set. Excluded attribute values are removed (all other values can be present or set on the attribute).
	X	X		Default attributes are set.	Optional attributes are valid and must be one of the defined values if a value is set. Default attributes are valid.
	X	X	X	Default attributes are set.	Optional attributes are valid, and must be one of the defined values if a value is set. Default attributes are valid. Excluded attribute values are removed (all other values can be present or set on the attribute).
	X		X	No action.	Optional attributes are valid, and must be one of the defined values if a value is set. Excluded attribute values are removed (all other values can be present or set on the attribute).
		X	X	Default attributes are set.	Default attributes are valid. Excluded attribute values are removed (all other values can be present or set on the attribute).

Creating a provisioning policy

An administrator can create a provisioning policy.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Organizational roles and services that the provisioning policy uses must be in place before you add the provisioning policy.

If a role is a member of another organizational role in a provisioning policy, then that role member also inherits the permissions of provisioning policy.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Provisioning Policies**.
2. On the **Manage Provisioning Policies** page, in the **Provisioning Policies** table, click **Create**.
3. On the **Manage Provisioning Policies** page, on the **General** page, type a name and a priority number, and select a business unit for your provisioning policy.
Optionally, you can also specify the scope, a caption, a description, keywords, and the policy status.
4. Click the **Members** page, and select the member type that you want to associate with the provisioning policy.
If you select **Roles specified below**, complete these steps to add one or more roles to the **Roles** table:
 - a) Click **Add**.
 - b) On the **Organizational Role** page, specify your search criteria, and then click **Search**.
 - c) In the **Roles** table, select one or more roles.
 - d) Click **OK**.
5. On the **Manage Provisioning Policies** page, click the **Entitlements** page, and add one or more entitlements to the provisioning policy:
 - a) Click **Create**.
 - b) On the **Account Entitlement** page, select the provisioning option, ownership type, target type, and a workflow. Select the service type and service, if applicable.
 - c) Click **OK**.
6. Click **Submit** to save the policy.
7. On the **Schedule** page, choose to create the provisioning policy immediately or select a specific date and time. Then, click **Submit**.
8. On the **Success** page, click **Close**.

Changing a provisioning policy

As an administrator, you can modify a provisioning policy.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

System administrators can modify provisioning policies by changing the policy definition, membership, or entitlement.

If a role is a member of another organizational role in a provisioning policy, then that role member also inherits the permissions of provisioning policy.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Provisioning Policies**.
2. On the **Manage Provisioning Policies** page, type information about the provisioning policy in the **Policy information** field, or type an asterisk (*), and click **Search**.
3. In the **Provisioning Policies** table, locate and select a provisioning policy, and click **Change**.
4. On the **Manage Provisioning Policies** page, modify the information on the **General, Members, and Entitlements** pages.
5. Click **Submit** to save the changes.
6. On the **Schedule** page, indicate whether to change the provisioning policy immediately or select a specific date and time. Then, click **Submit**.
You can indicate to submit changes only, or to submit the entire policy.
7. On the **Success** page, click **Close**.

Previewing a modified provisioning policy

An administrator can preview the effect of a provisioning policy on users before adding, modifying, or deleting the policy.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Previewing a provisioning policy provides you with a summary of the number of accounts that are affected and specific details for each account that the policy impacts. The provisioning policy preview provides details about the accounts that are:

- Provisioned
- Suspended
- Deleted
- Modified
- Marked as noncompliant
- Get a changed status from noncompliant to compliant

If the results of the preview are what you expected, you can continue submitting and activating the policy. If the results of the preview are not what you expected, you can revise the policy.

When you preview a modified policy, you can choose to have IBM Security Identity Manager compute the impact of the entire policy on all users that belong to policy memberships. Alternatively, you can choose to compute only the impact of the changes you made to the policy. For example, you modified an existing provisioning policy to include a newly defined role. You might want to preview the results of the modified policy selectively as they apply to users who were assigned to that role.

If a role is a member of another organizational role in a provisioning policy, then that role member also inherits the permissions of provisioning policy.

If you change the ownership type of a service policy entitlement, accounts are evaluated based on that ownership type. Accounts with a different ownership type than the one specified in the changed entitlement are disallowed on that service. The exceptions are if you change the ownership type to All or the ownership type is covered by another entitlement on the same policy. In those cases, the accounts are not disallowed.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Provisioning Policies**.
2. On the **Manage Provisioning Policies** page, type information about the provisioning policy in the **Policy information** field, or type an asterisk (*), and click **Search**.
3. In the **Provisioning Policies** table, locate and select a provisioning policy, and click **Change**.
4. On the **Manage Provisioning Policies** page, modify the information about the **General, Members, and Entitlements** pages, and click **Preview**.
5. On the **Preview Policy Enforcement** page, select **Enforce changes only** or **Enforce entire policy**.
6. Click **Continue**.

The preview is generated and displayed on the **Preview Policy Summary** page, which is categorized by the following states:

- Disallowed accounts
- Noncompliant accounts
- Compliant accounts

Click a category of account changes to view the individual accounts that the policy changes affect.

7. On the **Preview Policy Summary** page, click **Close**.

What to do next

After you determine that the effects of the policy changes are acceptable, the changes can be submitted to the system.

Creating a draft of an existing provisioning policy

As an administrator, you can modify an existing provisioning policy and save the modified policy as a draft, without committing the changes to the system.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You might save an existing provisioning policy as a draft. Both the original and the draft versions are listed on the **Manage Provisioning Policies** page in the **Provisioning Policies** table. When you commit the draft version to the system, it replaces the original, which is removed from the system, along with the draft version.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Provisioning Policies**.
2. On the **Manage Provisioning Policies** page, type information about the provisioning policy in the **Policy information** field, or type an asterisk (*), and then click **Search**.
3. In the **Provisioning Policies** table, locate and select a provisioning policy, and click **Change**.
4. On the **Manage Provisioning Policies** page, modify the information on the **General, Members, and Entitlements** pages.
5. Click **Save as Draft**.
6. On the **Success** page, click **Close**.

Committing a draft provisioning policy

As an administrator, you can commit a provisioning policy draft.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

When you commit a draft version to the system, it replaces the original provisioning policy, which is removed from the system, along with the draft version.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Provisioning Policies**.
2. On the **Manage Provisioning Policies** page, type information about the provisioning policy in the **Policy information** field, or type an asterisk (*), and click **Search**.
3. In the **Provisioning Policies** table, locate and select a provisioning policy draft, and click **Change**.
4. On the **Manage Provisioning Policies** page, click **Submit** to commit the draft.
5. On the **Schedule** page, indicate whether to change the provisioning policy immediately or select a specific date and time. Then, click **Submit**.
6. On the **Success** page, click **Close**.

Deleting a provisioning policy

An administrator can delete a provisioning policy. Deleting a provisioning policy removes all accounts that this policy created.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you delete a provisioning policy, confirm that you want to delete all the memberships and entitlements that are contained in that policy. If a role is a child role of another organizational role in a provisioning policy, then that child role also inherits the permissions of provisioning policy. Therefore, when you delete a provisioning policy, the permissions of the child roles might be deleted or suspended.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Provisioning Policies**.
2. On the **Manage Provisioning Policies** page, type information about the provisioning in the **Search information** field, or type an asterisk (*) and click **Search**.
3. In the **Provisioning Policies** table, locate and select a provisioning policy, and click **Delete**.
4. On the **Confirm** page, review the provisioning policy to be deleted, choose a date and time for the deletion to occur, and click **Delete**.
5. On the **Success** page, click **Close**.

Managing provisioning policies by role

As an administrator, you can manage provisioning policies that are associated with roles.

Before you begin


Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

System administrators can manage provisioning policies that are associated with roles.

If a role is a member of another organizational role in a provisioning policy, then that role member also inherits the permissions of provisioning policy.

Procedure

1. From the navigation tree, select **Manage Roles**.
The **Manage Roles** page is displayed.
2. On the **Manage Roles** page, complete these steps:
 - a) Type information about the role in the **Search information** field.
 - b) In the **Search by** field, specify whether to search against role name or description, or against business units, and then click **Search**.
A list of roles that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
3. In the **Roles** table, click the icon () next to the role, and then click **Manage Provisioning Policies**.
The **Work With Provisioning Policies** page is displayed.
4. On the **Work With Provisioning Policies** page, you can create, change, or delete provisioning policies.
5. When you are finished managing the provisioning policies, click **Close** to close the page.

Recertification policies

Recertification simplifies and automates the process of periodically revalidating a target type (account or access) or a membership (role or resource group). The recertification process validates whether the target type or membership is still required for a valid business purpose. The process sends recertification notification and approval events to the participants that you specify. A *recertification policy* includes activities to ensure that users provide confirmation that they have a valid, ongoing need for a specified resource or membership.

A recertification policy defines how frequently users must certify their need for a resource or membership. The policy also defines the operation that occurs if the recipient declines or does not respond to the recertification request. Recertification policies use a set of notifications to initiate workflow activities that are involved in the recertification process.

There are three recertification target types:

- User
- Account
- Access

A user recertification, unlike an account or access recertification, allows you to certify roles, accounts, and groups (which include accesses) for the specified user within a single activity.

A recertification policy is implemented as a workflow. A default workflow is automatically built for simple policies. A recertification policy can prompt a recipient, such as a manager or system administrator to certify periodically that users still need to use accounts. The workflow generates an e-mail notification of the work item to be completed for recertification and generates To Do activities to request that the participant accept or reject the recertification.

A service owner can create a recertification policy for services and accesses that are administered by the user. A system administrator can create a recertification policy for all users, services, and accesses. For example, as an administrator, you can define a recertification policy that sets a 90-day interval for account recertification. If the recipient of the recertification request declines recertification, the account

is suspended. The owner of the account that was rejected during recertification is notified by email based on the message template configured in the policy.

The recertification policy access control item (ACI) controls what a user can view or do with recertification policies. IBM Security Identity Manager provides default access control items that target recertification policies. The following table shows how changes to the default ACIs affect what you can see or do with the policies.

Who is permitted	Target object and access control item	Effect
Service owner group	Recertification policy - add, modify, remove, or search	Allows service owners to manage recertification policies.
Auditor or manager group	Recertification policy - search	Allows members of the auditor group or manager group to search or view recertification policies.
Auditor, manager, or service owner groups	Reports (recertification pending, history, and policies) run operation	Allows members of these groups to view these reports.

Audits that are specific to recertification are created for use by several reports that are related to recertification:

Accounts or access pending recertification

Provides a list of recertifications that are not completed.

Recertification change history (for accounts and accesses)

Provides a historical list of recertifications.

Recertification policies (for accounts and accesses)

Provides a list of all account and access recertification policies.

User recertification history report

Provides a historical list of user recertifications.

User recertification policy definition report

Provides a list of user recertification policies.

Resource selection for recertification

Security Identity Manager does not select accounts for recertification in the following circumstances:

- The ITIM Service account of the ITIM administrator (the actual name of the account and service inside Security Identity Manager) is not selected for recertification so that it is not deleted or suspended inadvertently. Any other ITIM account can be selected.
- Orphan accounts, which are accounts with no owners, are not selected for recertification.
- Account and access recertification policies do not select resources if the rejection of the resource results in the same operation. For example, if the rejection action is to suspend the accounts, the recertification policy does not select accounts that are already suspended because the rejection of the recertification would suspend the accounts, which has already occurred. If the rejection action is to delete the accounts after the accounts are suspended, the accounts are selected for recertification because a different action, such as deleting the suspended accounts, had not already occurred.

Recertification policy targets

Recertification policies can target various resources and memberships. Account recertification policies target accounts on specific services. Access recertification policies target specific accesses. User

recertification policies can target a combination of role memberships, accounts on services, and groups on services (including groups defined as access).

There is a restriction with account and access policies:

- A service can be a member of only one account recertification policy
- An access can be a member of only one access recertification policy

These restrictions do not apply to user recertification policies. A user recertification policy might include services or accesses that are already part of another policy.

Recertification policy configuration modes

The configuration mode determines how you build the policy. The following modes are available:

Simple

If you use the simple mode, a workflow is automatically built, using the options that are selected on the Policy page.

Advanced

If you use the advanced mode, the workflow designer is launched with a simple workflow defined as the base configuration, using the options selected on the **Policy** page. The workflow can be further customized for business needs.

Note: If a policy is changed from simple to advanced mode, the policy cannot revert to a simple state without losing changes. The policy reverts to the default simple recertification workflow.

Viewing recertification status

Recertification requests can be viewed in **View Requests**. To find recertification requests, select the **View All Requests By Service** view or **View All Requests** view.

For services, see the option in the task list by service to view Account Recertification Status, and navigate to **Manage Services > Select a Service**. Click the icon adjacent to a service name and select **Account Recertification Status** to get to the status page.

For group access entitlements, to view Access Recertification Status, navigate to **Manage Groups > Select a Service**. Select the service and click **OK**. Then, click the icon adjacent to the group for the accesses and select **Access Recertification Status**.

Note: On the service protection category for ACIs is a new operation called Recertification Override that specifies which users can view and override the recertification status of an account. A similar ACI exists on the group protection category to specify which users can view and override the recertification status of an access.

Recertification policies and reports

Recertification reports can be requested by system administrators, service owners, managers, and auditors, based on ACIs. Included are reports of the following types:

- Accounts/Access Pending Recertification Report
- Recertification Change History Report
- Recertification Policies Report
- User Recertification History Report
- User Recertification Policy Definition Report

The actions taken during an account or access recertification policy run are stored in a database table RECERTIFICATIONLOG that is referenced by the recertification history report.

The actions taken during a user recertification policy run are stored in database tables named USERRECERT_HISTORY, USERRECERT_ROLE, USERRECERT_ACCOUNT, and USERRECERT_GROUP, which are referenced by the user recertification history report.

Note: Recertification audit events are generated from recertification policy workflows only, rather than from operational workflows.

Recertification activities

A *recertification activity* is displayed in the to-do list, and you can use it to approve or reject a user's need for a membership or access to a resource.

While recertification is underway, the user can continue to use the target type in question. If recertification is rejected, the account, access, group membership, or role membership might be marked, suspended, or deleted based on the configuration of the policy. The recertification approval activity does not necessarily go to the account owner. The participant can be specified using the **Who approves recertification** field in the **Policy** tab. Approvers can be the account owner, administrator, service owner, manager, user, organizational role, group, or access owner, depending on the specific type of recertification policy.

Depending on the policy configuration, the to-do task does not necessarily require completion. For example, the policy can be configured to take the positive path for approving recertification, so that if no action is taken on the to-do task, continued use is approved.

Note: You can set the **Timeout** action on the **Policy** tab to dictate the behavior.

Based on provisioning policy configuration, certain accounts and groups might be omitted from a user recertification activity even when the accounts and groups are within the scope of the user recertification policy. For example, groups that are mandatory on an account are always omitted from the activity. Accounts that are automatically provisioned for the user are also omitted from the activity as long as the user does not have additional accounts on the same service. If the user has multiple accounts on an automatically provisioned service, all the accounts are displayed in the user recertification activity. The recertifier must recertify at least one of the accounts on the service to submit the activity. Some accounts might be displayed in the activity for display purposes only if the accounts themselves do not require recertification, but have groups that require recertification.

Run option

You can click **Run** on the recertification policy management interface to cause the recertification policy to be evaluated on demand.

Note: Any schedule that is defined inside the policy remains intact if you click **Run**. The scheduled evaluation occurs regardless of whether **Run** was recently performed on demand. If you want to run the policy on demand only, disable the policy so that the scheduled evaluation does not occur.

Recertification message templates and schedule

A recertification policy defines the content of an email notification to participants and the interval that triggers a request for recertification.

The email notification alerts you to recertify a need for a specified membership or access to a resource. The action to be taken when the user does not complete the request by the due date is specified using the **Timeout Action** setting, which is set to **Approve** by default.

Note: If the recertification is approved or rejected, you can provide optional text for justifying the rejection. The text that is entered in the to-do list is audited, and can be seen in the Recertification Change History report or the User Recertification History report, depending on the type of policy.

You can create customized message templates for the recertification email and the rejection email.

The recertification email goes to the person who is responsible for recertification and approves recertification. You can modify the email template to provide recertification notices to participants. The recertification email table contains the list of templates that can be used for notification of rejected recertification. The table, which can be sorted, contains **Select**, **Name** (such as Delete Access or Remove Account), and **Subject** columns.

The Rejection email template can be customized to provide rejection notices to participants. The Rejection email table contains the list of templates that can be used for notification of rejected

recertification. The table, which can be sorted, contains **Select, Name** (such as Delete Access or Remove Account), and **Subject** columns.

Note: You can also create your own template. The default templates cannot be modified, but they can be copied to use as the starting point for a new template.

Scheduling options

You can configure a schedule to specify the frequency at which recertification occurs.

You can use the following scheduling options when creating a recertification policy:

- Calendar option
- Rolling option

Calendar option

Use the calendar option to set the schedule for the policy evaluation period. Recertification for all users, accounts and accesses that are targeted by the given policy then occur at the same time. If the setting is monthly on the first day of the month, and the policy targets a service, the recertification policy workflow is triggered on all accounts on that service at the first of every month.

You can use the following types of options:

Daily

Recertifies targets every day.

Hourly

Specify the minute of the hour.

Weekly

Specify the day of the week.

Monthly

Specify the day of the month (1-28).

Quarterly

Specify the day of the quarter (1-90).

Annually

Specify the month and day (for example, Jan 28).

Semi-annually

Specify the day (1-180).

During a specific month

Specify the month and day of week or daily and set at a specific time, for example, 12:00 AM.

After specifying the policy evaluation period, you must set the time at which the recertification policy workflow is to be run (for example, 12:00 AM).

Rolling option

You can set the rolling option to ensure that only those targets that have not been recertified within a specified interval are subject to recertification when the policy is evaluated. For example, if an account policy is scheduled for weekly evaluation with a rolling interval of 90 days, only the accounts that were recertified more than 90 days prior are subject to recertification each week. The rolling option is not available for access recertification.

A rolling schedule and calendar schedule are identical in terms of how often the recertification policy is evaluated. The difference is that a calendar schedule always triggers recertification for the target resources when the policy evaluates. A rolling schedule, however, triggers recertification only for the target resources that have not been recertified within the specified interval when the policy evaluates.

Recertification policy results

Depending on the user response, a recertification policy can mark an account, access, group membership, or role membership as recertified. The recertification policy can also suspend or delete the resource or membership.

Recertification states for accounts and accesses

After an activity is completed, an account or access can be in one of the following states:

Active

The account or access target is marked as recertified, and no further action is taken. It is not suspended or deleted. If approved, the target remains active, and the entry of the owner is updated.

Marked

The workflow marks the account or access as not certified and issues a rejection notification. The contents of the rejection notification are configured in the policy definition.

Suspended

The workflow suspends the account or access and issues suspension notifications. Suspended is not an option for access recertifications because an access cannot be suspended.

Deleted

The workflow deletes the target type and issues rejection notifications.

Note: Audit records are created for each of these actions. The records can be read with the Recertification Change History report. Recertification status for accounts and access entitlements can also be seen with the **Account Recertification Status** or **Access Recertification Status** pages.

Recertification states for group membership and role membership

After a recertification activity is completed, a role membership or group membership can be in one of the following states:

Active

The membership is marked as recertified, and no further action is taken.

Marked

The membership is marked as not certified, and a rejection notification is sent according to the policy configuration.

Removed

The user is removed from the role, or the account is removed from the group. A rejection notice is sent according to the policy configuration.

Overrides

You can use recertification override tasks to update the recertification status of specific targets without re-evaluating an entire recertification policy.

The **Account Recertification Status** task allows authorized users to manually mark accounts on a service as Recertified. The task applies to owned accounts that are not already recertified. Overriding the recertification status of a suspended account changes the recertification status of the account to Recertified, but it does not restore the account. Authorization for the task is governed by the Recertification Override ACI operation on the service protection category.

To override the recertification status of accounts on a service, navigate to **Manage Services > Select a Service**. Click the icon next to the service name and select **Account Recertification Status** to get to the status page. On the status page, select the accounts to override and click the **Recertify** button. You must enter a justification before recertifying. The justification that you provide for the override is recorded in the audit record and is included in the Recertification Change History report.

The **Access Recertification Status** task allows authorized users to manually mark accesses on a service as Recertified. The task applies to accesses that are not already recertified. Authorization for the task is governed by the Recertification Override ACI operation on the service group protection category.

To override the recertification status of accesses on a service, navigate to **Manage Groups > Select a Service**. Select the service and click **OK**. Then, click the icon next to the group for the accesses and select **Access Recertification Status** to get to the status page. On the status page, select the accesses and click the **Recertify** button. You must enter a justification before recertifying. The justification that you provide for the override is recorded in the audit record and is included in the Recertification Change History report.

The **Recertify** task allows system administrators to trigger a user recertification activity for a specific user and policy.

Creating an account recertification policy

As an administrator, you can create an account recertification policy to use with one or more services or access instances. For example, you might create a recertification policy that specifies that managers must recertify their employee accounts every 60 days.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you create a recertification policy, one or more service instances must exist.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Recertification Policies**.
2. On the **Recertification Policies** page, in the **Recertification Policies** table, click **Create**.
3. On the **Manage Recertification Policies** page, on the **General** page, complete these steps:
 - a) Type a name for the recertification policy.
 - b) Optional: Type a description for the recertification policy.
 - c) Select the status of the policy, enabled or disabled.
 - d) Select the business unit to which the policy applies
 - e) Select the scope of the business unit that you selected.
 - f) Click **Next**.
4. On the **Target Type** page, select **Accounts**, and then click **Next**.
5. On the **Service Target** page, add one or more specific services to associate with the policy, and then click **Next**.
6. To add one or more services:
 - a) Click **Add**.
 - b) On the **Services** page, type your search criteria, and then click **Search**.
 - c) In the Services table, select one or more services.
 - d) Click **OK**.
7. On the **Schedule** page, select the schedule type and evaluation frequency, and then click **Next**.
8. On the **Policy** page, select either simple or advanced configuration mode, and then click **Next**. If you choose the advanced mode, use the workflow designer to configure the policy.

Note: On the **Policy** page, you can also specify the following options:

- Who approves recertification
- The action, such as suspend or delete, that occurs when a participant declines to recertify an account
- An optional recipient who receives the rejection email, which can be configured to none, such as a manager, who is notified when recertification is declined
- A value for the number of days in which the participant must respond to the recertification request

- An action, such as reject or approve, that occurs when the recertification response interval expires
- A user type to specify the scope of the recertification policy to apply only to people of a certain type on the specified policy schedule

Note: The user type option includes a performance penalty for using options other than all. If the person or business partner (bp) person type is chosen, IBM Security Identity Manager still retrieves all accounts from the LDAP server. IBM Security Identity Manager then iterates through the accounts, does an LDAP search to look up owners of the accounts, and determines if the owner is of the type person or bp person. If your user population is large, doing two searches per account can be expensive.

9. On the **Recertification E-mail** page, select an email template, and click **Next**.
10. On the **Rejection E-mail** page, select a rejection email template, and click **Finish**.
11. On the **Success** page, click **Close**.

Creating an access recertification policy

As an administrator, you can create an access recertification policy for use with one or more access instances.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Before you create a recertification policy, an access instance must exist.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Recertification Policies**.
2. On the **Recertification Policies** page, in the **Recertification Policies** table, click **Create**.
3. On the **Manage Recertification Policies** page, on the **General** page, complete these steps:
 - a) Type a name for the recertification policy.
 - b) Optional: Type a description for the recertification policy.
 - c) Select the status of the policy, enabled or disabled.
 - d) Select the business unit to which the policy applies
 - e) Select the scope of the business unit that you selected.
 - f) Click **Next**.
4. On the **Target Type** page, select **Access**, and then click **Next**.
5. On the **Access Target** page, add one or more specific accesses to associate with the policy, and then click **Next**.
6. To add one or more accesses, complete these steps:
 - a) Click **Add**.
 - b) On the **Accesses** page, type your search criteria, and then click **Search**.
 - c) In the **Accesses** table, select one or more accesses.
 - d) Click **OK**.
7. On the **Schedule** page, select the schedule type and evaluation frequency, and then click **Next**.
8. On the **Policy** page, select the configuration mode, and then click **Next**. If you choose the advanced mode, use the workflow designer to configure the policy.

Note: On the **Policy** page, you can also specify the following options:

- Who approves recertification
- The action, such as suspend or delete, that occurs when a participant declines to recertify an access
- An optional recipient who receives the rejection email, which can be configured to none), such as a manager, who is notified when recertification is declined
- A value for the number of days in which the participant must respond to the recertification request
- An action, such as reject or approve, that occurs when the recertification response interval expires
- A user type to specify the scope of the recertification policy to apply only to people of a certain type on the specified policy schedule

Note: The user type option includes a performance penalty for using options other than all. If the person or business partner (bp) type is chosen, IBM Security Identity Manager still retrieves all accounts from the LDAP server. IBM Security Identity Manager then iterates through the accounts, does an LDAP search to look up the owners of the accounts, and determines if the owner is of the type person or bp person. If your user population is large, doing two searches per account can be expensive.

9. On the **Recertification E-mail** page, select an e-mail template, and then click **Next**.
10. On the **Rejection E-mail** page, select a rejection e-mail template, and then click **Finish**.
11. On the **Success** page, click **Close**.

Creating a user recertification policy

As an administrator, you can create a user recertification policy to recertify the accounts, group membership of accounts, and memberships of users.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Recertification Policies**.
2. On the **Recertification Policies** page, in the **Recertification Policies** table, click **Create**.
3. On the **Manage Recertification Policies** page, on the **General** page, complete these steps:
 - a) Type a name for the recertification policy.
 - b) Optional: Type a description for the recertification policy.
 - c) Select the status of the policy, enabled or disabled.
 - d) Select the business unit to which the policy applies.
 - e) Select the scope of the business unit that you selected.
 - f) Click **Next**.
4. On the **Target Type** page, select **Users**, and then click **Next**.
5. On the **User Target** page, select the user type, and then click **Next**.
6. On the **Resource Target** page, complete these steps:
 - a) Select which roles you want the policy to recertify membership on.
 - b) Select which accounts you want the policy to recertify.
 - c) Select which groups you want the policy to recertify.
 - d) Click **Next**.
7. Optional: If you selected **Specified roles** on the **Resource Target** page, on the **Role Target** page, select one or more roles for which you want to recertify membership.

8. Optional: If you selected **Accounts on specified services** on the **Resource Target page**, on the **Account Target** page, select one or more services for which accounts on the service are recertified.
9. Optional: If you selected **Specified groups** on the **Resource Target** page, on the **Group Target** page, select one or more groups you want the policy to recertify.
10. On the **Schedule** page, select the schedule type and evaluation frequency, and then click **Next**.
11. On the **Policy** page, select the configuration mode, and then click **Next**. If you choose the advanced mode, use the workflow designer to configure the policy.

Note: On the **Policy** page, you can also specify the following options:

- Who approves recertification.
 - An action, such as Suspend accounts and mark others, that occurs when the recertification is rejected.
 - An optional recipient who receives the rejection email (which can be configured to None) such as a manager, who is notified when recertification is declined.
 - A value for the number of days in which the participant must respond to the request until the recertification is due.
 - An action, such as Reject All or Approve All, that occurs when the recertification is overdue. If you do not select an action, the recertification activity remains in the activity list of the participant after the due date until it is completed.
12. On the **Recertification E-mail** page, select an email template, and then click **Next**.
 13. On the **Rejection E-mail** page, select a rejection email template, and then click **Finish**.
 14. On the **Success** page, click **Close**.

Changing a recertification policy

As an administrator, you can change a recertification policy. For example, you can modify the recertification interval, add or remove users, services, or access instances. Alternatively, you can modify the template that provides a message when recertification is declined.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

If you modify a recertification policy, ensure that you consider the consequences of the changes. For example, when the schedule for recertification is modified, the changes might require users, accounts, or accesses that were recently recertified to be recertified again immediately. When setting the default timeout action, ensure that you properly set up the participant of recertification. An escalation participant is not specified in the default simple workflow.

Suppose that a recertification policy exists for LDAP accounts and the notifications for recertification are sent to all account owners. If the target for the recertification policy is changed from LDAP service to Win local service, the LDAP accounts still must be recertified by the LDAP account owners. Because the to-do activities for LDAP recertification are already created, the timeout action and the action upon rejection are applicable as specified in the LDAP recertification policy before updating. To-do items that are already in process are not deleted automatically, and progress to their natural ending.

You can use policy modification to *disable* a policy. If you disable a policy, the policy does not generate any additional recertification to-do items until it is re-enabled. However, any running recertifications are not stopped, and they complete as normal.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Recertification Policies**.

2. On the **Recertification Policies** page, type information about the recertification policy or service in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and then click **Search**.
3. In the **Recertification Policies** table, locate and select a recertification policy that you want to change, and then click **Change**.
4. On the **Manage Recertification Policies** page, modify the information on the available pages.
5. Click **OK** to save the changes.
6. On the **Success** page, click **Close**.

Deleting a recertification policy

As an administrator, you can delete a recertification policy that is no longer needed to manage user, account, or access recertification.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

If you delete the recertification policy, any users, accounts, or accesses that were targeted by that policy are no longer governed by any recertification policy.

Suppose that a recertification policy exists for LDAP accounts and the notifications for recertification are sent to all account owners. If the policy is deleted, the LDAP accounts still must be recertified by LDAP account owners. Because the to-do activities for LDAP recertification are already created, the timeout action and action upon rejection are applicable as specified in the LDAP recertification policy before deletion.

However, any running recertifications are not stopped, and they complete as normal.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Recertification Policies**.
2. On the **Recertification Policies** page, type information about the recertification policy or service in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and then click **Search**.
3. In the **Recertification Policies** table, locate and select a recertification policy that you want to delete and click **Delete**.
4. On the **Confirmation** page, review the recertification policy that you want to delete and click **Delete**.
5. On the **Success** page, click **Close**.

Recertification default notifications

IBM Security Identity Manager provides default templates for user, account, and access recertification notifications.

Default recertification templates

The default templates exist in LDAP and cannot be modified. An administrator can view the default templates in the recertification policy interface and copy them there.

The following labels are the default template names for the account and access recertification policy recertification email:

- Delete Account
- Mark Access

- Mark Account
- Remove Access
- Suspend Account

The following labels are the default template names for the account and access recertification policy rejection email:

- Access Marked
- Access Removed
- Account Deleted
- Account Marked
- Account Suspended

The following labels are the default template names for the user recertification policy recertification e-mail:

- User Recertification Pending

The following labels are the default template names for the user recertification policy rejection e-mail:

- User Recertification Rejected

Properties file values

To change templates, you can use all the key=value statements in the `CustomLabels.properties` file, or create your own properties and values.

These properties are referenced by the default templates. The properties can be modified if you want to reword some of the templates while keeping the same parameter substitutions. You can either modify these defaults, or make up your own keys and reference them from the templates.

The properties include the following items on one line:

```

recertOn={0} on {1}
recertTemplateSubject=Recertification required
  for account {0} on service {1}
recertTemplateAccessSubject=Recertification required
  for account {0} on access {1}
recertTemplateBody=You have received a recertification request
  for account {0} on service {1} owned by {2}.
recertTemplateAccessBody=You have received a recertification request
  for account {0} on access {1} owned by {2}.
recertDeclineSuspendBody=Rejection of this recertification request
  will result in the suspension of account {0} on {1}.
recertDeclineDeletesBody=Rejection of this recertification request
  will result in the deletion of account {0} on {1}.
recertDeclineMarksBody=Rejection of this recertification request
  will result in account {0} on {1} being marked as rejected for
  recertification.
recertDeclineDeletesAccessBody=Rejection of this recertification
  request will result in the deletion of access {0}.
recertDeclineMarksAccessBody=Rejection of this recertification request
  will result in access {0} being marked as rejected for recertification.
recertDeclinedAcctSuspendedSubj=Account {0} on service {1} has been
  suspended due to rejection of a recertification request
recertDeclinedAcctDeletedSubj=Account {0} on service {1} has been
  deleted due to rejection of a recertification request
recertDeclinedAcctMarkedSubj=Account {0} on service {1} has been
  marked as rejected for recertification due to rejection
  of a recertification request
recertDeclinedAccessDeletedSubj=Account {0} on access {1} has been
  deleted due to rejection of a recertification request
recertDeclinedAccessMarkedSubj=Account {0} on access {1} has been
  marked as rejected for recertification due to rejection of a
  recertification request
recertDeclinedAcctSuspendedBody=The account {0} on service {1} owned
  by {2} has been suspended due to rejection of a recertification request.
recertDeclinedAcctDeletedBody=The account {0} on service {1} owned
  by {2} has been deleted due to rejection of a recertification request.
recertDeclinedAcctMarkedBody=The account {0} on service {1} owned
  by {2} has been marked as rejected for recertification due to

```

```

rejection of a recertification request.
recertDeclinedAccessDeletedBody=The account {0} on access {1} owned
by {2} has been deleted due to rejection of a recertification request.
recertDeclinedAccessMarkedBody=The account {0} on access {1} owned
by {2} has been marked as rejected for recertification due to
rejection of a recertification request.
userRecertTemplateSubject=Recertification required for user {0}
userRecertTemplateBody=You have received a recertification request
for user {0}. The recertification includes their membership in {1} role(s)
and ownership of {2} account(s). Please indicate whether the user still
requires these resources.
userRecertDeclinedSubj=Recertification request rejected for user {0}
userRecertDeclinedBody=One or more resources for user {0} have been
rejected during recertification.
userRecertRolesRejectedLabel=The following roles were rejected:
userRecertAccountsRejectedLabel=The following accounts were rejected,
along with all groups associated with the accounts:
userRecertGroupsRejectedLabel=The following groups were rejected,
but the account was accepted:
userRecertAcctLabel=Account "{0}" on service "{1}"
userRecertGroupLabel=Group "{0}" for account "{1}" on service "{2}"

```

Separation of duty policies

A *separation of duty policy* is a logical container of separation rules that define mutually exclusive relationships among roles. Policies for separation of duty are defined by one or more business rules. The rules exclude users from membership in multiple roles that might present a business conflict.

A separation of duty policy uses business rules to define the relationships among roles. The separation of duty policy groups the business rules for ease of administration. For example, you can assign a set of administrators to a policy, making the administrators responsible for tracking the violations of a set of rules.

Policy owners

You can specify one or more owners for the policy. Owners can be any combination of users and roles. You can configure policy owners to participate in policy and role change workflows. For example, a policy owner can approve or reject separation of duty violation activities that occur when roles are added to a Security Identity Manager user. Separation of duty policy owners can also:

- Exempt users or revoke exemptions from any policy violations that occur
- Be used as principals in system access control items (ACIs)

Exemption approval and revocation

Policy owners can approve and revoke exemptions by default, but they do not necessarily require this ability. You can configure roles or users to have access control capabilities over separation of duty policies through ACIs. The ACIs allow policy owners to do tasks such as editing or tracking violations. You can also configure the approval workflow to use participants other than the policy owner.

Separation of duty rules

A separation of duty policy can include multiple rules. For each rule, two or more roles must be listed. The number of roles to which a user can belong depends on how many roles you allow in the rule. The number of roles that you allow to coexist must be one fewer than the total number of roles in the list. For example, you might create a rule that excludes procurement and order approval. The allowed number of roles in the rule must be one, meaning that a user can have only one role. If you add more roles, such as invoicing and financing, you can allow up to three roles. Each user can have three different roles and the system capabilities defined by that role.

Allowed roles set to greater than one are typically used to prevent one person from having complete control over a process. The process is described by a set of roles. For example, a rule named "A user cannot have full control over the procurement process" might be defined by three roles named purchaser, approver, and orderer. In this example, the rule has two allowed roles. A user can be a member of two of these roles, but the user cannot be a member of all three roles.

Enabled and disabled policies

An *enabled policy* creates exemption approvals and warns users before they submit a role membership change that breaks a separation of duty rule.

A *disabled policy* can still track violations, but it does not generate approvals or warn users. Violations from disabled policies are not displayed in audit reports. Using a disabled policy is a good way for a security administrator to track violations that occur before a policy is active in the system.

Role hierarchy and rules

Two roles in a rule cannot be direct ascendants or descendants of each other in the role hierarchy. For example, you cannot have a rule with both HR organization and HR department x if HR department x is a child role of HR organization.

ACI operations for the separation of duty policy protection category

You can configure role owners to have access control capabilities over separation of duty policies through access control items (ACIs). The ACIs allow role owners to do tasks such as editing or tracking violations. ACIs must apply to the business unit in which the policy is defined. Creators of separation of duty ACIs can define ACI filter rules to scope the policies to which an ACI applies.

Add

Protects separation of duty policy creation. The add operation fails if this ACI is not met.

Exemption Administration

Protects separation of duty policy violation and exemption management through the **Violations and Exemptions Summary** page. The ability to exempt a violation or revoke an exemption is governed by this operation. The **Approve** and **Revoke** buttons are not displayed if this ACI is not met. The operations of exempt and revoke also apply to the public API.

Modify

Protects separation of duty policy modifications. The modify operation fails if this ACI is not met. When change is denied and search is allowed, the user has a read-only view of the policy.

Reconcile

Protects separation of duty policy reconciliation. Separation of duty policy reconciliation is the operation that analyzes the policy separations and creates violations or cleans up violations or exemptions. Clicking the **Evaluate** button causes a "not authorized" message to be displayed if this ACI is not met.

Remove

Protects separation of duty policy deletions. Clicking the **Delete** button causes a "not authorized" message to be displayed if this ACI is not met.

Search

Protects separation of duty policy searches. With the search operation granted, the user can see details about violations and exemptions. If a user is authorized for search but not modify, the user can open the policy in a read-only mode and view violations and exemptions. However, the user cannot act on those violations and exemptions or change the policy.

Default ACIs for the separation of duty policy

See descriptions of the default access control items (ACIs) for separation of duty capabilities.

Grant Search to Auditor Group

Allows the auditor group to view the policies, rules, violations, and exemptions.

Grant All to Owner

Grants all operations to the owner of a separation of duty policy in the organization. You might allow a user who is not a system administrator to create a separation of duty policy. You must create an ACI that grants the **add** permission to that user.

Separation of duty approval workflow operation

After you create the policy, an approval workflow operation named *approveSoDViolation* for each violation is started during person operations. These operations might be role membership changes that cause separation of duty policy violations.

There is one separation of duty approval workflow that is called for all separation of duty violations. However, you can customize the workflow for individual policies to have multilevel approval, but the customizations must be done from within that one workflow.

To locate the *approveSoDViolation* approval operation, click **Configure System > Manage Operations**, and then select **Global level**. The approval operation is called for each violation that is found during the person operation (role membership change). You can modify this operation to include custom approval paths. For example, you can specify that both the policy owner and the user's manager approve the violation. By default, the policy owner is the approval participant. This image illustrates the *approveSoDViolation* approval operation.

Figure 2. *approveSoDViolation* approval operation

After the approval participant approves the operation, the person operation is allowed to occur (implying approved) or fail (implying the approval was rejected). During the approval path, a violation exemption is recorded, noting who approved the exemption. The violation and exemption statistics are updated. You can view the exemption by clicking **Manage Policies > Manage Separation of Duty Policies**, and then clicking a number in the **Exemptions** column of the **Separation of Duty Policies** table.

When you request a change, such as adding a role to a user, a warning might be displayed. The warning indicates that the change can cause a separation of duty violation. The warning lists the policy and rule in violation. You can continue to submit the request or cancel the request. The warning is displayed in both the administrative console and the Self Service or the Identity Service Center interface for the following requests:

- Modifying or creating a person
- Requesting an access
- Modifying static role membership
- Changing the role hierarchy

If you try to change role hierarchy in such a way that an existing separation of duty policy would become invalid, an error is displayed. The change does not occur. The error lists the policy and rule that would be in violation if the role hierarchy was modified as requested.

The audits of the exemption process occur automatically, depending on the result of the workflow. You do not need to manually call audit methods to have the audits recorded for use in the administrative console or reports.

However, you must set the process result with AA and process result detail with the string value that you want to audit as the justification for the exemption approval if the intent is to allow the violation to exist in the system. By default, the approval operation in the *approveSoDViolation* workflow has this PostScript code:

```
WorkflowRuntimeContext.setProcessResult(WorkflowRuntimeContext.getActivityResult());  
WorkflowRuntimeContext.setProcessResultDetail(WorkflowRuntimeContext.getActivityResultDetail());
```

The first line in the PostScript code sets the process result to the same value as the result of the approval. AA indicates approved and AR indicates rejected. The second line sets the process result detail to the comments that were typed by the user when the approval to do activity was approved.

You can use normal workflow customizations to get the values you want, but be sure to call `WorkflowRuntimeContext.setProcessResult()` and

`WorkflowRuntimeContext.setProcessResultDetail()` with some value if you want the system to treat the approval as an approved separation of duty exemption.

There might be multiple approvals in the workflow for separation of duty. The approver that is listed in the exemption record is the last person to approve an approval request in the workflow.

Separation of duty policy violations and exemptions

A *violation* is a specific violation of a separation of duty policy, and an *exemption* is an approved separation of duty violation. *Policy evaluation* is a way to discover violations.

Policy violations

A *violation* is a specific violation of a separation of duty policy, which means that the roles for a user have a conflict that is based on a defined separation of duty rule.

Violations are created when the following events occur:

- A user requests membership in a role that would violate one or more separation of duty policy rules.
- A user creates a separation of duty policy or rule.
- User records are fed into Security Identity Manager through an identity feed if they create a rule violation.
- Any other request to modify role membership if it creates a rule violation.
- When there are existing conflicts when a policy is introduced.
- A security administrator revokes an exemption.

When a policy is created or changed, the violations do not update automatically. You must either perform an evaluation on the policy or wait for a scheduled data synchronization.

Policy exemptions

An *exemption* is an approved separation of duty violation, which means that the conflict cannot be flagged as a violation in an audit, and additional updates to the user's role list do not require reapproval. Exemptions occur when a security administrator approves a request that violates a defined and active separation of duty policy. A security administrator can also convert existing violations into exemptions.

Exemptions are created for a specific policy rule, not for an entire policy. If a policy contains multiple rules and the user is approved for the violation of one rule, that user is not automatically allowed to violate the other rules in the policy.

Exemptions remain stored in the database when a policy is disabled. Therefore, if a policy is disabled and then re-enabled at a later date, the exemptions are remembered.

You can exempt a user from violating separation of duty policy rules manually or through an approval process.

When a rule violation event occurs and a policy and role change workflow activity have been defined, an approval activity is created for workflow participants (such as policy owners) to exempt the user from a specified separation of duty policy rule. Only a role membership change request for the user triggers an approval activity.

An approval activity is generated for each rule violation. If the approval is rejected, any modifications to the user that were made at the time of the role membership change are lost. If an exemption approval request is triggered as part of a person being created, that person is not created if the approval is rejected.

Policy evaluation

Policy evaluation is a way to discover violations, and can occur in any of these situations:

- Use the **Evaluate** button. This button causes the policy to be evaluated against all people who currently have roles in the policy.

- Perform a data synchronization. Rule violations are recorded for each policy, and the number of violations is displayed in the separation of duty policy table. You can then exempt any rule violations manually by clicking the link provided in the table and viewing or modifying any rule violations and exemptions.
- When you create any HR feed service, you can specify whether to evaluate the separation of duty policy. If you choose to evaluate the separation of duty policy, you must also enable workflow. If this option is enabled, an approval activity is generated for each separation of duty rule violation that is found in the incoming HR feed data. That approval process must be marked as approved to get the updates into Security Identity Manager. If the approval processes are rejected, the entire entry or change that was in that HR feed record is ignored and is not stored in Security Identity Manager.

Enabling the Manage Separation of Duty Policies portfolio task

System administrators have access to the Manage Separation of Duty Policies portfolio task. Other users must be assigned to a group that has access to the task.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To have the **Manage Separation of Duty Policies** portfolio task be displayed in the administrative console, you must enable the task in one of the default views or in a view that you created.

To enable the **Manage Separation of Duty Policies** portfolio task, complete these steps:

Procedure

1. From the navigation tree, select **Set System Security > Manage Views**.
The **Define Views** page is displayed.
2. On the **Define Views** page, complete these steps:
 - a) In the **Name** field, type information about the view and click **Search**.
The **Manage Views Results** table is displayed.
 - b) In the **Manage Views Results** table, select the check box next to a view and click **Change**.
 - c) Optional: In **General** tab, change the name or description of the view.
 - d) In the **Configure View** tab, in the tree of tasks, expand **Manage Policies**, and then select **Manage Separation of Duty Policies** task.
Both **Manage Policies** and **Manage Separation of Duty Policies** are selected.
 - e) Click **OK** to save the changes.

Results

A **Success** page is displayed, indicating that you successfully updated the views on the system.

What to do next

You can continue working with views, or click **Close**.

Creating separation of duty policies

An administrator can create a separation of duty policy to use for auditing purposes. For example, you might create a separation of duty policy to report users that belong to multiple roles that are mutually exclusive.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.


To create a valid policy rule, you must have two or more roles defined in the system for the business unit you select.

About this task

To create a separation of duty policy, complete these steps:

Procedure

1. From the navigation tree, select **Manage Policies > Manage Separation of Duty Policies**.
The **Manage Separation of Duty Policies** page is displayed.
2. On the **Manage Separation of Duty Policies** page, in the **Separation of Duty Policies** table, click **Create**.
The **Create a Separation of Duty Policy** page is displayed.
3. On the **Create a Separation of Duty Policy** page, complete these steps:
 - a) Type a name for the policy.
 - b) Provide a description for the policy.
 - c) Select the business unit to which this policy applies. Click **Search** to search for a business unit. The **Business Unit** page is displayed.
4. On the **Business Unit** page, complete these steps:
 - a) Type your search criteria, and then click **Search**.
 - b) In the **Business Units Found** table, select a business unit and click **OK**.
The **Create a Separation of Duty Policy** page is displayed.
5. On the **Create a Separation of Duty Policy** page, in the **Policy Rules** table, click **Create**. The **Create Policy Rule** page is displayed.
6. On the **Create Policy Rule** page, complete these steps:
 - a) In the **Description of separation** field, type a description for the policy rule. For example, you might describe a rule that you add to a policy as *People in the IT department may not be given accounting responsibilities*.
 - b) Type each role name that you want to add to the role separation list and click **Add**.
If you type the exact name of an existing role in the **Role name** field and click **Add**, the role is immediately added to the list. If you type a value in the **Role name** field that does not exactly match a role or matches more than one role, a search panel opens. Select the appropriate roles.
Note: You can search only for the roles for which you have permission.
 - c) In the **Allowed number of roles** list, select the number of roles to which a user can belong.
For each policy rule that you create, two or more roles must be listed. The number of roles to which a user can belong depends on how many roles you allow in the policy rule. The number of roles that you allow can be, at a maximum, one fewer than the total number of roles in the list.
 - d) Click **OK**.
The **Create a Separation of Duty Policy** is displayed.
7. On the **Create a Separation of Duty Policy** page, complete these steps:

- a) Create more policy rules as necessary.
- b) Click the  icon next to **Policy Owners**.
The **Role Policy Owners** table and the **User Policy Owners** table are displayed.
- c) In the **Role Policy Owners** table, click **Add** to search for and select roles to have ownership of the policy.
- d) In the **User Policy Owners** table, click **Add** to search for and select users to have ownership of the policy.
- e) In the **Policy state** field, select whether to enable or disable the policy.
An enabled policy creates exemption approvals and warns users before they submit a role membership change that breaks a separation of duty rule. A disabled policy can still track violations, but it does not generate approvals or warn users. Violations from disabled policies are not displayed in audit reports. Using a disabled policy is a good way for a security administrator to track violations that occur before a policy is active in the system.
- f) Click **Submit** to save the policy.

Results

A **Success** page is displayed, indicating that you successfully submitted a request for a new separation of duty policy.

What to do next

You can view your request, continue working with policies, or click **Close**.

Modifying separation of duty policies

An administrator can modify a separation of duty policy. For example, you can add or remove policy owners. You can also add or remove separation rules, change role attributes for a specific rule, and enable or disable the policy.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

You can use policy modification to disable or enable a policy. If you disable a policy, the policy does not generate any additional to-do items until you re-enable it.

You cannot change the business unit to which the policy applies.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Separation of Duty Policies**.

The **Manage Separation of Duty Policies** page is displayed.

2. On the **Manage Separation of Duty Policies** page, complete these steps:

- a) Type information about the policy in the **Search information** field.
- b) In the **Search by** field, specify whether to do the search against policy names or descriptions, business units, or role names, and then click **Search**.

A list of policies that match the search criteria is displayed.


If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

- c) In the **Separation of Duty Policies** table, select the check box next to the policy that you want to modify, and then click **Change**. Selecting the check box at the top of this column selects all policies.

The **Change Separation of Duty Policy** page is displayed.

3. On the **Change a Separation of Duty Policy** page, complete these steps:

- a) Provide any necessary updates to the policy name and description.
- b) In the **Policy Rules** table, create, delete, or modify any rules that apply to the policy.
- c) Click the  icon next to **Policy Owners**.

The **Role Policy Owners** table and the **User Policy Owners** table are displayed.

- d) Optional: In the **Role Policy Owners** table, click **Add** to search for and select roles to have ownership of the policy.
- e) Optional: In the **User Policy Owners** table, click **Add** to search for and select users to have ownership of the policy.
- f) Select whether to enable or disable the policy.
- g) Click **Submit** to save the policy.

Results

A **Success** page is displayed, indicating that you submitted a request to change a separation of duty policy.

What to do next

You can continue working with separation of duty policies, view your request, or click **Close**.

Evaluating separation of duty policies

An administrator can evaluate a separation of duty policy without doing a data synchronization. By running the evaluation, you can view current policy violation and exemption information. The evaluation process searches for violations to the policies that you specify.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Violations are kept current as user role membership is modified. There are some cases where a change in the system might require a re-evaluation of separation of duty policy violations for one or more specific policies. These situations include:

- Creating or changing a separation of duty policy
- Changing a role hierarchy
- Running an identity feed with evaluations disabled

In these cases, run a separation of duty policy violation evaluation on one or more policies. You can do the evaluation in one of these ways:

- By running a full report data synchronization, which finds violations for all policies
- By running evaluations on individual policies

When you disable a policy and then do another evaluation on the disabled policy, new violation warnings or exemption approval to-do activities are generated.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Separation of Duty Policies**.
The **Manage Separation of Duty Policies** page is displayed.
2. On the **Manage Separation of Duty Policies** page, complete these steps:
 - a) Type information about the policy in the **Search information** field.
 - b) In the **Search by** field, specify whether to do the search against policy names or descriptions, business units, or role names, and then click **Search**.
A list of policies that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Separation of Duty Policies** table, select the check box next to the policy that you want to evaluate, and then click **Evaluate**. Selecting the check box at the top of this column selects all policies.
A confirmation page is displayed.
 - d) On the **Confirm** page, click **Evaluate** to run the evaluation, or click **Cancel**.

Results

A **Success** page is displayed, indicating that you successfully submitted a request to do an evaluation on a separation of duty policy.

After the evaluation is complete, the violation count for the policy is updated.

What to do next

You can continue working with separation of duty policies, view your request, or click **Close**.

Deleting separation of duty policies

As an administrator, you can delete a separation of duty policy that is no longer needed to manage exclusive relationships between roles.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

If you delete the separation of duty policy, any roles that were targeted by that policy are no longer governed by the separation of duty policy.

When you delete a policy, all violations and exemptions for that policy are retained and marked with a statement that the policy is deleted.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Separation of Duty Policies**.
The **Manage Separation of Duty Policies** page is displayed.
2. On the **Manage Separation of Duty Policies** page, complete these steps:
 - a) Type information about the policy in the **Search information** field.
 - b) In the **Search by** field, specify whether to do the search against policy names or descriptions, business units, or role names, and then click **Search**.

A list of policies that match the search criteria is displayed.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
- c) In the **Separation of Duty Policies** table, select the check box next to the policy that you want to delete, and then click **Delete**. Selecting the check box at the top of this column selects all policies. A confirmation page is displayed.
3. On the **Confirm** page, click **Delete**, or click **Cancel**.

Results

A message is displayed, indicating that you successfully submitted the policy for deletion.

What to do next

Continue working with policies, view your request to confirm that the policy is deleted, or click **Close**.


Viewing policy violations and exemptions

An administrator or policy owner can view a summary of the separation of duty policy violations and exemptions for each rule in the policy. The administrator or policy owner can also do administrative operations, such as approve or revoke, on the violations and exemptions.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Separation of Duty Policies**.
The **Manage Separation of Duty Policies** page is displayed.
2. On the **Manage Separation of Duty Policies** page, complete these steps:
 - a) Type information about the policy in the **Search information** field.
 - b) In the **Search by** field, specify whether to do the search against policy names or descriptions, business units, or role names, and then click **Search**.
A list of policies that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Separation of Duty Policies** table, click the link provided in the **Violations** or **Exemptions** column of the policy that you want to view.
The link is displayed only if there are one or more violations or exemptions for the separation of duty policy.
The **Violations and Exemptions Summary** page is displayed.
3. On the **Violations and Exemptions Summary** page, complete these steps:
 - a) Select the order in which you want to sort the rules, and then click **Sort**.
You can sort alphabetically by rule name, or sort by the number of violations or exemptions.
 - b) Click the icon () next to each rule that you want to view, or click the rule name.

Results

Two tables that provide information about violations and exemptions are displayed.

What to do next

You can approve violations or revoke exemptions.

When you are done viewing violations and exemptions, click **Close**.

Approving policy violations

An administrator or policy owner can approve separation of duty policy violations for each rule in the policy.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.


About this task

When you approve a violation, an exemption is created for the specified user and the combination of roles that caused the violation. After you approve a policy violation, that violation is removed from the violation list, and a new exemption is displayed in the exemption list.

Having an exemption means that the user is allowed to be a member of the violating roles. Updates to the user's person record do not cause additional violations or warnings unless the user introduces a new violation that is not covered by the exemption.

Updates to the record of a person do not trigger an approval unless the roles of the person are updated and the combination violates a separation of duty policy, assuming that an exemption does not exist for the policy.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Separation of Duty Policies**.
The **Manage Separation of Duty Policies** page is displayed.
2. On the **Manage Separation of Duty Policies** page, complete these steps:
 - a) Type information about the policy in the **Search information** field.
 - b) In the **Search by** field, specify whether to do the search against policy names or descriptions, business units, or role names, and then click **Search**.
A list of policies that match the search criteria is displayed.
If the table contains multiple pages, you can:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Separation of Duty Policies** table, click the link provided in the **Violations** column of the policy that you want to view.
The link is displayed only if there are one or more violations for the separation of duty policy.
The **Violations and Exemptions Summary** page is displayed.
3. On the **Violations and Exemptions Summary** page, complete these steps:
 - a) Select the order in which you want to sort the rules, and then click **Sort**.
You can sort alphabetically by rule name, or sort by the number of violations or exemptions.
 - b) Click the icon () next to each rule that you want to view.

The **Violations** table is displayed, providing information about violations for the rule that you specified.

- c) In the **Violations** table, select the check box next to one or more violations that you want to approve, and then click **Approve**. Selecting the check box at the top of this column selects all violations.

The **Approve Violations** page is displayed.

4. On the **Approve Violations** page, complete these steps:

- a) In the **Violation Summary**, ensure that the policies and rules are correct.
- b) In the **Notes** field, type a reason for approving the violation, and then click **Approve**.

Results

A **Success** page is displayed, indicating that you successfully approved the violations for the specified policy and rule.

What to do next

You can approve additional violations or revoke exemptions.

When you are done viewing violations and exemptions, click **Close**.

Revoking policy exemptions

An administrator or policy owner can revoke separation of duty policy exemptions for each rule in the policy.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

When you revoke an exemption, that exemption is removed from the exemption list. The user to which the exemption applies might continue to have roles that are in violation of a separation of duty policy rule. In that case, the violation is displayed again the list of violations for that policy.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Separation of Duty Policies**.

The **Manage Separation of Duty Policies** page is displayed.

2. On the **Manage Separation of Duty Policies** page, complete these steps:

- a) Type information about the policy in the **Search information** field.
- b) In the **Search by** field, specify whether to do the search against policy names or descriptions, business units, or role names, and then click **Search**.

A list of policies that match the search criteria is displayed.

If the table contains multiple pages, you can:


- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

- c) In the **Separation of Duty Policies** table, click the link provided in the **Exemptions** column of the policy that you want to view.

The link is displayed only if there are one or more exemptions for the separation of duty policy.

The **Violations and Exemptions Summary** page is displayed.

3. On the **Violations and Exemptions Summary** page, complete these steps:

- a) Select the order in which you want to sort the rules, and then click **Sort**.
You can sort alphabetically by rule name, or sort by the number of violations or exemptions.
 - b) Click the icon () next to each rule that you want to view.
The **Exemptions** table is displayed, providing information about exemptions for the rule that you specified.
 - c) In the **Exemptions** table, select the check box next to one or more exemptions that you want to revoke, and then click **Revoke**. Selecting the check box at the top of this column selects all exemptions.
The **Revoke Exemptions** page is displayed.
4. On the **Revoke Exemptions** page, complete these steps:
 - a) In the **Exemption Summary**, ensure that the policies and rules are correct.
 - b) In the **Notes** field, type a reason for revoking the exemption, and then click **Revoke**.
The **Notes** field is for auditing purposes and is not displayed in the administrative console after an exemption is revoked.

Results

A **Success** page is displayed, indicating that you successfully revoked the exemptions for the specified policy and rule.

What to do next

You can revoke additional exemptions or approve violations.

You can use a custom audit data report to provide justification for revoking exemptions.

When you are done viewing violations and exemptions, click **Close**.

Service selection policies

A *service selection policy* extends provisioning policies by enabling selection of a service based on person attributes. To be enforced, a service selection policy must be the target of a provisioning policy. The service selection policy then identifies the service type to target and defines the service based on JavaScript.

The service selection policy can be in the same container as the provisioning policy or in a container located above the container of the provisioning policy. The scope of a service selection policy determines which provisioning policies can target it. Service selection policies with single scope can be targeted only by provisioning policies at the same level in the organization tree as the service selection policy. Service selection policies with subtree scope can be targeted by provisioning policies at the same level or below the service selection policy.

Service selection policies are evaluated in the following circumstances:

- When a user is added to an organizational role that is a member of a provisioning policy that targets the service selection policy
- When a user's attributes are modified
- When the policy itself is modified

Evaluating the policy might require moving a user's account to a different service instance than the one the user is currently using. A new account for the user is created on the new service instance. One of the following actions completes, depending on the policy enforcement setting of the service instance:

- Suspends the existing user account on the old service instance.

Note: The account is deleted, suspended, or marked as disallowed only if the service selection policy does not allow the account on that service. An account on the new service is not created.

- Deletes the existing user account on the old service instance.

- Sends a work item to alert the recipient to delete the existing user account on the old service instance.
- Marks the account on the old service instance as disallowed.

Creating a service selection policy

An administrator can create a service selection policy.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

A service selection policy is not used by the IBM Security Identity Manager Server until a provisioning policy targets it. If you enable a service selection policy after you enable a provisioning policy, the Security Identity Manager Server does a policy check and uses the policy to provision new and existing accounts.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Service Selection Policies**.
2. On the **Work With Service Selection Policies** page, in the **Service Selection Policies** table, click **Create**.
3. On the **Manage Service Selection Policies** page, on the **General** page, type a name and select a business unit for your service selection policy.
4. Click the **Service Type** tab, and select the type of service you want to associate with the service selection policy.
5. On the **Manage Service Selection Policies** page, on the **Service Selection Script** page, type a selection script.

Important: The Security Identity Manager Server does not verify that the JavaScript is correctly coded. Verify that the JavaScript is correctly coded before using it to define the service selection policy.

6. Click **Submit Now** to save the policy.
7. On the **Success** page, click **Close**.

Changing a service selection policy

An administrator can change a service selection policy. Service selection policies are not usually modified after being created.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Modifying an existing, enabled service selection policy can cause deprovisioning of user accounts. Modifying the scope or status of a service selection policy can affect user access as soon as the policy changes take effect.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Service Selection Policies**.

2. On the **Work With Service Selection Policies** page, type information about the service selection policy or business unit in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and click **Search**.
3. In the **Service Selection Policies** table, locate and select a service selection policy, and then click **Change**.
4. On the **Manage Service Selection Policies** page, modify the information on the **General**, **Service Type**, and **Service Selection Script** pages.
Important: The IBM Security Identity Manager Server does not verify that the JavaScript is correct. Verify that the JavaScript is correctly coded before using it to define the service selection policy.
5. Click **Submit Now** to save the changes.
6. On the **Success** page, click **Close**.

Deleting a service selection policy

An administrator can delete a service selection policy, which can be removed when no provisioning policy references it.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the navigation tree, select **Manage Policies > Manage Service Selection Policies**.
2. On the **Work With Service Selection Policies** page, type information about the service selection policy or business unit in the **Search information** field, or type an asterisk (*). Select a filter in the **Search by** field, and click **Search**.
3. In the **Service Selection Policies** table, locate and select a service selection policy, and then click **Delete**.
4. On the **Confirm** page, review the service selection policy to delete, choose a date and time for the deletion to occur, and then click **Delete**.
5. On the **Success** page, click **Close**.

Chapter 13. Workflow management

Workflows for entitlements to an account or access can be added, deleted, and modified from the workflow design page. Additionally, you can change workflow properties, escalation, notification, and other workflow activities.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Adding an entitlement workflow

As an administrator, you can create a workflow for either an account request or an access request.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you begin, determine whether additional access control items are needed for the new workflow.

About this task

You can use the **Workflow Designer** page to add a workflow to either an account request or an access request.

Procedure

1. From the navigation tree, select **Design Workflows**. Then, click either **Manage Account Request Workflows** or click **Manage Access Request Workflows**.
2. In the page that is displayed, in the table that lists the workflows, click **Create**.
3. In the **General** tab, complete the name and description of the workflow, and select a business unit and service type. Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.
4. In the **Activities** tab, complete either a simple or an advanced workflow:

You can create a simple workflow and convert it to an advanced one if you later decide that you require more advanced capabilities. However, you cannot convert an advanced workflow to a simple one. If you do so, all of your advanced activities are discarded and you start with a new, simple workflow.

Option	Description
Simple	Click to add a workflow that consists of a linear series of approval, mail, or request for information activities. Complete the activity name, participant type, and escalation time and escalation participant type. Then, click OK .
Advanced	Click to add an advanced workflow potentially consisting of other types of activities, loops, and conditional branches. The workflow designer applet starts. Using the workflow designer, specify the workflow. Click other tabs to specify additional information. Then, either click OK to save the changes or Apply to save your changes and continue.

5. On the **Success** page, click **Close**.

What to do next

You might associate this workflow with an access or account entitlement.

Changing an entitlement workflow

As an administrator, you can change a workflow for either an account request or an access request.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Before you begin, determine whether changes are also needed to access control items that apply to the workflow.

You can use the **Workflow Designer** page to change a workflow for either an account request or an access request.

Procedure

1. From the navigation tree, select **Design Workflows**. Then, click either **Manage Account Request Workflows** or click **Manage Access Request Workflows**.
2. In the page that is displayed, in the **Search information** field, type information about the workflow, and click **Search**.

You can also type information about the service to which the account request workflow is associated, or information about the access to which the access request workflow is associated.

Note: A search done by **Access** type returns only workflows that have an existing association with the access definition. To see all workflows, select **Workflow** as the search type.

3. In the table that lists the available workflows, select the workflow that you want to modify, and click **Change**.
4. In the **General** tab or the **Activities** tab, complete your changes. Then, click **OK**.
5. On the **Success** page, click **Close**.

What to do next

You might make additional changes to an access control item, or associate this workflow with a different provisioning policy.

Deleting an entitlement workflow

As an administrator, you can delete a workflow for either an account request or an access request.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you begin, make sure the workflow that you are deleting is no longer referenced by a provisioning policy or access definition.

Procedure

1. From the navigation tree, select **Design Workflows**. Then, click either **Manage Account Request Workflows** or click **Manage Access Request Workflows**.
2. In the page that is displayed, in the **Search information** field, type information about the workflow, and click **Search**.

You can also type information about the service to which the account request workflow is associated, or information about the access to which the access request workflow is associated.

3. In the table that lists the available workflows, select the workflow that you want to delete, and click **Delete**.
4. In the Confirm page, ensure that you want to proceed, and click then **Delete**.
5. On the **Success** page, click **Close**.

Creating a mail activity template with the workflow designer

Using the workflow designer, you can create a mail activity template that is based on a default template.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

You can use the **Workflow Designer** page to create a mail activity workflow template that specifies content to be used by mail activities across different workflows.

Procedure

1. From the navigation tree, select **Design Workflows**. Then, click either **Manage Account Request Workflows** or click **Manage Access Request Workflows**.
2. In the page that is displayed, in the table that lists the workflows, click **Create**.
3. In the **General** tab, complete the name and description of the workflow, and select a business unit and service type. Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.
4. In the **Activities** tab, click either **Simple** or click **Advanced**.

Option	Description
Simple	<ol style="list-style-type: none">a. In the Simple Activities Definition table, select an activity for approval, mail, or request for information. Then, click Go.b. Depending on the activity, complete the fields and click OK.
Advanced	<ol style="list-style-type: none">a. After the workflow designer applet starts, select the Mail node. Then, copy (click and drag) an instance of the Mail node to the Workflow Diagram workspace. Double-click the Mail node instance to open the Properties: Mail Node page.<ol style="list-style-type: none">1) In the General tab, make these entries:<ul style="list-style-type: none">• In the Activity ID field, type a value that identifies the activity, such as <code>mytesttemplate</code>.• In the Recipient field, select a recipient from the list.• Optionally, type a value for the activity name, and change the default value of the Join Type and Split Type conditions.

Option	Description
	<p>2) In the Notification tab, either type the tags and other information that you want to be displayed in a customized message notification, by completing the Subject, Text, and XHTML fields as needed. Alternatively, click Load From Template.</p> <p>If you load a template, complete these tasks:</p> <ul style="list-style-type: none"> • In the templates table, select a template. Then, click a button such as Create Like. • On the Mail Activity Template page, accept or modify the entries that populate the Template Name, Subject, Text, and XHTML fields. • Change the Text and Dynamic entries as needed. Then, click OK. <p>3) In the Postscript tab, type any postscript information.</p> <p>4) Click OK to complete the task.</p> <p>Depending on the customized steps that you took or the template that you selected, you might need to change the notification recipient.</p>

5. Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.
6. On the **Success** page, click **Close**.

Workflow notification properties

Some workflow properties can be configured to apply globally to workflows in IBM Security Identity Manager

IBM Security Identity Manager can be configured with a default escalation period that is used to determine when work items that result from workflow activities are escalated. Activity notification message templates can be customized to send notifications.

All workflow activities are escalated when the escalation period expires. The default escalation period serves as the initial value for newly defined workflow activities. To override the default escalation period, configure the escalation period for a specific activity contained in a workflow.

IBM Security Identity Manager sends email notifications for specific type of account requests and for specific events in the workflow system. The notification can be enabled or disabled based on the request type or event type. The notification template can be customized for each type of notification.

The following is a list of account requests in which an email notification can be generated:

- New account
- New password
- Change account
- Deprovision account
- Suspend account
- Restore account

For access requests that are submitted from the Identity Service Center, an email notification can be generated at the following times:

- Before the access request batch is processed
- After access request batch processing is completed

The following is a list of workflow system events in which an email notification can be generated:

- Activity timeout
- Process timeout

- Process complete
- Approval work item
- Request for input work item
- Work order
- Compliance alert
- Work item reminder

IBM Security Identity Manager can also be configured to send activity notifications and to-do list item reminders through email to workflow participants after a configured amount of time. IBM Security Identity Manager can create default notifications for a type of activity in the form of templates. Notification templates provide a consistent notification style and content across manual activities and system activities such as adding accounts and changing passwords.

Configuring the workflow escalation period

Administrators can set the default escalation limit for work items in workflows.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Before you begin, determine the escalation period that your organization needs for customary escalations.

You can use the **Workflow Notification Properties** page to change the workflow escalation limit.

Procedure

1. From the navigation tree, select **Configure System > Workflow Notification Properties**.
2. On the **Workflow Notification Properties** page, in the **Escalation Limit** field, specify the time in days, hours, and minutes. Click **OK**.
3. On the **Success** page, click **Close**.

What to do next

You might also change the default reminder interval and message.

Configuring the work item reminder interval and reminder content

Administrators can set the work item reminder interval and define reminder content.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Before you begin, determine the work item reminder interval and the reminder content that your organization needs. Because there are multiple notification templates, you might read the list of templates and their notification content first.

About this task

You can use the **Workflow Notification Properties** page to change the work item reminder interval and reminder content.

Procedure

1. From the navigation tree, select **Configure System > Workflow Notification Properties**.
2. On the **Workflow Notification Properties** page, you might complete these tasks:
 - In the **Reminder Interval** field, specify the time in days. The value that you enter cannot be less than the time interval for the escalation limit.
 - In the **Reminder Interval** table, select a notification template, and click **Change**. Your changes depend on the content of the template.
3. When your changes are complete, click **OK**.
4. On the **Success** page, click **Close**.

What to do next

You might also configure notification aggregation (post office).

Enabling workflow notification

You can use the **Workflow Notification Properties** page to enable workflow notification.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the navigation tree, select **Configure System > Workflow Notification Properties**.
2. On the **Workflow Notification Properties** page, in the **E-mail Notification Templates** table, locate the template for the notification you want to enable. In the **Status** column of the table, click the popup menu icon, and then click **Enable**.
3. After the value of the field changes to Enabled, click **OK**.
4. On the **Success** page, click **Close**.

Disabling workflow notification

You can use the **Workflow Notification Properties** page to disable workflow notification.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the navigation tree, select **Configure System > Workflow Notification Properties**.
2. On the **Workflow Notification Properties** page, in the **E-mail Notification Templates** table, locate the template for the notification you want to enable. In the **Status** column of the table, click the popup menu icon, and then click **Disable**.
3. After the value of the field changes to Disabled, click **OK**.
4. On the **Success** page, click **Close**.

Changing a workflow notification template

You can use the **Workflow Notification Properties** page to change a workflow notification template.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the navigation tree, select **Configure System > Workflow Notification Properties**.
2. On the **Workflow Notification Properties** page, in the **E-mail Notification Templates** table, select the template for the notification you want to configure. Then, click **Change**.
3. In the **Notification Template** page, make your changes to the **Template name**, **Subject**, **Plaintext body**, and **XHTML body** fields. Then, click **OK**.
4. On the **Workflow Notification Properties** page, click **OK**.
5. On the **Success** page, click **Close**.

Related tasks

[“Manually applying the email notification template changes for canceling a request” on page 963](#)

You can use the **Workflow Notification Properties** page to manually add information about canceling a request to the email notification template. When you install the IBM Security Identity Manager Fix Pack 6.0.0.3, the email notification template content that includes information about canceling a request is not automatically applied. The template changes that are available with Fix Pack 6.0.0.3 are not automatically applied so that the installation process does not overwrite any custom changes that you might have made to the email templates.

Manually applying the email notification template changes for canceling a request

You can use the **Workflow Notification Properties** page to manually add information about canceling a request to the email notification template. When you install the IBM Security Identity Manager Fix Pack 6.0.0.3, the email notification template content that includes information about canceling a request is not automatically applied. The template changes that are available with Fix Pack 6.0.0.3 are not automatically applied so that the installation process does not overwrite any custom changes that you might have made to the email templates.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the navigation tree, select **Configure System > Workflow Notification Properties**.
2. On the **Workflow Notification Properties** page, in the **E-mail Notification Templates** table, select **Process Completion Template**. Then, click **Change**.
3. In the **Notification Template** page, modify the **Plaintext body** field by adding this code to the end of the existing code:

```
<JS> if (process.canceledBy != null) { '<RE key="CanceledBy"/>: ' + process.canceledBy; }</JS>
<JS> if (process.canceledBy != null) { '<RE key="DateCanceled"/>: '; }</JS> <RE
key="readOnlyDateFormat"><PARAM>
<JS> if (process.canceledDate != null) return process.canceledDate.getTime(); else return '';</JS></
PARAM></RE>
<JS> if (process.canceledBy != null) { '<RE key="CanceledReason"/>:
<JS> (process.canceledJustification == null)? '': process.canceledJustification;</JS>'; }</JS>
```

4. In the **Notification Template** page, modify the **XHTML body** field by adding this code inside the table:

```

<tr align="left" valign="middle"><td class="text-description" bgcolor="EBEDF3">
  <RE key="CanceledBy"/></td><td width="773" class="text-description" bgcolor="white">
    <JS>process.canceledBy;</JS></td></tr>
<tr align="left" valign="middle"><td class="text-description" bgcolor="EBEDF3">
  <RE key="DateCanceled"/></td><td width="773" class="text-description" bgcolor="white">
    <RE key="readOnlyDateFormat"><PARM>
      <JS>if (process.canceledDate != null) return process.canceledDate.getTime();
      else return '';</JS>
    </PARM></RE></td></tr>
<tr align="left" valign="middle"><td class="text-description" bgcolor="EBEDF3">
  <RE key="CanceledReason"/></td><td width="773" class="text-description" bgcolor="white">
    <JS>process.canceledJustification;</JS></td></tr>

```

Place the new code inside the table between these two sets of existing code:

```

<pre><JS>Enrole.localize(process.resultDetail, "$LOCALE");</JS></pre></td></tr>

```

and

```

</table>
</td>
<!-- End Of Notification body -->

```

5. To save the changes, click **OK**.
6. On the **Workflow Notification Properties** page, click **OK**.
7. On the **Success** page, click **Close**.

Related tasks

[“Canceling pending requests” on page 1002](#)

You can cancel requests that are not completed.

[“Changing a workflow notification template” on page 963](#)

You can use the **Workflow Notification Properties** page to change a workflow notification template.

Sample workflows

This section contains sample workflows.

Sample workflow: manager approval of accounts

In this scenario, an organization has a policy that requires all accounts provisioned on a WinLocal service to be approved by the direct manager of the requestee.

The request for approval is sent to the manager of the requestee, who has two full days to approve the request. The manager might not respond to the request within the allotted time period. Then, the request is escalated to the service owner who has two full days to act on the request. The task is removed from the task list of the manager at this time. If the service owner fails to act on the request within the allotted time, the request fails, and it is canceled by the system.

The manager or service owner might act on the request within the allotted time period. An Approve response sets the process result to Approved and a Reject response sets the process result to Rejected. An Approved result provisions the account and logs the process activity in the audit log. A Rejected result cancels the process and logs the rejection in the audit log.

The graphic demonstrates this business case with the default script nodes RETURN_APPROVED and RETURN_REJECTED, which set the process result based upon participant response. The table identifies the workflow node properties and their values for a workflow named Approval_Example, defined with a service type of WinLocal Profile.

—

Figure 3. Sample workflow for manager approval

<i>Table 94. Node properties: Sample workflow for manager approval</i>		
Node	Feature	Value
Start	Activity ID	Start
	Split Type	AND
	JavaScript	N/A
Approval	Activity ID	Supervisor
	Participant	Supervisor
	Escalation Participant	Service Owner
	Escalation Limit	2 days
	Join Type	AND
	Split Type	AND
	Entity Type	Account
RETURNED_APPROVED	Activity ID	RETURNED_APPROVED
	Join Type	AND
	Split Type	AND
	JavaScript	[Custom] <code>process.setResult("AA")</code>
RETURN_REJECTED	Activity ID	RETURN_REJECTED
	Join Type	AND
	Split Type	AND
	JavaScript	[Custom] <code>process.setResult("AR")</code>

Sample workflow: multiple approvals

In this scenario, an organization has a policy in place for provisioning an account on a Windows server that is used for financial applications.

When a request is generated, a service owner must enter the appropriate account information before any approvals can take place. Then the request must be approved by both the Chief Financial Officer and the direct manager of the requestee. Each approver has one full day to act on the request.

After receiving a result from both approval requests, an email is generated and sent to the direct manager of the requestee. The email details the result and the process completes.

If both participants approve the request, the request is completed and the account is provisioned. If either of the participants rejects the request for approval, the process is completed without provisioning the account and the process result is set to Rejected.

All relevant activity is logged in the Audit Log.

Figure 4. Sample workflow: multiple approvals required

Table 95. Node properties: Sample workflow for multiple approvals

Node	Feature	Value
Start	Activity ID	Start
	Split Type	AND
	JavaScript	N/A
RFI	Activity ID	Service_Owner
	Participant	Service_Owner
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Entity Type	Account
	Entity	WinLocal
Subprocess	Activity ID	Supervisor_Approval
	Subprocess	Workflow created in "Sample workflow: manager approval of accounts"
	Join Type	AND
	Split Type	AND
Approval	Activity ID	CFO
	Participant	[Org Role] Chief Financial Officer
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Entity Type	Account
Script	Activity ID	Process_Status
	Join Type	AND
	Split Type	AND
	JavaScript	<pre> supervisorApproval= process.getActivity("Supervisor_Approval").result Summary cfoApproval=process.getActivity("CFO").resultSumma ry if(supervisorApproval==activity.APPROVED && cfoApproval==activity.APPROVED) { process.setResult(process.APPROVED) } else { process.setResult(process.REJECTED) } </pre>

Table 95. Node properties: Sample workflow for multiple approvals (continued)

Node	Feature	Value
Work Order	Activity ID	Notify_Supervisor
	Participant	Manager
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Subject	New <JS>process.subject;</JS> provisioning request for <JS>process.requesteeName;</JS>
	Message	Process Result: <JS>process.resultSummary</JS>
End	Activity ID	End
	Join Type	AND
	JavaScript	N/A
Transition Line Start > Service_Owner RFI	JavaScript	[Custom] true
Transition Line Service_Owner RFI > Supervisor_Approval Subprocess	JavaScript	[Custom] true
Transition Line Service_Owner RFI > CFO Approval	JavaScript	[Custom] true
Transition Line Supervisor_Approval Subprocess > Process_Status Script	JavaScript	[Custom] true
Transition Line CFO Approval > Process_Status Script	JavaScript	[Custom] true
Transition Line Process_Status Script > Notify_Supervisor Work Order		[Custom] true
Transition Line Notify_Supervisor Work Order > End	JavaScript	[Custom] true

Sample workflow: multiple approvals with loop processing

In this scenario, an organization has a policy in place for all new hires. A human resources staff member submits the person information, which initiates a workflow process to provision a Windows account.

A request is sent the immediate manager of the requestee and must first be approved whether the account is okay to be provisioned. If the manager rejects the approval, the account is not provisioned and the process is cancelled. Then the manager is requested to enter the information needed to provision the account. The service owner then reviews the account data to assure the account is created correctly. If any of the account information is incorrect the service owner comments on errors and rejects the request. The request is then sent back to the manager for changes. This process is repeated up to three times or until the Service Owner is satisfied with the account data and approves it. The service owner approval is strictly for approving the RFI data submitted by the manager. The service owner approval has no bearing on the end process result or provisioning of the account.

Even though the service owner is not satisfied with the manager's third correction, the department manager is requested for the approval. After the approval from the department manager, the account is provisioned. If rejected, the account is not provisioned and the process is canceled.

Basically, provisioning a new Windows account requires the approval from both the manager of the requestee and manager of the department. During the process, the account information gets audited from the service owner.

All activities are logged in the audit log.

Figure 5. Sample workflow: multiple approvals with loop processing

Table 96. Node properties: Sample workflow for multiple approvals with loop processing		
Node	Feature	Value
Start	Activity ID	Start
	Split Type	AND
	JavaScript	N/A
Approval	Activity ID	Supervisor
	Participant	Manager
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	OR
	Entity Type	Account
Loop	Name	LOOP
	Join Type	AND
	Split Type	AND
	Loop Type	While
	Loop Condition	<pre>(loopcount<=1) (loopcount <=3 && (process.getActivity ("LOOP_ServiceOwner", loopcount-1)).resultSummary ==activity.REJECTED)</pre>

Table 96. Node properties: Sample workflow for multiple approvals with loop processing (continued)

Node	Feature	Value
RFI	Name	LOOP_Supervisor
	Participant	Manager
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Entity Type	Account
	Entity	WinLocal
Approval	Name	LOOP_ServiceOwner
	Participant	Service Owner
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Entity Type	Account
Approval	Name	Department_Manager
	Participant	[Organizational Role] Department_Manager
	Escalation Participant	System Administrator
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Entity Type	Account

Table 96. Node properties: Sample workflow for multiple approvals with loop processing (continued)

Node	Feature	Value
Script	Activity ID	Process_Status
	Join Type	OR
	Split Type	AND
	JavaScript	[Custom] <pre>supervisorApproval=process.getActivity("Supervisor") .resultSummary if(supervisorApproval==activity.REJECTED) { process.setResult(process.REJECTED) }else if(supervisorApproval==activity.APPROVED) { departmentManagerApproval= process.getActivity("Department_Manager") .resultSummary if (departmentManagerApproval==activity.APPROVED) { process.setResult(process.APPROVED) } else if (departmentManagerApproval==activity.REJECTED) { process.setResult(process.REJECTED) } }</pre>
End	Activity ID	End
	Join Type	AND
	JavaScript	N/A
Transition Line Start > Supervisor Approval	JavaScript	[Custom] <pre>true</pre>
Transition Line Supervisor Approval > LOOP	JavaScript	[Approved] <pre>activity.resultSummary==activity.APPROVED;</pre>
Transition Line Supervisor Approval > Process_Status Script	JavaScript	[Rejected] <pre>activity.resultSummary==activity.REJECTED;</pre>
Loop Begin Transition Line LOOP > LOOP_Supervisor RFI		
Transition Line LOOP_Supervisor RFI > LOOP_ServiceOwner Approval	JavaScript	[Custom] <pre>true</pre>
Loop End Transition Line LOOP_ServiceOwner Approval > LOOP		
Transition Line LOOP > Department_Manager Approval	JavaScript	[Custom] <pre>true</pre>

Node	Feature	Value
Transition LineDepartment_Manager Approval > Process_Status Script	JavaScript	[Custom] true
Transition LineProcess_Status Script > End	JavaScript	[Custom] true

Sample workflow: RFI and subprocess

This example displays an entitlement workflow that uses an RFI and a subprocess.

For the request to be approved and reach completion, the following actions must occur:

- The workflow initiated by the Subprocess node must be completed with a result of approved.
- The participant defined in the RFI node is sent a request for information.

An approved response must come from the subprocess for the request to continue to the RFI.

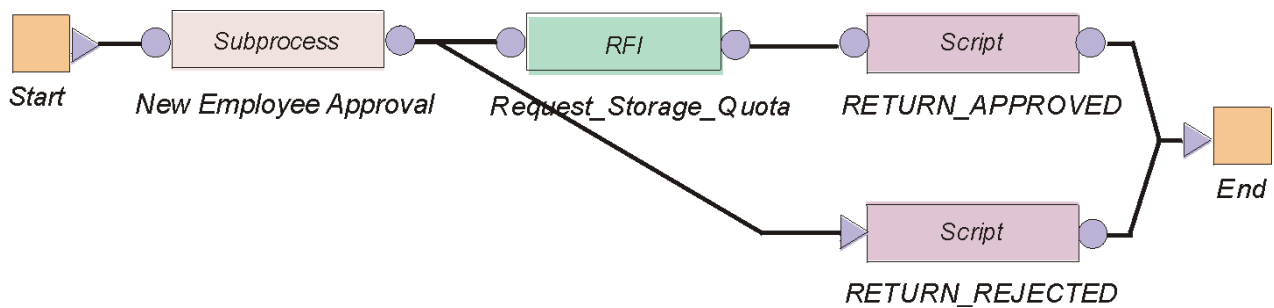


Figure 6. Sample workflow: RFI and subprocess

Node	Feature	Value
Start	Activity ID	Start
	Split Type	AND
	JavaScript	N/A
Subprocess	Activity ID	New_Employee_Approval
	Subprocess	Workflow created in "Sample workflow: supervisor approval of accounts"
	Join Type	OR
	Split Type	OR

Table 97. Node properties: Sample workflow with an RFI and a subprocess (continued)

Node	Feature	Value
RFI	Activity ID	Request_Storage_Quota
	Participant	Service Owner
	Escalation Limit	3 days
	Entity Type	Account
	Entity	WinLocalAccount
	Attribute Selection	Max. Storage
	Join Type	OR
	Split Type	OR
RETURNED_APPROVED	Activity ID	RETURNED_APPROVED
	Join Type	OR
	Split Type	OR
	JavaScript	<pre>process.setResult (process.APPROVED);</pre>
RETURN_REJECTED	Activity ID	RETURN_REJECTED
	Join Type	OR
	Split Type	OR
	JavaScript	<pre>process.setResult (process.REJECTED);</pre>
End	Activity ID	End
	Join Type	OR
	JavaScript	N/A
Transition Line Start > New Employee Approval	JavaScript	[Custom] <pre>true</pre>
Transition Line New Employee Approval > Request Storage Quota	JavaScript	[Approved] <pre>activity.resultSummary ==activity.APPROVED;</pre>
Transition Line New Employee Approval > RETURN_REJECTED	JavaScript	[Rejected] <pre>activity.resultSummary ==activity.REJECTED;</pre>
Transition Line Request Storage Quota > RETURN_APPROVED		[Custom] <pre>true</pre>
Transition Line RETURN_APPROVED > End	JavaScript	[Custom] <pre>true</pre>

Table 97. Node properties: Sample workflow with an RFI and a subprocess (continued)

Node	Feature	Value
Transition Line RETURN_REJECTED > End	JavaScript	[Custom] true

Sample workflow: approval loop

This example displays a workflow that loops an Approval node.

In this workflow, the manager approval is set within the Loop node. The manager approval repeats five times before failing if an approved or rejected response is not received within the escalation Limit.

Conditions for the transition lines to the RETURN_APPROVED and RETURN_REJECTED script nodes must be defined to retrieve and evaluate the results of the Approval node. The loop node does not return a response from the Approval.

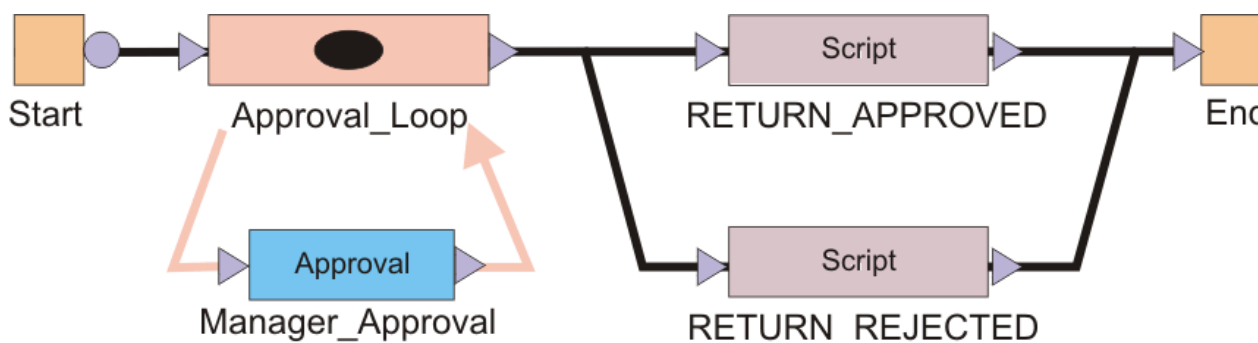


Figure 7. Sample workflow: approval loop

Table 98. Node properties: Sample workflow with an approval loop

Node	Feature	Value
Start	Activity ID	Start
	Split Type	AND
	JavaScript	N/A
Loop	Activity ID	Approval_Loop
	Loop Type	Until
	Loop Condition	var flag = approvalFlag.get();return (loopcount <= 5 && (flag != "APPROVED" && flag != "REJECTED"));
	Split Type	OR
	Join Type	OR

Table 98. Node properties: Sample workflow with an approval loop (continued)

Node	Feature	Value
Approval	Activity ID	Manager_Approval
	Participant	Manager
	Escalation Limit	1 day
	Entity Type	Account
	Postscript	if (activity.resultSummary == activity.APPROVED) { approvalFlag.set("APPROVED");} else if (activity.resultSummary == activity.REJECTED) {approvalFlag.set("REJECTED");}
	Join Type	OR
	Split Type	OR
RETURNED_APPROVED	Activity ID	RETURNED_APPROVED
	Join Type	OR
	Split Type	OR
	JavaScript	<pre>process.setResult(process.APPROVED);</pre>
RETURN_REJECTED	Activity ID	RETURN_REJECTED
	Join Type	OR
	Split Type	OR
	JavaScript	<pre>process.setResult(process.REJECTED);</pre>
End	Activity ID	End
	Join Type	OR
	JavaScript	N/A
Transition Line Start > Approval Loop	JavaScript	[Custom] <pre>true</pre>
Transition Line Approval Loop > RETURN_APPROVED	JavaScript	[Custom] <pre>approvalFlag.get() == "APPROVED"</pre>
Transition Line Approval Loop > RETURN_REJECTED	JavaScript	[Custom] <pre>approvalFlag.get() == "REJECTED"</pre>
Transition Line RETURN_APPROVED > END	JavaScript	[Custom] <pre>true</pre>

Table 98. Node properties: Sample workflow with an approval loop (continued)

Node	Feature	Value
Transition LineRETURN_REJECTED > END	JavaScript	[Custom] true
Relevant Data approvalFlag	ID	approvalFlag
	Description	Data for storing the last approval result
	Context	N/A
	Type	String
	Default Value	FALSE

Sample workflow: mail activity

Use the **Workflow Designer** page to create a mail activity workflow template that specifies content to be used by mail activities across different workflows.

Use this page to specify the contents and recipient of an email message. You can also create, change, or delete email templates used for defining contents of mail activities. To create a notification that uses an existing notification template as its initial content, or to create an entirely new notification, complete these steps:

1. From the navigation tree, select **Design Workflows**. Then, click either **Manage Account Request Workflows** or click **Manage Access Request Workflows**.
2. In the page that appears, in the table that lists the workflows, click **Create**.
3. In the **General** tab, complete the name and description of the workflow, and select a business unit and service type.
4. In the **Activities** tab, click **Simple**.
5. In the **Simple Activities Definition** table, select **Create a mail activity**. Then, click **GO**.
6. In the **Mail Activity** page, complete the following fields:

Activity name

Provides a name for the mail activity.

Recipient type

Select a recipient for mail from the list. You might select **User name** or **Group**. An additional field is displayed for you to search for and specify a specific user or group that is not in the list.

Load from Template

Click to select the mail template from which to load the content and to do other mail template management tasks. After loading the contents from a mail template, editing the content in the mail activity will affect only the mail activity, not the template.

Subject

Provides a description of the activity to the recipient of the mail notification.

Plaintext body

Provides additional details to the recipient that describe the outcome of the activity, in plaintext format. For example, an account or access request was approved.

XHTML body

Provides additional details to the recipient that describe the outcome of the activity, in XHTML format. For example, an account or access request was denied.

7. When the fields are complete, click **OK**.
8. Click other tabs to specify additional information. Then, either click **OK** to save the changes or **Apply** to save your changes and continue.

9. On the **Success** page, click **Close**.

Sample workflow: sequential approval for user recertification with packaged approval node

This scenario shows an organization policy that requires user recertification to be approved by two levels of approvers. The first approver submits decisions that are reviewed by the second approver. The second approver can change the decisions made by the first approver and then submit the final decisions. The request in this scenario is for recertification approval of user resources (accounts, groups, or roles).

For the request to be approved and reach completion, the following actions must occur:

1. A user sends the request to an IBM Security Identity Manager user (*Approver1*).
2. *Approver1* has one day to approve the request.
3. *Approver1* submits decisions for the item in the To-Do list.
4. *Approver1* sends the request to the second Security Identity Manager user (*Approver2*).
5. *Approver2* can view the decisions from *Approver1* in the To-Do list.
6. *Approver2* can make and submit additional decisions.
7. Security Identity Manager does the recertification of the user resources based on decisions of *Approver2*.

The following workflow graphic demonstrates this business case. The workflow uses the two packaged approval nodes *DECISION_OF_APPROVER1* and *DECISION_OF_APPROVER2* in a sequence. The decisions from *Approver1* are stored in the *ApprovalDocument* so that *Approver2* can view them before submitting final decisions.

Figure 8. Sample workflow: sequential approval with packaged approval node

Table 99 on page 976 identifies the workflow node properties and values for *User_Recertification_Sequential_Approval_Example*.

Node	Feature	Value
Start	Activity ID	START
	Activity Name	Start Activity
	Join Type	AND
	Split Type	AND
	JavaScript	RejectionAction.set('SUSPEND')
Extension	Activity ID	CONSTRUCT_APPROVAL_DOCUMENT
	Activity Name	CONSTRUCT_APPROVAL_DOCUMENT
	Description	Get all account and access recertification targets for person extension for recertification.
	Join Type	OR
	Split Type	AND
	Extension Name	constructApprovalDocument(Person person, RecertificationPolicy policy)

Table 99. Node properties: sample workflow for packaged approvals (continued)

Node	Feature	Value
Packaged Approval	Activity ID	DECISION_OF_APPROVER1
	Participant	Approver1
	Escalation Limit	1 day
	Skip Escalation	Checked
	Join Type	AND
	Split Type	AND
	Postscript	<pre> if (activity.resultSummary == activity.TIMEOUT) { var auditMessage = "Recertification period exceeded with no action taken, all items were approved based on policy configuration."; activity.setResult(activity.TIMEOUT, auditMessage); var doc = ApprovalDocument.get(); doc.setDecisionCodeForAllItems(activity.APPROVED); ApprovalDocument.set(doc); RecertificationWorkflow.auditTimeout(Entity.get(), Policy.get(), doc, false, true); } else if (activity.resultSummary != activity.FAILED) { RecertificationWorkflow.auditCompletion(Entity.get(), Policy.get(), ApprovalDocument.get(), false, true); } </pre>
Packaged Approval	Activity ID	DECISION_OF_APPROVER2
	Activity Name	\$ITIM_RECERTIFY
	Participant	Approver2
	Escalation Limit	10 days
	Skip Escalation	Checked
	Join Type	AND
	Split Type	AND
	Postscript	<pre> if (activity.resultSummary == activity.TIMEOUT) { var auditMessage = "Recertification period exceeded with no action taken, all items were approved based on policy configuration."; activity.setResult(activity.TIMEOUT, auditMessage); var doc = ApprovalDocument.get(); doc.setDecisionCodeForAllItems(activity.APPROVED); ApprovalDocument.set(doc); RecertificationWorkflow.auditTimeout(Entity.get(), Policy.get(), doc); } else if (activity.resultSummary != activity.FAILED) { RecertificationWorkflow.auditCompletion(Entity.get(), Policy.get(), ApprovalDocument.get()); } </pre>
Mail	Activity ID	RECERTMAIL
	Activity Name	\$RECERTMAIL
	Recipient	Requestee
	Join Type	AND
	Split Type	AND
Extension	Activity ID	REMEDiate_ACCTS_GROUPS
	Activity Name	REMEDiate_ACCTS_GROUPS
	Description	Performs account, group, and access remediation
	Join Type	OR
	Split Type	AND
	Extension Name	remediateAccountsAndGroups(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy, String rejectionAction)
Extension	Activity ID	REMEDiate_PERSON_ROLES
	Activity Name	REMEDiate_PERSON_ROLES
	Description	Performs role remediation, including policy enforcement for the person
	Join Type	OR
	Split Type	AND
	Extension Name	remediateRoleMemberships(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy, String rejectionAction)
Extension	Activity ID	UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED
	Activity Name	UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED
	Description	Updates recertification status
	Join Type	OR
	Split Type	AND
	Extension Name	updateRecertificationStatusAllApproved(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy)

Table 99. Node properties: sample workflow for packaged approvals (continued)		
Node	Feature	Value
Extension	Activity ID	UPDATE_RECERTIFICATION_STATUS_EMPTY
	Activity Name	UPDATE_RECERTIFICATION_STATUS_EMPTY
	Description	Updates recertification status
	Join Type	OR
	Split Type	AND
	Extension Name	updateRecertificationStatusEmptyDocument(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy)
End	Activity ID	END
	Activity Name	End Activity
	Join Type	OR
	Split Type	AND

Table 100 on page 978 identifies the link properties and their values for the packaged approval sample workflow.

Table 100. Link properties: sample workflow for packaged approvals			
From	To	Feature	Value
Start START	Extension CONSTRUCT_APPROVAL_DOCUMENT	Name	startToConstructApprovalDocumentExtension
		Description	Start node to construct approval document extension
		Custom Condition	true
Extension CONSTRUCT_APPROVAL_DOCUMENT	Packaged Approval DECISION_OF_APPROVER1	Name	constructApprovalDocumentExtensionToApprover1Approval
		Description	Construct approval document extension to Approver1 approval node
		Custom Condition	activity.resultSummary == activity.SUCCESS
Extension CONSTRUCT_APPROVAL_DOCUMENT	Extension UPDATE_RECERTIFICATION_STATUS_EMPTY	Name	constructApprovalDocumentExtensionToUpdateStatusEmpty
		Description	Construct approval document extension to update status for empty document
		Custom Condition	activity.resultSummary == activity.WARNING
Extension CONSTRUCT_APPROVAL_DOCUMENT	End END	Name	constructApprovalDocumentExtensionToEnd
		Description	Construct approval document extension to end node
		Custom Condition	activity.resultSummary != activity.SUCCESS && activity.resultSummary != activity.WARNING
Packaged Approval DECISION_OF_APPROVER1	Packaged Approval DECISION_OF_APPROVER2	Name	approver1ApprovalToApprover2Approval
		Description	Approver1 approval node to Approver2 approval node
		Custom Condition	activity.resultSummary != activity.FAILED
Packaged Approval DECISION_OF_APPROVER2	Mail RECERTMAIL	Name	approver2ApprovalToMail
		Description	Approver2 approval node to mail node
		Custom Condition	(activity.resultSummary != activity.FAILED) && (ApprovalDocument.get().containsDecisionCode(activity.REJECTED))
Packaged Approval DECISION_OF_APPROVER2	Extension UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED	Name	approver2ApprovalToUpdateStatus
		Description	Approver2 approval node to update recertification status
		Custom Condition	(activity.resultSummary != activity.FAILED) && (! ApprovalDocument.get().containsDecisionCode(activity.REJECTED))
Mail RECERTMAIL	Extension REMEDiate_ACCTS_GROUPS	Name	mailToRemediateAccts
		Description	Mail node to remediate accounts, groups, and accesses
		Custom Condition	true
Extension REMEDiate_ACCTS_GROUPS	Extension REMEDiate_PERSON_ROLES	Name	remediateAcctsToRemediateRoles
		Description	Remediate accounts, groups, and accesses to remediate roles
		Custom Condition	true
Extension REMEDiate_PERSON_ROLES	End END	Name	remediateRolesToEnd
		Description	Remediate roles to end node
		Custom Condition	true

From	To	Feature	Value
Extension UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED	End END	Name	updateStatusToEnd
		Description	Update recertification status to end node
		Custom Condition	true
Extension UPDATE_RECERTIFICATION_STATUS_EMPTY	End END	Name	updateStatusEmptyToEnd
		Description	Update status for empty document to end node
		Custom Condition	true

Sample workflow: packaged approval combined with simple approval node

This scenario shows an organization with a policy that requires user recertification. User recertification validates user resources (accounts, groups, or roles).

IBM Security Identity Manager does the request based on the following decisions:

- The request for recertification approval of user roles is sent to the respective role owners.
- The request for recertification approval of user accounts and groups is sent to the manager of the user to be recertified.

The following workflow graphic demonstrates this business case:

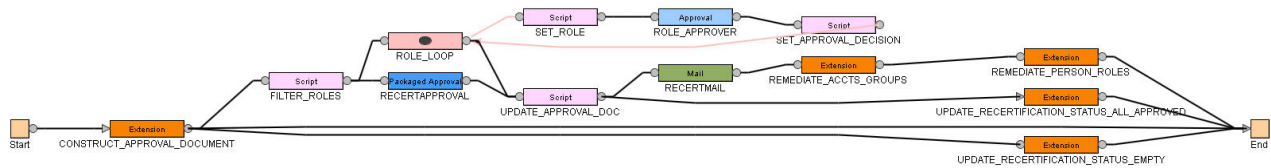


Figure 9. Sample workflow: simple approval with packaged approval node

Table 101 on page 979 identifies the workflow node properties and values for *User_Recertification_Simple_Approval_Example*.

Node	Feature	Value
Start	Activity ID	Start
	Activity Name	Start Activity
	Join Type	AND
	Split Type	AND
	JavaScript	RejectionAction.set('SUSPEND');
Extension	Activity ID	CONSTRUCT_APPROVAL_DOCUMENT
	Activity Name	CONSTRUCT_APPROVAL_DOCUMENT
	Description	Get all account and access recertification targets for person extension for recertification
	Join Type	OR
	Split Type	AND
	Extension Name	constructApprovalDocument(Person person, RecertificationPolicy policy)

Table 101. Sample workflow node properties: Simple approval for user recertification with packaged approval node (continued)

Node	Feature	Value
Script	Activity ID	FILTER_ROLES
	Activity Name	FILTER_ROLES
	Description	Extracts roles from the approval document and creates a temporary approval document with the roles
	Join Type	AND
	Split Type	AND
	JavaScript	<pre> var updatedDoc=ApprovalDocument.get(); var tempDoc=new PackagedApprovalDocument(); TemporaryDocument.set(tempDoc); var tempRoles=new Array(); var roleItems=updatedDoc.getItemsByType (ApprovalDocument.get().TYPE_ROLE); for(var i=0;i<roleItems.length;i++) { updatedDoc.removeItem(roleItems[i]); var role=roleItems[i].getValue().dn; var role=new Role(role); tempRoles.push(role); RolesThere.set("true"); } Roles.set(tempRoles); ApprovalDocument.set(updatedDoc); var accountsCount=updatedDoc.getItemsByType (ApprovalDocument.get().TYPE_ACCOUNT); var groupCount=updatedDoc.getItemsByType (ApprovalDocument.get().TYPE_GROUP); if(!accountsCount.length==0 !groupCount.length==0) { OnlyRoles.set("false"); } else { OnlyRoles.set("true"); } </pre>
Packaged Approval	Activity ID	RECERTAPPROVAL
	Activity Name	ITIM_RECERTIFY
	Participant	Manager
	Escalation Participant	Participant Type
	Escalation Limit	10 days
	Skip Escalation	Checked
	No Timeout Action	Unchecked
	Join Type	AND
	Split Type	AND
Loop	Activity ID	ROLE_LOOP
	Activity Name	ROLE_LOOP
	Description	This loop is required to iterate through the roles.
	Join Type	AND
	Split Type	AND
	Loop Type	Until
	Loop Condition	return loopcount<=Roles.get().length;
Script	Activity ID	UPDATE_APPROVAL_DOC
	Activity Name	UPDATE_APPROVAL_DOC
	Description	Gets the role information from the temporary approval document and updates in into the approval document
	Join Type	AND
	Split Type	AND
	JavaScript	<pre> var approvalDoc=ApprovalDocument.get(); var tempDoc=TemporaryDocument.get(); var roleItems=tempDoc.getItemsByType (TemporaryDocument.get().TYPE_ROLE); for(var i=0;i<roleItems.length;i++) { approvalDoc.addItem(roleItems[i]); } ApprovalDocument.set(approvalDoc); </pre>

Table 101. Sample workflow node properties: Simple approval for user recertification with packaged approval node (continued)

Node	Feature	Value
Script	Activity ID	SET_ROLE
	Activity Name	SET_ROLE
	Description	Sets the role in relevant data
	Join Type	AND
	Split Type	AND
	JavaScript	<pre>var roles=Roles.get(); var role=roles[loopcount-1]; RoleHolder.set(role);</pre>
Work Order	Activity ID	RECERTWORKORDER
	Activity Name	RECERTWORKORDER
	Escalation Limit	9 days
	Join Type	AND
	Split Type	AND
Approval	Activity ID	ROLE_APPROVER
	Activity Name	ROLE_APPROVER
	Participant	Custom var owner=RoleHolder.get().getProperty("owner")[0]; return new Participant(ParticipantType.USER,owner);
	Escalation Participant	Participant Type
	Escalation Limit	1 day
	Join Type	AND
	Split Type	AND
	Entity Type	Organizational Role
Mail	Activity ID	RECERTMAIL
	Activity Name	RECERTMAIL
	Recipient	Person (With Email Account)
	Join Type	AND
	Split Type	AND
Extension	Activity ID	REMIATE_ACCTS_GROUPS
	Activity Name	REMIATE_ACCTS_GROUPS
	Description	Does account, group, and access remediation
	Join Type	AND
	Split Type	AND
	Extension Name	remediateAccountsAndGroups(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy, String rejectionAction)
Script	Activity ID	SET_APPROVAL_DECISION
	Activity Name	SET_APPROVAL_DECISION
	Description	Updates the temporary approval document with the role and its decision
	Join Type	AND
	Split Type	AND
	JavaScript	<pre>var updatedDoc=TemporaryDocument.get(); var res=result.get(); var roleItems=Roles.get(); var roleItem=new PackagedApprovalItem (ApprovalDocument.get().TYPE_ROLE,roleItems[loopcount-1],res); var dec=roleItem.getDecisionCode() updatedDoc.addItem(roleItem); TemporaryDocument.set(updatedDoc);</pre>
Extension	Activity ID	REMIATE_PERSON_ROLES
	Activity Name	REMIATE_PERSON_ROLES
	Description	Does role remediation, including policy enforcement for the person
	Join Type	AND
	Split Type	AND
	Extension Name	remediateRoleMemberships(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy, String rejectionAction)

Table 101. Sample workflow node properties: Simple approval for user recertification with packaged approval node (continued)		
Node	Feature	Value
Extension	Activity ID	UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED
	Activity Name	UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED
	Description	Updates recertification status with all approved user resources
	Join Type	OR
	Split Type	AND
	Extension Name	updateRecertificationStatusAllApproved(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy)
Extension	Activity ID	UPDATE_RECERTIFICATION_STATUS_EMPTY
	Activity Name	UPDATE_RECERTIFICATION_STATUS_EMPTY
	Description	Updates recertification status with no user resources
	Join Type	AND
	Split Type	AND
	Extension Name	updateRecertificationStatusEmptyDocument(PackagedApprovalDocument approvalDocument, Person person, RecertificationPolicy policy)
End	Activity ID	End
	Activity Name	End Activity
	Join Type	OR
	Split Type	AND
	JavaScript	

Table 102 on page 982 identifies the link properties and values for the simple approval node.

Table 102. Link properties: Simple approval for user recertification			
From	To	Feature	Value
Start	Extension CONSTRUCT_APPROVAL_DOCUMENT	Name	startToConstructApprovalDocumentExtension
		Description	Start node to construct approval document extension
		Custom Condition	true
Extension CONSTRUCT_APPROVAL_DOCUMENT	Script FILTER_ROLES	Name	ConstructApprovalDocumentExtensionToFilterRolesScript
		Description	Construct approval document extension to filter roles script
		Custom Condition	activity.resultSummary == activity.SUCCESS
Extension CONSTRUCT_APPROVAL_DOCUMENT	End	Name	ConstructApprovalDocumentExtensionToEnd
		Description	Construct approval document extension to end node
		Custom Condition	activity.resultSummary != activity.SUCCESS && activity.resultSummary != activity.WARNING
Extension CONSTRUCT_APPROVAL_DOCUMENT	Extension UPDATE_RECERTIFICATION_STATUS_EMPTY	Name	ConstructApprovalDocumentExtensionToUpdateStatusEmpty
		Description	Construct approval document extension to update status for empty document
		Custom Condition	activity.resultSummary == activity.WARNING
Script FILTER_ROLES	Packaged Approval RECERTAPPROVAL	Name	FilterRolesScriptToRecertApproval
		Description	Filter roles script to recert approval
		Custom Condition	OnlyRoles.get()=="false"
Script FILTER_ROLES	Loop ROLE_LOOP	Name	FilterRolesScriptToRoleLoop
		Description	Filter roles script to role loop
		Custom Condition	RolesThere.get()=="true"
Loop ROLE_LOOP	Script COMBINE_APPROVAL_DOC	Name	RoleLoopToCombineApprovalDocScript
		Description	Role loop to combine approval document script
		Custom Condition	true
Script COMBINE_APPROVAL_DOC	Packaged Approval RECERTAPPROVAL	Name	CombineApprovalDocScriptToRecertApproval
		Description	Combine approval document script to recert approval
		Custom Condition	true

Table 102. Link properties: Simple approval for user recertification (continued)

From	To	Feature	Value
Script COMBINE_APPROVAL_DOC	Mail RECERTMAIL	Name	CombineApprovalDocScriptToMail
		Description	Combine approval document script to mail node
		Custom Condition	(activity.resultSummary != activity.FAILED) && (ApprovalDocument.get().containsDecisionCode(activity.REJECTED))
Script COMBINE_APPROVAL_DOC	Extension UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED	Name	CombineApprovalDocScriptTo
		Description	Combine approval document script to
		Custom Condition	(activity.resultSummary != activity.FAILED) && (!ApprovalDocument.get().containsDecisionCode(activity.REJECTED))
Script SET_ROLE	Approval ROLE_APPROVER	Name	SetRoleScriptToRoleApproverApproval
		Description	Set role script to role approver approval
		Custom Condition	true
Approval ROLE_APPROVER	Script SET_APPROVAL_DECISION	Name	RoleApproverApprovalToSetApprovalDecisionScript
		Description	Role approver approval to set approval decision script
		Custom Condition	true
Mail RECERTMAIL	Extension REMEDiate_ACCTS_GROUPS	Name	mailToRemediateAccts
		Description	Mail node to remediate accounts, groups, and accesses
		Custom Condition	true
Extension REMEDiate_ACCTS_GROUPS	Extension REMEDiate_PERSON_ROLES	Name	remediateAcctsToRemediateRoles
		Description	Remediate accounts, groups, and accesses to remediate roles
		Custom Condition	true
Extension REMEDiate_PERSON_ROLES	End	Name	remediateRolesToEnd
		Description	Remediate roles to end node
		Custom Condition	true
Extension UPDATE_RECERTIFICATION_STATUS_ALL_APPROVED	End	Name	updateStatusToEnd
		Description	Update recertification status to end node
		Custom Condition	true
Extension UPDATE_RECERTIFICATION_STATUS_EMPTY	End	Name	updateStatusEmptyToEnd
		Description	Update status for empty document to end node
		Custom Condition	true

Table 103 on page 983 identifies the relevant data used in the simple approval node.

Table 103. Relevant Data

ID	Type
ApprovalDocument	PackagedApprovalDocument
Roles	List
RoleHolder	OrgRole
TemporaryDocument	PackagedApprovalDocument
RejectionAction	String
result	String
OnlyRoles	String
RolesThere	String

Sample workflow: access owner approval

In this scenario, an organization has a policy that requires access to be provisioned for a user to access an application.

Note that this example applies only to group accesses. It does not apply to roles that are exposed as accesses. See [\\${ISIM_HOME}/extensions/6.0/examples/workflow/roleApproval/index.html](#) for examples of configuration changes needed to require or skip access owner (or other) approval for role-based examples.

The access request must be approved by the access owner. The request for approval is sent to the access owner, who has two full days to approve the request. The access owner might not respond within the allotted period. In that case, the request is removed from the task list of the access owner and is escalated to the service owner. The service owner then has two full days to act on the request. If the service owner fails to act on the request within the allotted time, the request fails, and is canceled by the system.

The access owner or the service owner might act on the request within the allotted time period. An Approve response sets the process result to Approved and a Reject response sets the process result to Rejected. An Approved result provisions the access and logs the process activity in the audit log. A Rejected result cancels the process and logs the rejection in the audit log.

The graphic demonstrates this business case with the default script nodes RETURN_APPROVED and RETURN_REJECTED, which set the process result based upon participant response. The table identifies the workflow node properties and their values for the workflow.

Figure 10. Sample workflow for access request

Table 104. Node properties: Sample workflow for access request		
Node	Feature	Value
Start	Activity ID	Start
	Split Type	AND
	JavaScript	N/A
Approval	Activity ID	AccessOwnerApproval
	Participant	Access Owner
	Escalation Participant	Service Owner
	Escalation Limit	2 days
	Join Type	AND
	Split Type	AND
	Entity Type	UserAccess
RETURNED_APPROVED	Activity ID	RETURNED_APPROVED
	Join Type	AND
	Split Type	AND
	JavaScript	[Custom] <code>process.setResult("AA")</code>
RETURN_REJECTED	Activity ID	RETURN_REJECTED
	Join Type	AND
	Split Type	AND
	JavaScript	[Custom] <code>process.setResult("AR")</code>

Chapter 14. Activity administration

An activity is the smallest unit of work in a workflow. For a user assigned to the activity, it represents a task to perform.

Collectively, the activities assigned to you represent your "to-do" list. You can perform the following actions with an activity assigned to you:

- view it
- complete it
- lock it (to claim exclusive access to completing it)
- assign it to another user
- delegate it to another user

Depending on the workflow type and configuration, if you do not complete an activity within a defined time, the activity may be escalated to another user.

Administrators can view their own activities and activities that belong to another user. Depending on the workflow and the policies affecting the workflow, administrators may also be able to complete, lock, reassign, or delegate activities that belong to another user.

Access and permissions

Your options for working with activities appear in the **Manage Activities** section of the navigation tree. You can view activities and perform actions on them as defined by system policies and permissions, including those defined within a workflow. Contact your system administrator if you encounter issues in working with activities.

Viewing activities

You can view a list of to-do items that require action.

About this task

Activities that you can view are part of workflow processes that require your participation in order to proceed.

The **View Activities** page contains the following item types:

- Approval requests
- Recertification requests
- Work order requests
- Requests for Information (RFI)
- Policy Compliance alerts

From this page you work with the activities you select.

Procedure

1. In the navigation tree, select **Manage Activities** > **View Activities**.
2. On the **View Activities** page, click **Refresh** to update the **Activities** table.
3. To view the details of an activity, click the activity.
The information about the activity is read-only.
4. Click **Close** to close the activity details.
5. When you are done reviewing activities, click **Close**.

Viewing activities for a user

You can view activities for other users if you have the appropriate permissions.

Procedure

1. In the navigation tree, select **Manage Activities > View Activities by User**.
2. On the **Select Account** page, type the user ID in the **User ID** field and then click **Search**.
3. In the ITIM Accounts table, select the accounts that you want to view activities for.
These activities are associated with a specific user ID and activity owner.
4. Click **Continue**.
5. On the **View Activities by User** page, click the activity to view information about the activity. The information about the activity is read-only.
6. Click **Close** to close the activity details.
7. When you are done reviewing activities for a user, click **Close**.

Locking an activity

Lock an activity to claim exclusive access to working with it. When you lock an activity, other users cannot act on it.

About this task

Activities that are assigned to you are displayed in your activities list. In some cases, you might be only one of many participants who are permitted to complete the activity. For items that are assigned to multiple people, you can select one or more activities and lock them. Use the lock to act on the item and prevent others from duplicating or otherwise conflicting with your efforts. Locked items are displayed as locked in the queues of other participants. Only the lock owner or a system administrator can unlock them.

Lock actions are an audited process. If the lock owner is removed from the system, their locks are also removed.

Procedure

1. In the navigation tree, select **Manage Activities > View Activities**.
2. Select one or more activities, then click **Lock** to lock the activities.

Unlocking an activity

You can unlock activities that you locked. Once it is unlocked, an activity can be completed by other users.

About this task

Locked items are displayed as locked in your activities list and in the activities lists of other participants. Only the lock owner or a system administrator can unlock a locked activity.

To unlock an activity, complete these steps:

Procedure

1. In the navigation tree, select **Manage Activities > View Activities**.
2. Select one or more locked activities, then click **Unlock** to unlock the activities.

Delegating activities

You can delegate activities for completion.

To delegate activities from one user to another user, the user you are delegating to must have authorization from the system administrator to manage activities. If you are delegating activities for yourself, you must have both read and write Delegate access control item attribute permissions set to Grant. The logged-in user must have the access control item permission to write the delegate attribute of the user who is delegated.

You can add or delete delegation schedules for the user whose activities you are delegating. Adding a delegation schedule requires you to select a user who can manage activities and specify a time period in which to delegate activities. You can set up multiple delegation schedules for multiple delegates, but time periods cannot overlap. If you already delegated activities and want to turn off delegation, delete the delegation schedule.

Delegation does not affect the escalation period for an activity. That is, it does not restart the escalation period.

Creating a delegation schedule

You can delegate your to-do items to another user during a time when you are not available to manage them by creating delegation schedules.

About this task

Your activities can be delegated only to one user. Your activities might be delegated to one user. If you delegate them to another user without stopping the first delegation, the second delegation replaces the first one.

Delegation does not affect the escalation period for an activity. That is, it does not restart the escalation period.

Procedure

1. In the navigation tree, select **Manage Activities > Manage Delegation Schedules**.
2. On the **Manage Delegation Schedules** page, click **Add** to create a delegation schedule.
3. On the **Setup Delegation** page, click **Search** to find a user.
4. On the **Select Delegate Account** page, complete these steps:
 - a) Type information about a user in the **User ID** field and click **Search**.
 - b) In the Accounts table, click the name of the user whose account you want to delegate your activities to, then click **OK**.
5. On the **Setup Delegation** page, click the calendar and clock icons to choose a date and time for starting and ending the delegation, then click **OK**.
6. On the **Success** page, click **Close**.

Changing delegation schedules

You can change your current delegation schedule.

About this task

If you change a delegation schedule, you are only allowed to change the schedule and not the delegation owner.

Delegation does not affect the escalation period for an activity. That is, it does not restart escalation period.

Procedure

1. In the navigation tree, select **Manage Activities > Manage Delegation Schedules**.
2. On the **Manage Delegation Schedules** page, select the delegation schedule you want to change and click **Change** to modify the delegation schedule.
3. On the **Setup Delegation** page, click the calendar and clock icons to choose a new date and time for starting and ending the delegation. After you set the times, click **OK**.
4. On the **Success** page, click **Close**.

Deleting delegation schedules

You can delete or cancel delegation schedules.

About this task

When you delete an active delegation, you are stopping the current delegation.

Deleting a delegation does not affect the escalation period for an activity. That is, it does not restart the escalation period.

Procedure

1. From the navigation tree, select **Manage Activities > Manage Delegation Schedules**.
2. On the **Manage Delegation Schedules** page, select the delegation schedule you want to remove, then click **Delete**.
3. On the **Confirm** page, click **Delete**.
4. On the **Success** page, click **Close**.

Assigning activities to another user

You can assign activities to other users for completion.

About this task

A person can be designated as the new owner of the activity if they are a participant of the selected activity as an individual. A new owner of an activity can be a member of a relevant group, such as a service owner. For example, you might assign an activity to another person who is listed as a required approver for the activity.

To assign an activity to another user, complete these steps:

Procedure

1. In the navigation tree, select **Manage Activities > View Activities**.
2. Select one or more activities, then click **Assign**.
3. Select an authorized user from the table, then click **Assign**. Only authorized users are displayed in this table for selection.
4. On the **Success** page, click **Close**.

Requests and activities

Requests initiate a workflow or a work order for manual service operations.

There are many different types of requests that can occur, such as requesting changes to accounts, adding and modifying users, and changing policies. Some requests might require the completion of an activity by another user, such as an approval or recertification. Other requests can be completed without any further actions.

Note: Requests that do not initiate a workflow, such as Orphan Account Requests, do not get displayed in the pending or completed requests.

Requests can involve several steps to complete. Each step might require different users to complete an action. You can view the status of a request by viewing pending requests or all requests that are both pending and completed.

Completed requests are requests that completed processing. The completion of a request does not mean that it was successful. Requests might fail, might complete with a warning message, or might be canceled while in a pending state.

Pending requests are requests that are submitted but are not finished. These requests might be in the process of running or might require the completion of a workflow activity, such as a recertification or approval activity.

Escalation

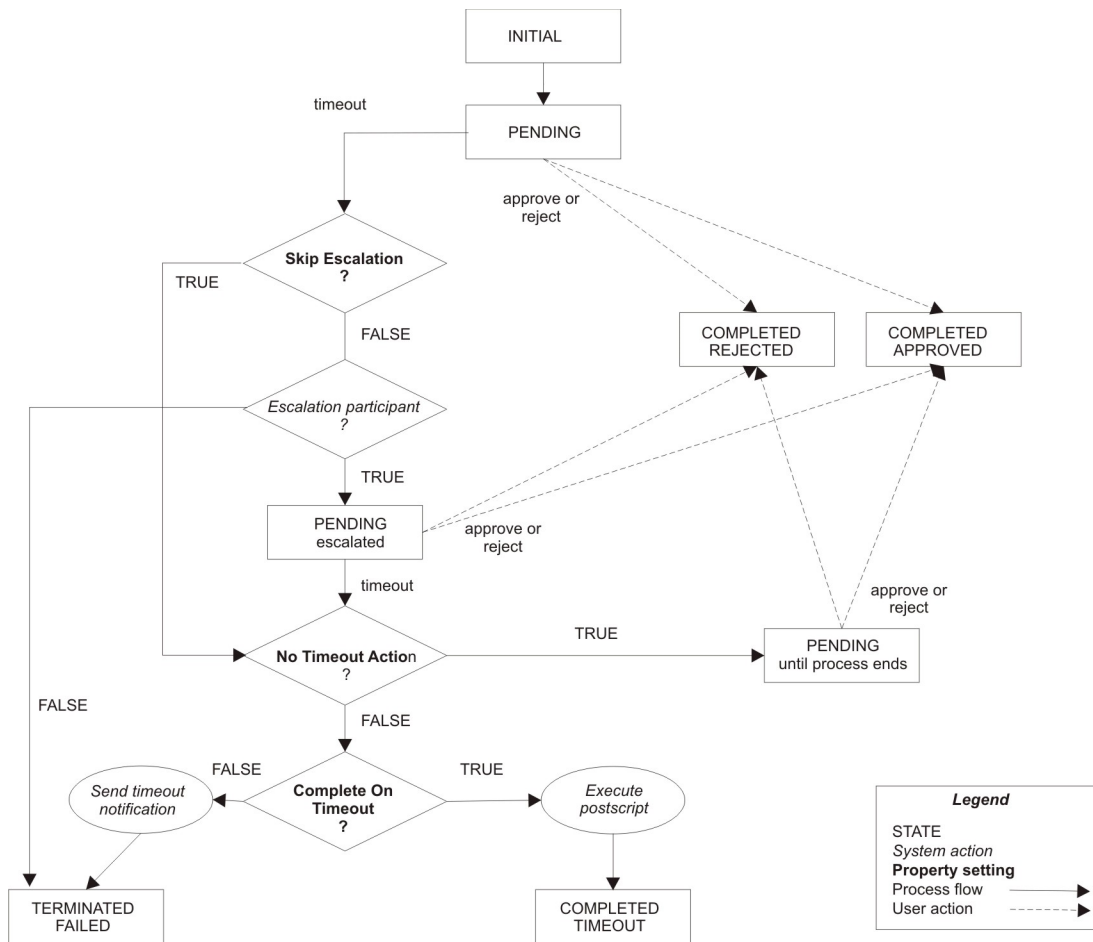
The escalation period specifies the period within which an assigned party must do an activity before it is designated to a specified escalation participant.

Escalation is the period in which the participant must process approvals, requests for information, work orders, compliance alerts, and recertifications. If the participant does not complete the activity by the escalation date, the activity is sent to the escalation participant and the escalation period restarts. Activity is terminated if none of the participants act on it. Activity is sent to the system administrator only if participant resolution fails.

Escalation behavior is controlled through properties on approval, RFI, or work order nodes. The following properties affect escalation behavior:

- **Skip Escalation**
- **No Timeout Action**
- **Complete on Timeout**

The following figure shows a flow diagram that illustrates how each property affects the process.



The following list describes escalation process that is pictured in the diagram.

1. Request arrives

- If a participant handles the request by accepting it or rejecting it, the activity ends in the corresponding state.
- If the request times out, the system checks the **Skip Escalation** property.

2. Check for skipping escalation.

- If **Skip Escalation** is set, the activity continues and checks the **No Timeout Action** property.
- If **Skip Escalation** is not set, the systems checks for the escalation participant. If it can identify the configured escalation participant, the activity is put into PENDING state for the escalation participant to handle. If no escalation participant is configured for the activity or the check for the escalation participant fails, the activity ends with state TERMINATED/FAILED.

3. Check for timeout action. If **Skip Escalation** is set or the activity times out of the PENDING state for escalation, the system checks the **No Timeout Action** property.

- If FALSE, the system proceeds and checks the **Complete On Timeout** property.
- If TRUE, the activity is placed in PENDING state. A participant can approve or reject the request.

4. Check for what to do when the activity times out.

- If **Complete On Timeout** is set (TRUE), the postscript for the activity runs and the activity state is set to COMPLETED/TIMEOUT.
- If **Complete On Timeout** is not set (FALSE), the system sends a timeout notification and the activity state is set to TERMINATED/FAILED.

Activity types

An activity in your activities list may be one of several types.

Activities that you can view are part of workflow processes that require your participation in order to proceed.

The **View Activities** page contains the following types of activity:

- Approval activities
- Requests for Information (RFI) activities
- Work order activities
- Compliance alert activities
- Recertification activities

From this page you work with the activities you select.

Approval activities

An approval activity prompts the assigned user to approve or reject a request.

If the request is approved, the next activity in the workflow is processed. If, however, the request is rejected, the workflow stops and no additional activities are processed.

If you submit a request that must be approved, the approval activity is sent to all participants in the assigned group except to the user who makes the request. You might be a member of the group who normally approves requests. If you are the person who makes the request, you do not see the approval activity in your activities list.

If a timeout occurs, the Activity Result Summary Code is set to SF (failed). If a participant resolution failure occurs, the Activity Result Summary Code can take the following values:

AA (approved)

If the request is submitted by the system administrator, the request is automatically approved by the system administrator. The approval occurs even though the system administrator is not explicitly set as an escalation participant. The result is set to Approved.

SF (failed)

The Approval activity ends with result set to Failed, if:

- The request is submitted by a non-admin user.
- The escalation participant is not defined at all.

Note: This result is true even when the requester is the system administrator.

- The participant resolution failed.

If the property `enrole.workflow.skipapprovalforrequester` is set to `true` in `enRole.properties` file and the requester is identified as one of the participant users, the approval is completely skipped. The Activity Result Summary Code is set to AA (approved). When an RFI activity times out or fails because of participant resolution failure, the Activity Result Summary Code is set to SF (failed) for both cases.

Approval states

When you view the status of an approval, the approval activity is in one of several states.

The states of an approval activity can be viewed only by the user who submitted the request.

Approval activity state	Description
Approved	The account request was approved, and the next activity in the workflow is processed.

Approval activity state	Description
Rejected	The account request was rejected. No additional activities are processed.
Pending	No action was taken to complete the approval.

Completing an approval activity

You can approve or reject approval activities.

Procedure

1. In the navigation tree, select **Manage Activities > View Activities**.
2. On the **View Activities** page, click the name of the approval activity.
3. On the **Approval Details** page, review the approval details, enter a comment for the approval or rejection of the request, then click **Approve** or **Reject**.
4. On the **Success** page, click **Close**.

Request for information activities

A request for information activity prompts you to supply information about a request.

Request-for-information activities in your activities list are part of workflow processes that require your response before they can be completed. For example, a user submits an account request but does not have the knowledge required to specify a value for a particular attribute. The system administrator creates a process to send the request to a more knowledgeable user. That user can then specify the appropriate value for the attribute.

Request for information (RFI) states

Request for information (RFI) activities have several states.

The states of an RFI activity can be viewed only by the user who submitted the request. The following table shows a description of each RFI state.

Request state	Description
Canceled	A pending request is canceled and any action items associated with the request are canceled.
Escalated	Because the original approver did not complete the RFI in the allotted amount of time, the RFI was sent to another approver.
Failed	The activity could not be completed. No further activity occurs.
Participant Resolution Failed	The activity could not be completed because the approver was deleted from the system.
Pending	No action was taken to complete the activity.
Submitted	The activity was submitted for approval.
Success	The RFI was successfully completed.
Terminated	The process run fails with an unknown exception.
Timeout	The specified amount of time to complete an activity passed. The activity is completed and a new activity is created and sent to the escalation participant.

Table 106. Descriptions of the states of RFIs (continued)

Request state	Description
Warning	The activity was partially completed. A problem occurred, preventing the work order from being successfully completed.

Related reference

[ACTIVITY table](#)

Completing a request for information activity

You can provide information for request-for-information activities.

Procedure

1. In the navigation tree, select **Manage Activities > View Activities**.
2. On the **View Activities** page, click the name of the request for information activity.
3. On the **RFI Details** page, review the request for information details, then click **Provide Information**.
4. On the **Provide Information** page, provide information for the request as needed, then click **Submit**.
5. On the **Success** page, click **Close**.

Work order activities

Work order activities are part of workflow processes that require your response in order to be completed.

Work order activities are displayed in your to-do list and consist of action items that you must complete outside the system. For example, you can be assigned a work order to have an office key made for a new employee. After you complete the work order activity, you enter the outcome of the work order when you complete the activity in IBM Security Identity Manager.

Work order states

When you view the status of a work order, the work order activity is in one of several states.

The states of a work order activity can be viewed only by the user who submitted the request. [Table 107](#) on page 993 gives a description of each work order state.

Table 107. Descriptions of the states of work order requests

Work order state	Description
Success	The work order was successfully completed, and the next activity in the workflow is processed.
Warning	The work order was partially completed. A problem occurred, preventing the work order from being successfully completed. No additional activities are processed.
Failure	The work order was not completed. No additional activities are processed.
Pending	No action was taken to complete the work order.

Completing a work order activity

You can complete work order activities.

Procedure

1. In the navigation tree, select **Manage Activities > View Activities**.
2. On the **View Activities** page, click the name of the work order activity.
3. On the **Work Order Details** page, review the work order, enter any comments as needed, then click one of the following options:

- Click **Successful** to indicate that the work order was completed successfully.
 - Click **Warning** to indicate that the work order completed successfully, but with warnings or exceptions.
 - Click **Failure** to indicate that the work order was not completed successfully.
4. On the **Success** page, click **Close**.

Compliance alert activities

A compliance alert creates an activity for a user who is not in compliance. The user or an administrator can respond.

Compliance rules can govern access to an account and can specify attributes that are required in a resource or asset.

The user who owns the compliance alert activity typically must update the account or attribute that is not in compliance.

An administrator may also perform the following actions:

- remove a noncompliant account
- update noncompliant attributes in a resource or asset
- change the due date of compliance alert activities for any user

See also the following topics:

- [“Configuring compliance alert rules” on page 742](#)
- [“Completing a compliance alert activity” on page 994](#)
- [“Deferring policy compliance alerts” on page 995](#)

Completing a compliance alert activity

You can correct or defer accounts or access entitlements that do not comply with a policy.

About this task

Policy compliance alerts can be displayed when accounts or access entitlements do not comply with a policy. For example, you have an existing account to use an employee records database. An administrator creates a policy that states that you must be assigned to the role of HRManager π to access the records. To bring the account back into compliance, you must be assigned the role of HRManager π .

You might need to defer policy compliance alerts. In the example, assume that you cannot assign the HRManager π role to each account without first verifying that the owner of each account belongs in the role of HRManager π . You determine that the amount of time it takes to verify that each account owner exceeds the escalation period of the alert, at which time, the alert is forwarded. You can decide to defer the compliance alert, which keeps the item in your activities list for an extended period.

You can correct or defer multiple policy compliance alerts at one time if they are grouped together in your activities list.

Policy compliance alerts listed in your activities list are part of workflow processes that require your response before they can complete.

Procedure

1. In the navigation tree, select **Manage Activities > View Activities**.
2. On the **View Activities** page, click the name of the compliance alert activity.
3. On the **Compliance Alert Details** page, review the compliance alert, enter any comments as needed, then click one of the following options:
 - Click **Correct** to correct the compliance alert.
 - Click **Defer** to defer the compliance alert to a later time.

4. On the **Success** page, click **Close**.

Deferring policy compliance alerts

You can defer policy compliance alerts in your activities list.

About this task

You might need to defer policy compliance alerts. For example, assume that you are responsible for accounts used to access an employee records database. An administrator creates a policy that states that all accounts must be assigned to the role of HRManager to access the records. The accounts are currently not compliant with the policy. In order to bring the accounts back into compliance, they each must be assigned the role of HRManager. Now assume that you cannot assign the HRManager role to each account without first verifying that each account owner belongs in the role of HRManager. You determine that the amount of time required to verify each account owner is greater than the escalation period of the alert. Escalation forwards the alert. You decide to defer the compliance alert, which keeps the item in your activities list for an extended period.

You can defer multiple policy compliance alerts at one time if they are grouped together in your activities list.

Procedure

1. In the navigation tree, select **Manage Activities > View Activities**.
2. Click **Defer**.
3. On the **Success** page, click **Close**.

Recertification activities

Recertification activities are part of workflow processes that require your response before they can be complete.

Recertification activities are displayed in your activities list. Three types of recertification activities exist:

Access

Certifies whether an access is still required.

Account

Certifies whether an account is still required.

User

Certifies whether the roles, accounts, and accesses for a specific user are still required.

Completing a recertification activity

You can complete recertification activities.

Procedure

1. In the navigation tree, select **Manage Activities > View Activities**.
2. On the **View Activities** page, click the name of the recertification activity.
3. On the **Approval Details** page, review the recertification, enter any comments as needed, then click **Approve** or **Reject** to approve or reject the recertification.
4. On the **Success** page, click **Close**.

Chapter 15. Requests administration

The **View Requests** task indicates the progress and completion of submitted changes and requests that you and other users make to the system.

Request status is available through the View Requests task from the main navigation tree. You can choose to filter your search for requests by user or service. To view pending requests, click **View Requests > View Pending Requests by User** or **View Requests > View Pending Requests by Service**. You can also choose to view the status of all pending and completed requests from the **View Requests > View All Requests** task.

Requests and activities

Requests initiate a workflow or a work order for manual service operations.

There are many different types of requests that can occur, such as requesting changes to accounts, adding and modifying users, and changing policies. Some requests might require the completion of an activity by another user, such as an approval or recertification. Other requests can be completed without any further actions.

Note: Requests that do not initiate a workflow, such as Orphan Account Requests, do not get displayed in the pending or completed requests.

Requests can involve several steps to complete. Each step might require different users to complete an action. You can view the status of a request by viewing pending requests or all requests that are both pending and completed.

Completed requests are requests that completed processing. The completion of a request does not mean that it was successful. Requests might fail, might complete with a warning message, or might be canceled while in a pending state.

Pending requests are requests that are submitted but are not finished. These requests might be in the process of running or might require the completion of a workflow activity, such as a recertification or approval activity.

Request states

When you view the status of a request, the request might be in one of several states.

The states of a request can be viewed only by the user who submitted the request. The following table provides a description of each request state.

Request state	Description
Not started	The request was not started.
In process	The request is running and is not waiting for any activity for which there is a participant.
Pending approval	The request requires approval, and no action is taken to complete the request.
Pending information	The request requires that an information provider completes a request for information (RFI) activity.
Pending response	The request requires that a responder complete a workflow activity, such as a work order or compliance alert.
Canceled	The request is canceled.
Successful	The request was completed successfully.

Table 108. Descriptions of the states of requests (continued)

Request state	Description
Completed with warning	The request was partially completed. A problem occurred, preventing the request from being successfully completed.
Failed	The request was not able to complete. No further activity can occur.

This section describes the workflow request status and its indicators and how the request status indicator works, including few examples.

Status

A status of a request is associated with several child requests or processes, and each child request has a status of its own. The status of the parent request depends on the status of the child requests.

Errors

An error occurs when a subsequent child request failed or was rejected. For example, when an incorrect URL is specified for reconciliation of the service or when an approver rejects a request.

Warnings

A warning occurs when one or more child requests failed. For example, you want to change passwords of five accounts simultaneously. However, even if one change password request failed and other four change password requests succeeded, the status of the parent request is Warning.

Note: A warning might also include activities that are marked as Terminated. For example, two approvers are involved in an approval workflow and none of them approve the request within the specified time period. Then the approval activity is marked as Terminated and the status of the parent request is Warning.

Success

A request is successful in one of the following situations:

- When all the child requests are successful
- When the primary child requests are successful

When the primary child requests are successful, it might also include approval activities that are marked as Approved. For example, two approvers are involved in an approval workflow and the first approver approves the request. In this case, the status of the approval activity is Approved, but the status of the parent request is Success.

Pending

A pending request occurs when one or more child requests are in a pending state. For example, you request to create an account that requires approval workflow. In this case, if the approval activity is pending, then the status of the parent request is also Pending.

Note: Pending requests might also include activities that are marked as Escalated. For example, a user requests an account on a service with an associated approval workflow that involves two approvers. If the first approver fails to approve the request within the specified time period, the status of the approval activity is Escalated. But the status of the parent request is Pending.

Viewing all requests

You can view all the requests that users submitted.

Before you begin



Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Use the **View All Requests** page to use various search criteria to find all requests are submitted to the system, regardless of their completion status.

View All Requests is only intended for users that have full, unrestricted access to the audit trail. There is no ACI checking in this view. Use caution when exposing this task in a user's view.

Procedure

1. From the navigation tree, select **View Requests > View All Requests**.
2. On the **View All Requests** page, complete these steps:
 - a) Select a request type from the list.
 - b) Select a time interval.
 - c) Optionally, click the icon () next to **More Search Criteria** to filter by status, date request was completed or submitted, service, user, or request ID.
 - d) Click **Search Requests** when you are done specifying search criteria.
3. To view the details of a request, click the request type. The information about the request is read-only.
4. Click the icon () below the **Process Data** section to view further information about the initial process data of the request.
5. On the **View All Requests** page, click the root structure to view the request details.
The information about the request is read-only.
6. Click **Close** to close the **View All Requests** page.
7. When you are done reviewing the requests, click **Close**.

Viewing pending requests of users

You can view those requests that are submitted by a user, but are not completed.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.


About this task

Use the **View Pending Requests by User** page to search by user information to find requests that are submitted to the system, but are not yet completed.

View Pending Requests by User is intended for the help desk administrators and managers that need to view the audit trail related to specific users. ACIs are only applied when initially searching for a user. ACIs are not applied to any of the request data shown as a result of selecting a user.

Procedure

1. From the navigation tree, select **View Requests > View Pending Requests by User**.
2. On the **View Pending Requests by User** page, click **Search** to specify a user in the **User name** field.
3. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Value** field, select an attribute from the **Attribute** list, and then click **Search**.
 - b) In the **Users** table, select the user whose requests you want to view.
 - c) Click **OK**.
4. Select the time period that you want to search. Specify a start date in the **Start Date** field and an end date in the **End Date** field, and then click **Search Requests**.

5. To view the details of a request, click the request type. The information about the request is read-only.
6. Click the icon () below the **Process Data** section to view further information about the initial process data of the request.
7. On the **View Pending Requests by User** page, click the root structure to view the request details. The information about the request is read-only.
8. Click **Close** to close the **View Pending Requests by User** page.
9. When you are done reviewing the pending requests of others, click **Close**.

Viewing all requests of users

You can view all the requests that a user submitted.

Before you begin


Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Use the **View All Requests by User** page to search by user information to find all requests that are submitted to the system, regardless of their completion status.

View All Requests by User is intended for the help desk administrators and managers that need to view the audit trail related to specific users. ACIs are only applied when initially searching for a user. ACIs are not applied to any of the request data shown as a result of selecting a user.

Procedure

1. From the navigation tree, select **View Requests > View All Requests by User**.
2. On the **View All Requests by User** page, click **Search** to specify a user in the **User name** field.
3. On the **Select a User** page, complete these steps:
 - a) Type information about the user in the **Value** field, select an attribute from the **Attribute** list, and then click **Search**.
 - b) In the **Users** table, select the user whose requests you want to view.
 - c) Click **OK**.
4. Select the time period that you want to search. Specify a start date in the **Start Date** field and an end date in the **End Date** field. Optionally, filter for request status in the **Status** field, and then click **Search Requests**.
5. To view the details of a request, click the request type. The information about the request is read-only.
6. Click the icon () below the **Process Data** section to view further information about the initial process data of the request.
7. On the **View All Requests by User** page, click the root structure to view the request details. The information about the request is read-only.
8. Click **Close** to close the **View All Requests by User** page.
9. When you are done reviewing the requests, click **Close**.

Viewing pending requests by service

You can view all pending requests that are submitted for a particular service.

Before you begin


Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Use the **View Pending Requests by Service** page to search by service information to find requests that are submitted to the system, but are not yet completed.

View Pending Requests by Service is intended for service and application owners that need to view the audit trail related to services they administer. ACIs are only applied when initially searching for a service. ACIs are not applied to any of the request data shown as a result of selecting a service.

Procedure

1. From the navigation tree, select **View Requests > View Pending Requests by Service**.
2. On the **View Pending Requests by Service** page, click **Search** to specify a service in the **Service name** field.
3. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Service information** field. Select a service type from the **Service Type** list and then click **Search**.
 - b) In the **Services** table, select the service whose requests you want to view.
 - c) Click **OK**.
4. Select the time period that you want to search. Specify a start date in the **Start Date** field and an end date in the **End Date** field and then click **Search Requests**.
5. To view the details of a request, click the request type. The information about the request is read-only.
6. Click the icon () below the **Process Data** section to view further information about the initial process data of the request.
7. On the **View Pending Requests By Service** page, click the root structure to view the request details. The information about the request is read-only.
8. Click **Close** to close the **View Pending Requests by Service** page.
9. When you are done reviewing the requests for a service, click **Close**.

Viewing all requests by service

You can view all the requests that are submitted for a particular service.

Before you begin


Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Use the **View All Requests by Service** page to search by service information to find all requests that are submitted to the system, regardless of their completion status.

View All Requests by Service is intended for service and application owners that need to view the audit trail related to services they administer. ACIs are only applied when initially searching for a service. ACIs are not applied to any of the request data shown as a result of selecting a service.

Procedure

1. From the navigation tree, select **View Requests > View All Requests by Service**.
2. On the **View All Requests by Service** page, click **Search** to specify a service in the **Service name** field.
3. On the **Select a Service** page, complete these steps:
 - a) Type information about the service in the **Service information** field, select a service type from the **Service Type** list, and then click **Search**.
 - b) In the **Services** table, select the service whose requests you want to view.
 - c) Click **OK**.
4. Select the time period that you want to search. Specify a start date in the **Start Date** field and an end date in the **End Date** field. Optionally, filter for request status in the **Status** field, and then click **Search Requests**.
5. To view the details of a request, click the request type. The information about the request is read-only.
6. Click the icon () below the **Process Data** section to view further information about the initial process data of the request.
7. On the **View All Requests By Service** page, click the root structure to view the request details. The information about the request is read-only.
8. Click **Close** to close the **View All Requests by Service** page.
9. When you are done reviewing the requests for a service, click **Close**.

Canceling pending requests

You can cancel requests that are not completed.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task


Pending requests are requests that are submitted to the system, but are not yet completed. When a pending request is canceled, the request is canceled. Any action items associated with the request are canceled and the request status is changed to canceled.

Note: When you cancel a request, the workflow is interrupted and is not fully processed.

Administrators can also choose to search for requests to cancel from the navigation tree by selecting **View Requests > View Pending Requests by Service** and **View Requests > View Pending Requests by User**.

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. From the main navigation tree, click **View Requests > View All Requests**.
2. On the **View All Requests** page, complete these steps:
 - a) Click the icon () next to **More Search Criteria**.
 - b) Under **Status**, clear all items except **Pending**.
 - c) Optionally, you can filter by date, service, and user to narrow your options.
 - d) Click **Search Requests** to display a list of pending requests.
 - e) Select the request that you would like to cancel, and click **Cancel Request**.

3. On the **Confirm** page, click **Cancel Requests**.

4. On the **Success** page, click **Close**.

Results

When a request is canceled, an email notification is sent to the requester, provided that:

- Notification is not disabled. (By default, notification is enabled.)
- The email server and other properties are configured in the `enroleMail.properties` file.
- The requester has a valid email address.

The email notification lists the person who canceled the request, the date and time that the request was canceled, and the reason that the request was canceled.

Related tasks

[“Manually applying the email notification template changes for canceling a request” on page 963](#)

You can use the **Workflow Notification Properties** page to manually add information about canceling a request to the email notification template. When you install the IBM Security Identity Manager Fix Pack 6.0.0.3, the email notification template content that includes information about canceling a request is not automatically applied. The template changes that are available with Fix Pack 6.0.0.3 are not automatically applied so that the installation process does not overwrite any custom changes that you might have made to the email templates.

Related reference

[“Request for information \(RFI\) states” on page 992](#)

Request for information (RFI) activities have several states.

Index

A

access

- clearing from service instance [747](#)
- configuration, namespace [856](#)
- configuration, query items [856](#)
- configuration, query subjects [856](#)
- deleting [621](#)
- management [620](#)
- overview [620](#)
- requesting [620](#)
- type, creating, based on role [689](#)
- viewing [621](#)

access audit

- history, reports [788](#)
- namespace [852](#)
- query items [853](#)
- query subjects [852](#)
- report models [785](#)

access audit (Deprecated)

- namespace [847](#)
- query items [849](#)
- query subjects [847](#)

access control

- overview [656](#)
- reports [779](#)

access control items

- administrator domains [645](#)
- changing [663](#)
- creating [663](#)
- default [657](#)
- definition [656](#)
- deleting [664](#)

access data

- CSV
 - formats [670](#), [706](#), [759](#)
 - values [670](#), [706](#), [759](#)

access definition

- filters [787](#)
- report, base icon URL path [794](#)

access information

- configuring for a group [764](#)
- configuring for a role [680](#)
- configuring for a service [709](#)

access reports, defining [781](#)

account

- audit history, reports [789](#)
- audit, namespace [807](#)
- audit, query items [808](#)
- audit, query subjects [807](#)
- changing details [616](#)
- configuration, namespace [810](#)
- configuration, query items [812](#)
- defaults, adding to service [732](#)
- defaults, changing [733](#)
- defaults, global [735](#)
- defaults, management [731](#)

account (*continued*)

- defaults, removing from service [734](#)
- management on a service [721](#)
- status filters [787](#)
- types [614](#)
- viewing details [616](#)

account information

- modifying [724](#)

account information, editing [724](#)

account recertification

- displaying status [744](#)
- overview [744](#)

accounts

- active, inactive [614](#)
- adding default values [732](#)
- assigning users [728](#)
- changing [724](#)
- changing defaults in a service [724](#)
- deleting [617](#), [725](#)
- displaying [721](#)
- editing [724](#)
- modifying [724](#)
- orphan [730](#)
- overview [614](#), [721](#)
- policy enforcement [924](#)
- recertification overview [744](#)
- recertification, displaying status [744](#)
- report models [784](#)
- requesting [615](#), [722](#)
- restoring [619](#), [727](#)
- suspending [618](#), [726](#)
- viewing [616](#)

ACIs

- administrator domains [645](#)
- changing [663](#)
- creating [663](#)
- default [657](#)
- deleting [664](#)
- report filters [902](#)
- reports [901](#)

activities

- administration overview [985](#)
- approval [991](#), [992](#)
- assigning [988](#)
- compliance [994](#)
- compliance alert [994](#)
- deferring compliance [995](#)
- definition [985](#)
- delegate [626](#), [987](#)
- delegating [626](#)
- delegating, changing schedule [987](#)
- delegating, creating schedule [987](#)
- delegating, overview [626](#), [987](#)
- delegating, stopping [988](#)
- locking [986](#)
- overview [626](#), [987](#)
- recertification [933](#), [995](#)

activities (*continued*)
request for information [992, 993](#)
RFI [993](#)
unlocking [986](#)
viewing [985](#)
viewing user [986](#)
work order [993](#)

activity reminder in workflow [960](#)

administration
creating nodes, organizational tree [647](#)
organization [645](#)

administrator
access restriction [780](#)
domains, ACIs [645](#)

adoption
changing policies [907](#)
creating policies [904](#)
deleting policies [907](#)
orphan account policies [908](#)
policies
attribute matching [908](#)
policies overview [903](#)
policies, JavaScript examples [905](#)
policy reconciliation [908](#)
writing policies [905](#)

advanced tuning [20](#)

aliases [607](#)

application interfaces
management [15](#)

approvals
activities [991](#)
completing [992](#)
states [991](#)

approveSoDViolation [944](#)

assignment attributes
defining for existing role [678](#)
defining when creating role [677](#)
setting values [679](#)

attribute matching [908](#)

attributes
defining assignment for existing role [678](#)
defining assignment for new role [677](#)
mapping [860, 883](#)
unmapping [883](#)

audit
and security, generating [871](#)
history report [788](#)
report, example [878](#)

authentication
IBM Cognos reports [776](#)

authorization
IBM Cognos reports [776](#)

C

cancel request
notification template [963](#)

changelog [898](#)

child roles
adding to parent role [687](#)
managing [686](#)
removing from parent role [688](#)

Cognos Analytics installation [772](#)

comma-separated value file

comma-separated value file (*continued*)
reconciliation [720](#)

compliance alert rules, configuring [742](#)

connection mode
changing [704](#)
enabling [700](#)

console reports
IBM Security Identity Manager [868](#)

content store, creation [773](#)

CSV
data values, formats [670, 706, 759](#)

CSV file
reconciliation [720](#)

custom reports
creating [873](#)
generating [875](#)
shared access objects [876](#)

custom tables, adding [862](#)

custom tasks
changing [655](#)
changing task parameters [655](#)
deleting [656](#)
managing [470](#)

customization
model [862](#)
password age rules [922](#)
password rules
adding customized password generator [919](#)
adding customized rule [918](#)
customized rules and generator [919](#)
report banner [894](#)
reports [872](#)

D

dashboard
IBM Security Identity Manager environment [790](#)

data source
IBM Security Identity Manager Cognos reports [775](#)

data synchronization
creating a schedule [896](#)
deleting a schedule [897](#)
modifying a schedule [897](#)
overview [894, 895](#)
synchronizing data immediately [896](#)

db2admin
changing password [644](#)

db2inst1 [643](#)

default values, accounts [732](#)

define base icon URL path
access definition report [794](#)

delegation schedules
changing [987](#)
creating [987](#)
deleting [988](#)

domain administrator, creating [646](#)

draft provisioning policies [929](#)

drill-through reports [776](#)

E

email response objects [30](#)
enabling connection mode [700](#)

- entities
 - mapping [860](#)
 - mapping attributes [860](#)
- entitlements
 - report filters [789](#)
- escalation
 - period in workflow [961](#)
- event log
 - view [13](#)
- events
 - SNMP [29](#)
- example
 - accounts, filters [890](#)
 - audit report check-in [878](#)
 - checking out shared access credentials [876](#)
 - filters [891](#)
 - person and organization roles [891](#)
 - persons and account, filters [892](#)
 - role and shared access entitlement [879](#)

F

- filters
 - access definition [787](#)
 - account status [787](#)
 - accounts [890](#)
 - custom reports [890](#)
 - entitlements report [789](#)
 - persons and account [892](#)
 - separation of duty policy definition [791](#)
 - services report [792](#)
- fix pack, installation [7](#)
- form designer
 - constraints [515](#)
 - control types [510](#)
 - interface description [507](#)
 - properties [515](#)
- form templates
 - modifying [507](#), [510](#), [515](#)
- forms
 - customizing [507](#), [510](#), [515](#)
- Framework manager
 - configuration [773](#)
 - IBM Cognos [770](#)
 - installation [772](#)

G

- global account defaults [735](#)
- globalization, language support [782](#)
- groups
 - access information [764](#)
 - adding members [755](#)
 - administration overview [753](#)
 - configuring manual service type [718](#)
 - creating [753](#)
 - defining access on [763](#)
 - deleting [762](#)
 - enabling automatic membership [767](#)
 - exporting access data [760](#)
 - importing access data [761](#)
 - modifying attributes [758](#)
 - recertifying access on [766](#)

- groups (*continued*)
 - removing members [756](#)
 - viewing members [754](#)

H

- hosts
 - files [21](#)

I

- IBM Cognos
 - components [861](#)
 - connection [770](#)
 - installation prerequisites, report models [770](#)
 - objects, report models [783](#)
 - prerequisites, report models [770](#)
 - report server, software requirements [771](#)
 - reporting framework [770](#)
- IBM Security Identity Manager
 - Cognos reports troubleshooting [865](#)
 - Cognos reports, data source [775](#)
 - console reports [868](#)
- identities [909](#)
- identity
 - creating policies [911](#)
 - definition [909](#)
 - deleting policies [913](#)
 - policies [908](#)
 - policies, changing [912](#)
 - policies, creating [911](#)
 - policies, deleting [913](#)
 - policies, overview [908](#)
 - policies, script [910](#)
- Incremental Data Synchronizer
 - changelog [898](#)
 - overview [898](#)
 - starting [899](#)
 - tuning [899](#)
- ISIM Environment dashboard
 - editing [774](#)
 - refresh interval [774](#)
- itimuser
 - changing password [643](#)

J

- JOIN conditions, design reports [892](#)
- join directive [923](#)

L

- language preferences, setting [783](#)
- language support, globalization [782](#)
- LDAP
 - creating users [778](#)
- LDAP namespace
 - configuration [777](#)
- ldapdb2 [643](#)
- ldapdb2, changing password [644](#)
- lmi_security.protocol [20](#)
- lmi.security.ciphers [20](#)
- log response objects [31](#)

- login
 - administration [629](#)
 - overview [629](#)
 - setting maximum attempts [629](#)
- logs [31](#)

M

- management
 - hosts files [21](#)
- management, account defaults [731](#)
- management, reconciliation schedules [711](#)
- manual connection mode
 - creating a service [698](#)
- manual services
 - changing [705](#)
 - creating [701](#)
- members, adding [780](#)

N

- namespace
 - access audit [852](#)
 - access audit (Deprecated) [847](#)
 - access configuration [856](#)
 - account audit [807](#)
 - account configuration [810](#)
 - provisioning policy audit [819](#)
 - provisioning policy configuration [821](#)
 - recertification audit [795](#)
 - recertification configuration [801](#)
 - report models [783](#)
 - role audit [824](#)
 - role configuration [826](#)
 - separation of duty audit [831](#)
 - separation of duty configuration [836](#)
 - service audit [844](#)
 - user configuration [838](#)
- node tree
 - administering [645](#)
 - changing [648](#)
 - creating [647](#)
 - deleting [648](#)
- notification
 - escalation in workflow [960](#)
 - in workflow, disabling [962](#)
 - in workflow, enabling [962](#)
- notification for passwords [636](#)
- notification template
 - cancel request [963](#)
- notifications [29–31](#)

O

- object
 - email [30](#)
 - log [31](#)
- objects [30, 31](#)
- organization
 - administration [645](#)
 - changing a node [648](#)
 - creating a node [647](#)
 - deleting a node [648](#)

- organization (*continued*)
 - node tree [645](#)
- organizational roles
 - access information [680](#)
 - adding users to membership [683](#)
 - administration [667](#)
 - assignments [676](#)
 - child, adding to parent role [687](#)
 - child, managing [686](#)
 - child, removing from parent role [688](#)
 - classifying [673](#)
 - creating [668](#)
 - creating access type [689](#)
 - deleting [682](#)
 - displaying role-based access [675](#)
 - exporting access data [670](#)
 - importing access data [671](#)
 - managing users as members [682](#)
 - modifying [669](#)
 - overview [667](#)
 - removing users from membership [685](#)
 - specifying owners [674](#)
- orphan accounts
 - account reconciliation [908](#)
 - making [730](#)
 - overview [730](#)
- overview
 - data synchronization [894](#)
 - format [769](#)
 - incremental data synchronizer [898](#)
 - report data synchronization utility [899](#)
 - reports [769](#)

P

- packages, publishing [861](#)
- parameter enforcement rules [924](#)
- password
 - policies [913](#)
- password age rules
 - configuration [921](#)
- password policies
 - changing [916](#)
 - creating [914](#)
 - definition [913](#)
 - deleting [918](#)
- password policy
 - adding targets [915](#)
 - changing rules [917](#)
 - changing targets [917](#)
 - creating rules [915](#)
- password rules, customized logic [919](#)
- password strength rules [637, 913](#)
- passwords
 - adding minimum password age [922](#)
 - administration of system settings [631](#)
 - administration overview [631](#)
 - changing [622, 624](#)
 - changing for db2admin [644](#)
 - changing for itimuser [643](#)
 - changing for ldapdb2 [644](#)
 - configuring administrator-defined questions for [641](#)
 - configuring minimum password age [921](#)
 - configuring user-defined questions for [641](#)

- passwords *(continued)*
 - creating strength rules [637](#)
 - customized rules
 - adding customized logic [919](#)
 - adding customized password generator [919](#)
 - adding customized rule [918](#)
 - enabling editing [633](#)
 - enabling resetting [631](#)
 - excluding [642](#)
 - expiration [629](#)
 - forgotten [640](#)
 - hiding generated [632](#)
 - management [622](#)
 - resetting [623](#), [625](#)
 - setting on user creation [635](#)
 - setting retrieval expiration [635](#)
 - setting the notification method [636](#)
 - synchronization [634](#)
- pending requests
 - viewing by service [1001](#)
 - viewing by users [999](#)
- person and organization roles filters [891](#)
- person profiles [607](#)
- policies
 - adoption
 - changing [907](#)
 - creating [904](#)
 - deleting [907](#)
 - approving [952](#)
 - changing identity [912](#)
 - creating identity [911](#)
 - definition [903](#)
 - deleting identity [913](#)
 - enforcing [743](#)
 - identity [908](#)
 - password
 - changing [916](#)
 - creating [914](#)
 - deleting [918](#)
 - provisioning
 - changing [926](#)
 - creating [926](#)
 - deleting [929](#)
 - preview [927](#)
 - recertification
 - changing [939](#)
 - creating [936](#)–[938](#)
 - default notifications [940](#)
 - deleting [940](#)
 - results [935](#)
 - separation of duty
 - ACI operations [943](#)
 - changing [948](#)
 - creating [947](#)
 - default ACI [943](#)
 - deleting [950](#)
 - disabled [942](#)
 - enabled [942](#)
 - enabling the portfolio task [946](#)
 - evaluating [949](#)
 - exemptions [945](#), [951](#)
 - revoking exemptions [953](#)
 - violations [945](#), [951](#)
 - service selection

- policies *(continued)*
 - service selection *(continued)*
 - change [955](#)
 - create [955](#)
 - delete [956](#)
 - overview [954](#)
 - policy enforcement
 - compliance alerts [737](#)
 - configuring enforcement [740](#)
 - definition [924](#)
 - overview [737](#)
 - policy enforcement actions [737](#)
 - policy enforcement alerts [737](#)
 - scheduling on service [743](#)
 - policy evaluation [945](#)
 - policy management [903](#)
 - portfolio tasks [946](#)
 - provisioning
 - policies [923](#)
 - report models [784](#)
 - provisioning policies
 - changing [926](#)
 - creating [926](#)
 - definition [923](#)
 - deleting [929](#)
 - draft
 - change [929](#)
 - commit [929](#)
 - create [928](#)
 - managing by role [929](#)
 - parameter enforcement rules [924](#)
 - preview [927](#)
 - provisioning policies draft, creating [928](#)
 - provisioning policy audit
 - namespace [819](#)
 - query items [820](#)
 - query subjects [819](#)
 - provisioning policy configuration
 - namespace [821](#)
 - query items [822](#)
 - query subjects [821](#)

Q

- query items
 - access audit [853](#)
 - access audit (Deprecated) [849](#)
 - access configuration [856](#)
 - account audit [808](#)
 - account configuration [812](#)
 - provisioning policy audit [820](#)
 - provisioning policy configuration [822](#)
 - recertification audit [796](#)
 - recertification configuration [803](#)
 - role audit [824](#)
 - role configuration [827](#)
 - separation of duty audit [832](#)
 - separation of duty configuration [837](#)
 - service audit [845](#)
 - user configuration [839](#)
- query studio [770](#)
- query subjects
 - access audit [852](#)
 - access audit (Deprecated) [847](#)

- query subjects (*continued*)
 - access configuration [856](#)
 - account audit [807](#)
 - account configuration [810](#)
 - provisioning policy audit [819](#)
 - provisioning policy configuration [821](#)
 - recertification audit [795](#)
 - recertification configuration [801](#)
 - role audit [824](#)
 - role configuration [826](#)
 - separation of duty audit [831](#)
 - separation of duty configuration [836](#)
 - service audit [844](#)
 - user configuration [838](#)

R

- recertification
 - account [744](#)
 - activities [933](#)
 - completing [995](#)
 - message templates [933](#)
 - notification [933](#)
 - overview [995](#)
 - report models [784](#)
 - schedule [933](#)
- recertification audit
 - namespace [795](#)
 - query items [796](#)
 - query subjects [795](#)
- recertification configuration
 - namespace [801](#)
 - query items [803](#)
 - query subjects [801](#)
- recertification definition
 - access [791](#)
 - account [791](#)
 - subreports [791](#)
 - user [791](#)
- recertification policies
 - changing [939](#)
 - creating [936–938](#)
 - default notifications [940](#)
 - deleting [940](#)
 - overview [930](#)
 - results [935](#)
- reconciliation
 - changing a schedule [716](#)
 - creating a schedule [715](#)
 - deleting a schedule [717](#)
 - deleting reconciliation schedule [717](#)
 - managing schedules [711](#)
 - manual service overview [718](#)
 - overview [711, 712](#)
 - reconciling accounts immediately [714, 719](#)
- references
 - mapping entities [860](#)
 - security configuration [782](#)
- regular expression notation, searching [872](#)
- relationship
 - creating [861](#)
 - modifying [861](#)
 - with existing tables, creating [863](#)
- reminder interval in workflow [961](#)

- removing account defaults [734](#)
- report
 - server execution mode [773](#)
 - shared access entitlement creation [879](#)
- report banner customization [894](#)
- report data synchronization utility
 - overview [899](#)
 - run [900](#)
 - running [900](#)
 - troubleshooting errors [900](#)
- report generation [864](#)
- report models
 - access audit [785](#)
 - accounts [784](#)
 - IBM Cognos objects [783](#)
 - provisioning [784](#)
 - recertification [784](#)
 - roles [784](#)
 - separation of duty [785](#)
 - services [785](#)
 - users [785](#)
- report package
 - defining access [781](#)
 - importing [774](#)
- report parameters and descriptions
 - access approval and rejection [785](#)
 - audit, account [785](#)
 - noncompliant account [785](#)
 - shared access, entitlements by owner [785](#)
 - shared access, entitlements by role [785](#)
- report studio [770](#)
- reporting framework
 - reporting model [770](#)
 - static reports [770](#)
- reports
 - access audit history [788](#)
 - access control [779](#)
 - access control items [901, 902](#)
 - account audit history [789](#)
 - ACI [901](#)
 - adhocreporting.properties [894](#)
 - audit and security [871](#)
 - audit history report [788](#)
 - configuration files [894](#)
 - custom [875](#)
 - custom reports [890](#)
 - customization [872](#)
 - DatabaseFunctions.conf [894](#)
 - define access [781](#)
 - delete custom templates [875](#)
 - deleting custom templates [875](#)
 - designing, JOIN conditions [892](#)
 - drill-through [776](#)
 - filters [890](#)
 - format [769](#)
 - generate [870, 875](#)
 - generating [870, 871](#)
 - mapping attributes [883](#)
 - modify custom templates [874](#)
 - modifying custom templates [874](#)
 - overview [769](#)
 - requests [870](#)
 - schema mapping [882](#)
 - separation of duty policy violation [792](#)

- reports (*continued*)
 - services [871](#)
 - synchronizing data [895–897](#)
 - templates [872](#)
 - types [868](#)
 - unmapping attributes [883](#)
 - user and accounts [870](#)
 - user input filters [886](#)
 - user input values [884](#)
 - user recertification history [793](#)
- request for information
 - completing [993](#)
 - overview [992](#)
 - states [992](#)
- requests
 - accounts [722](#)
 - cancelling [1002](#)
 - definition [988](#), [991](#), [997](#)
 - generating [870](#)
 - overview [988](#), [991](#), [997](#)
 - states [997](#)
 - view all [998](#)
 - view all by service [1001](#)
 - view pending [999](#)
 - view pending by service [1001](#)
 - viewing [997](#)
 - viewing all by service [1001](#)
 - viewing all submitted by user [1000](#)
- response objects
 - email [30](#)
 - log [31](#)
 - SNMP [29](#)
- restoration, accounts [727](#)
- retry blocked request [695](#)
- RFI overview [992](#)
- role audit
 - namespace [824](#)
 - query items [824](#)
 - query subjects [824](#)
- role configuration
 - namespace [826](#)
 - query items [827](#)
 - query subjects [826](#)
- role custom report templates
 - creating [881](#)
- roles
 - adding users to membership [683](#)
 - assignment attributes [676](#)
 - child, adding to parent role [687](#)
 - child, managing [686](#)
 - child, removing from parent role [688](#)
 - classifying [673](#)
 - creating [668](#), [780](#)
 - creating access type [689](#)
 - deleting [682](#)
 - displaying role-based access [675](#)
 - exporting access data [670](#)
 - hierarchies [668](#)
 - importing access data [671](#)
 - managing users as members [682](#)
 - modifying [669](#)
 - removing users from membership [685](#)
 - report models [784](#)
 - specifying owners [674](#)

- rules
 - compliance alert, configuring [742](#)
 - configuring, password [921](#)
 - customized logic, password [919](#)
 - customizing password age rule [922](#)
 - customizing, password [918](#)

S

- sample workflow
 - access owner approval [983](#)
 - approval loop [973](#)
 - mail activity [975](#)
 - manager approval of accounts [964](#)
 - multiple approvals [965](#)
 - multiple approvals with loop [968](#)
 - packaged approval [979](#)
 - RFI and subprocess [971](#)
 - sequential approval for user recertification [976](#)
- scenario
 - adding custom tables [862](#)
 - creating a relationship [863](#)
 - customize model [862](#)
 - generating report [864](#)
- schedules, delegating [626](#)
- schema mapping
 - reports [882](#)
- script, identity policy [910](#)
- search, regular expression notation [872](#)
- security administration overview [651](#)
- security configuration references [782](#)
- security layer configuration [776](#)
- separation of duty audit
 - namespace [831](#)
 - query items [832](#)
 - query subjects [831](#)
- separation of duty configuration
 - namespace [836](#)
 - query items [837](#)
 - query subjects [836](#)
- separation of duty policies
 - ACI operations [943](#)
 - changing [948](#)
 - creating [947](#)
 - default ACI [943](#)
 - definition, filters [791](#)
 - deleting [950](#)
 - disabled policy [942](#)
 - enabled policy [942](#)
 - enabling the portfolio task [946](#)
 - evaluating [949](#)
 - exemptions [945](#), [951](#)
 - exemptions, revoking [953](#)
 - overview [942](#)
 - violation, reports [792](#)
 - violations [945](#), [951](#)
 - violations, approving [952](#)
- separation of duty report models [785](#)
- server monitoring
 - management [10](#)
- service
 - access information [709](#)
 - changing [703](#)
 - clearing access [747](#)

- service (*continued*)
 - creating [696](#)
 - creating, manual connection mode [698](#)
 - managing access [746](#)
 - managing accounts on [721](#)
 - managing groups [746](#)
 - status [695](#)
 - tagging [736](#)
- service audit
 - namespace [844](#)
 - query items [845](#)
 - query subjects [844](#)
- service selection policies
 - changing [955](#)
 - creating [955](#)
 - deleting [956](#)
 - overview [954](#)
- service tags, adding [737](#)
- service template, adding tag attribute [737](#)
- service types
 - default [693](#)
 - overview [693](#)
- services
 - deleting [710](#)
 - exporting access data [707](#)
 - generating [871](#)
 - importing access data [708](#)
 - manual, changing [705](#)
 - manual, creating [701](#)
 - policy enforcement [924](#)
 - reconciling accounts [714–717](#), [719](#)
 - report filters [792](#)
 - report models [785](#)
 - viewing all requests [1001](#)
 - viewing pending requests [1001](#)
- set of tasks [651](#)
- setup, user authentication [777](#)
- shared access configuration [773](#)
- shared access credentials, example [876](#)
- shared access objects
 - custom reports [876](#)
- simple network management protocol (SNMP) [29](#)
- snapshots, management [24](#)
- SNMP monitoring
 - management [14](#)
- software requirements
 - IBM Cognos report server [771](#)
- sponsored accounts
 - changing passwords [624](#)
 - resetting passwords [625](#)
- static reports, IBM Cognos models [770](#)
- static routes
 - management [22](#)
- support files, management [26](#)
- suspension, accounts [726](#)
- syslog [31](#)
- system audit events
 - configuration [28](#)
- system users
 - db2admin [643](#)
 - db2inst1 [643](#)
 - default [643](#)
 - itimuser [643](#)
 - ldapdb2 [643](#)

- system users (*continued*)
 - passwords [643](#)

T

- tag attribute, adding [737](#)
- tagging, service [736](#)
- tags, adding to service [737](#)
- tasks
 - managing custom [470](#)
- TCR reports
 - migrating to IBM Cognos reports [862](#)
 - migration to IBM Cognos reports [862](#)
- templates, reports [872](#)
- troubleshooting
 - IBM Security Identity Manager Cognos reports [865](#)
 - report data synchronization utility [900](#)
- tuning [899](#)
- types, reports [868](#)

U

- user accounts
 - deleting [617](#)
 - requesting [615](#)
 - restoring [619](#)
 - suspending [618](#)
- user activities, viewing [986](#)
- user and accounts, generating [870](#)
- user authentication
 - setup [777](#)
- user configuration
 - namespace [838](#)
 - query items [839](#)
 - query subjects [838](#)
- user input
 - filters, reports [886](#)
 - values, reports [884](#)
- user passwords
 - changing [622](#), [624](#)
 - resetting [623](#), [625](#)
- user profiles
 - changing [609](#)
 - creating [608](#)
 - deleting [610](#)
 - user information, changing [609](#)
- user recertification
 - history, reports [793](#)
- users
 - adding to membership of role [683](#)
 - administration overview [607](#)
 - assigning to accounts [728](#)
 - creating [608](#)
 - delegating activities [626](#)
 - deleting [610](#)
 - deleting access [621](#)
 - managing as members of role [682](#)
 - removing from membership of role [685](#)
 - report models [785](#)
 - requesting access [620](#)
 - requesting accounts for [615](#)
 - restoring [612](#)
 - suspending [612](#), [613](#)

users (*continued*)
transferring [611](#)
viewing access [621](#)
viewing accounts for [616](#)
viewing activities for [986](#)
viewing all requests submitted [1000](#)

V

view
changing [652](#)
changing custom tasks [655](#)
creating [651](#)
deleting [652](#)
deleting custom tasks [656](#)
virtual appliance
system settings, manage [5](#)
virtual appliance dashboard
administrator settings, manage [24](#)
date and time, manage [23](#)
firmware settings, management [6](#)
manage about page [7](#)
manage CPU usage [9](#)
manage memory usage [8](#)
manage storage usage [9](#)
restart or shutdown [32](#)
update history, manage [5](#)
viewing cluster status [4](#)
viewing disk usage [1](#)
viewing IP addresses [2](#)
viewing licensing [6](#)
viewing middleware monitor widget [3](#)
viewing notifications [2](#)
viewing partition information [1](#)
viewing quick links [3](#)
viewing server control [3](#)

W

web gateway configuration [773](#)
web server configuration [773](#)
work order
states [993](#)
work orders
activities [993](#)
completing [993](#)
workflows
adding [957](#)
changing [958](#)
deleting [958](#)
disable [962](#)
enabling [962](#)
escalation period [961](#)
mail activity template [959](#)
management overview [957](#)
notification [962](#), [963](#)
notification, activity reminder [960](#)
notification, escalation [960](#)
reminder content in workflow [961](#)
reminder interval [961](#)
sample, access owner approval [983](#)
sample, approval loop [973](#)
sample, mail activity [975](#)

workflows (*continued*)
sample, manager approval of accounts [964](#)
sample, multiple approvals [965](#)
sample, multiple approvals with loop [968](#)
sample, packaged approval [979](#)
sample, RFI and subprocess [971](#)
sample, sequential approval for user recertification [976](#)
template [963](#)

