Contents

Introduction .............................................................. xi

Chapter 1. What's New? ................................................. 1
New features in version 10.2.1 ....................................... 1
  New security standards in IBM Cognos BI ....................... 1
  Store reports in an external object store ......................... 1
New Features in Version 10.2.0 ..................................... 1
  Option to initialize Cognos Configuration from a different file . 2
  Option to view the status of silent installations on the screen .. 2
  Predefined LDAP configurations .................................. 2
New Features in Version 10.1.0 ..................................... 2
  Access to Software Development Kit Installation and Configuration Guide ........................................... 2
Changed Features in Version 10.1.0 ............................... 3
  Default Installation Location and Web Alias .................... 3
  PowerPlay Batch Administration ................................ 3
  IBM Cognos Go! Dashboard is Merged with Features from IBM Cognos Viewer into One User Interface .... 3
  Enhanced Support for Authentication Using a RACF Provider . 3
  Secure Access When Monitoring System Metrics Externally .. 3
Removed Features in Version 10.1.0 ............................ 4
  Managing Memory for the IBM Cognos Service .................. 4

Chapter 2. Distribution options .................................... 5
Product components .................................................. 5
  Server components .............................................. 5
  Optional server components .................................. 7
  Migration Components .......................................... 8
  Client Components ............................................. 8
  Required database components ................................ 8
Distributing components ............................................. 9
  All server components on one computer ......................... 10
  Gateways on separate computers ................................ 10
  Application Tier Components and Content Managers on separate computers ............................................. 11
  Installing 64-bit versions of IBM Cognos BI products ......... 13
IBM Cognos PowerPlay with Other IBM Cognos Products ....... 14
  IBM Cognos Series 7 Products That Can Be Migrated to IBM Cognos PowerPlay ................................. 14
  IBM Cognos Products That Interoperate with IBM Cognos PowerPlay ................................................. 16
  IBM Cognos Series 7 content that can be recreated in IBM Cognos Business Intelligence ....................... 19

Chapter 3. Preparing to install ..................................... 21
Review the Release Notes Before You Install ..................... 21
Review supported environments ..................................... 21
Verify system requirements ........................................... 22
  Memory settings .................................................. 23
Java requirements .................................................... 24
Review the Default Port Settings for IBM Cognos Business Intelligence ............................................. 25
Guidelines for creating the content store .......................... 27
  Suggested settings for creating the content store in DB2 on Linux, Windows, and UNIX operating systems . 28
  Suggested settings for creating the content store in DB2 on z/OS ......................................................... 30
  Suggested settings for creating the content store in Oracle ................................................................. 30
  Suggested settings for creating the content store in Microsoft SQL Server ............................................. 31
  Suggested settings for creating the content store in IBM Informix Dynamic Server ............................... 32
  Suggested settings for creating the content store in Sybase .............................................................. 32
Configure a User Account or Network Service Account for IBM Cognos Business Intelligence ................... 33
Configure Web Browsers .............................................. 34
<table>
<thead>
<tr>
<th>Chapter 7. Installing the Cognos PowerPlay samples</th>
<th>139</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a data source connection to the PowerCube samples</td>
<td>139</td>
</tr>
<tr>
<td>Importing the Cognos PowerPlay samples</td>
<td>140</td>
</tr>
<tr>
<td>Testing a sample report</td>
<td>140</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 8. Configuring IBM Cognos Components to Use an Authentication Provider</th>
<th>141</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Anonymous Access</td>
<td>142</td>
</tr>
<tr>
<td>Restrict User Access to the Cognos Namespace</td>
<td>142</td>
</tr>
<tr>
<td>Configuring IBM Cognos Components to Use Active Directory Server</td>
<td>143</td>
</tr>
<tr>
<td>Configure an Active Directory Namespace</td>
<td>144</td>
</tr>
<tr>
<td>Make Custom User Properties for Active Directory Available to IBM Cognos Components</td>
<td>145</td>
</tr>
<tr>
<td>Enabling Secure Communication to the Active Directory Server</td>
<td>146</td>
</tr>
<tr>
<td>Include or Exclude Domains Using Advanced Properties</td>
<td>146</td>
</tr>
<tr>
<td>Enable single signon between Active Directory Server and IBM Cognos components</td>
<td>148</td>
</tr>
<tr>
<td>Configuring IBM Cognos to Use IBM Cognos Series 7 Namespace</td>
<td>151</td>
</tr>
<tr>
<td>Configure an IBM Cognos Series 7 Namespace</td>
<td>152</td>
</tr>
<tr>
<td>Enabling Secure Communication to the Directory Server Used by the IBM Cognos Series 7 Namespace</td>
<td>153</td>
</tr>
<tr>
<td>IBM Cognos Series 7 Namespaces and the IBM Cognos Series 7 Trusted Signon Plug-in</td>
<td>153</td>
</tr>
<tr>
<td>Configuring IBM Cognos to Use a Custom Authentication Provider</td>
<td>154</td>
</tr>
<tr>
<td>Configure a Custom Authentication Namespace</td>
<td>156</td>
</tr>
<tr>
<td>Hide the Namespace from Users During Login</td>
<td>156</td>
</tr>
<tr>
<td>Configuring IBM Cognos Components to Use LDAP</td>
<td>157</td>
</tr>
<tr>
<td>LDAP Mapping</td>
<td>157</td>
</tr>
<tr>
<td>Configure an LDAP Namespace</td>
<td>158</td>
</tr>
<tr>
<td>Configure an LDAP namespace for Active Directory Server</td>
<td>159</td>
</tr>
<tr>
<td>Configure an LDAP Namespace for IBM Directory Server</td>
<td>161</td>
</tr>
<tr>
<td>Configure an LDAP Namespace for Novell Directory Server</td>
<td>163</td>
</tr>
<tr>
<td>Configure an LDAP Namespace for Oracle Directory Server</td>
<td>165</td>
</tr>
<tr>
<td>Make Custom User Properties for LDAP Available to IBM Cognos Components</td>
<td>167</td>
</tr>
<tr>
<td>Enable Secure Communication to the LDAP Server</td>
<td>168</td>
</tr>
<tr>
<td>Enabling Single Signon Between LDAP and IBM Cognos Components</td>
<td>169</td>
</tr>
<tr>
<td>Replace operation</td>
<td>169</td>
</tr>
<tr>
<td>Configure IBM Cognos components to use CA SiteMinder</td>
<td>170</td>
</tr>
<tr>
<td>Configuring the SiteMinder namespace</td>
<td>171</td>
</tr>
<tr>
<td>Configuring IBM Cognos to Use a RACF Provider for Authentication</td>
<td>173</td>
</tr>
<tr>
<td>Configuring a RACF Namespace</td>
<td>173</td>
</tr>
<tr>
<td>Enabling single signon between RACF and IBM Cognos</td>
<td>174</td>
</tr>
<tr>
<td>Configure IBM Cognos to use SAP</td>
<td>174</td>
</tr>
<tr>
<td>Configure an SAP Namespace</td>
<td>175</td>
</tr>
<tr>
<td>Enable Single Signon Between SAP and IBM Cognos</td>
<td>176</td>
</tr>
<tr>
<td>Delete an Authentication Provider</td>
<td>177</td>
</tr>
</tbody>
</table>
Chapter 9. Configuration options

Start IBM Cognos Configuration ........................................ 179
Changing the version of Java used by IBM Cognos BI components ......... 180
Back up existing IBM Cognos information ................................ 180
Change your Java version ...................................................... 181
Changing Default Configuration Settings .................................. 182
Change Default User and Password for Cognos Content Database ............ 183
Port and URI Settings ......................................................... 184
Configuring Cryptographic Settings ....................................... 186
IBM Cognos Application Firewall ......................................... 190
Encrypt Temporary File Properties ....................................... 192
Configure the Gateway to Use a Namespace ................................ 193
Enable and Disable Services .................................................. 193
Configuring fonts .................................................................. 194
Change the default font for PDF reports ................................... 196
Configure Embedded Fonts for PDF Reports ................................ 197
Saved Report Output .............................................................. 197
Changing the Location of Temporary Report Output .......................... 199
Use an external object store for report output .................................. 200
Verify access to the external object store .................................... 201
Customizing Server-side Printing for UNIX and Linux Platforms ............. 201
Change the notification database .............................................. 202
Change the Connection Properties for the Notification Database ........... 203
Create a New Content Store Using Cognos Content Database .................. 203
Change the security standard compliance for IBM Cognos trust stores ....... 204
Restore non-NIST SP800-131a standard certificates to IBM Cognos trust stores ... 204
Remove non-NIST SP800-131a standard certificates from the IBM Cognos trust stores ... 205
Configuring IBM Cognos components to use another certificate authority .... 205
Create certificate signing request (CSR) files ................................ 206
Import the CA certificates into IBM Cognos components .................... 208
Configure IBM Cognos BI Components to use certificates generated by your CA ... 210
Configuring the SSL protocol for IBM Cognos components ................. 210
Configure SSL for IBM Cognos components ................................ 211
Set up shared trust between IBM Cognos servers and other servers .......... 212
Select and rank cipher suites for Secure Socket Layer ........................ 213
Configure IBM Cognos for SSL enabled Web servers ........................ 214
Configuring a Repository for Log Messages ................................ 215
Guidelines for creating a logging database .................................. 216
Database connectivity for the logging database ................................ 216
Log message repositories ....................................................... 218
Enabling User-specific Logging .............................................. 222
Changing Global Settings ...................................................... 223
Customize Language Support to the User Interface ......................... 223
Customizing Currency Support .............................................. 224
Customize content locale support .......................................... 225
Content Locales .................................................................. 225
Map Product Locales ........................................................... 227
Customize the Server Time Zone ............................................ 228
Encoding for Email Messages .................................................. 228
Cookie Settings ................................................................... 229
Change the IP Address Version .............................................. 230
Setting the IP version ................................................................ 231
Manually configuring IBM Cognos Configuration to start with the IPv6 option ... 231
Configuring IBM Cognos Configuration to always start with the IPv6 option on Windows ... 232
File Location Properties on Windows Vista .................................. 232
Update File Location Properties on Windows Vista .......................... 232
Change Configuration Settings for the IBM Cognos Series 7 Migration Service .... 233
Assign a User Account to the PowerPlay and Migration Services for Migration ... 233

Chapter 10. Configuring Portal Services .................................. 235
 Specify the Location of the Applications.xml File ......................... 235
Chapter 11. Using an application server other than Tomcat ...................... 247

- Create a separate JVM instance ................................................. 247
- Set JVM parameters for performance ........................................ 248
- Check the setup of IBM Cognos components .............................. 248
- Back up existing IBM Cognos information .................................. 249
- Set environment variables ......................................................... 250
- Adjusting the default connection time-out value for IBM Cognos Business Intelligence ........... 251
- Configure IBM Cognos components to run within the application server ........................................... 251
  - Use the Build Application Wizard to build and install IBM Cognos on IBM WebSphere Application Server . . 253
- Identifying the JDK for WebLogic 9 on AIX ................................ 254
- Change the application server startup script ................................ 254
  - Change the application server startup script for WebLogic .................. 255
  - Change the application server startup script for JBoss ......................... 256
- Configure application server properties and install IBM Cognos components .................. 256
  - Install IBM Cognos on WebSphere ............................................ 256
  - Install IBM Cognos on WebLogic ............................................. 257
  - Install IBM Cognos on SAP NetWeaver ..................................... 259
  - Install IBM Cognos on JBoss ................................................ 260
- Enabling the secure socket layer ................................................. 261
- Configuring web communication .................................................. 261
  - Configure virtual directory for SAP NetWeaver ......................... 262
- Unregister dispatchers that were configured for Tomcat ................ 262
- Upgrade to IBM Cognos BI in an application server environment ........... 263

Chapter 12. Using an unattended installation and configuration .................. 265

- Unattended installations .......................................................... 265
  - Use a response file from an installation on another computer ............. 266
  - Modifying a response file ....................................................... 267
  - Starting an unattended installation ......................................... 268
- Use an unattended configuration ................................................ 268
- Use an unattended uninstallation ................................................. 270

Chapter 13. Performance Maintenance ............................................. 271

- System Performance Metrics ..................................................... 271
  - Monitoring System Metrics Externally ..................................... 271
- Enabling Only Services That are Required .................................. 272
- Tuning a DB2 Content Store ..................................................... 275
- Adjusting the Memory Resources for the IBM Cognos Service ............... 275
- Reducing the number of requests per process ................................ 276
- Tune Apache Tomcat settings for 64-bit installations ......................... 276
- Increase the Request-handling Capacity for Cognos Content Database ........ 276
- Improve Metric Store Database Performance ................................ 277
- Reduce Delivery Time for Reports in a Network ................................ 277
- Increase Asynchronous Timeout in High User Load Environments ............ 277

Chapter 14. Manually configuring IBM Cognos Business Intelligence on UNIX and Linux operating systems ....................... 279

- Manually change default configuration settings ............................ 279
- Adding a component to your configuration .................................... 280
- Changing manually encrypted settings ....................................... 281
- Global settings on UNIX and Linux operating systems .................... 282
  - Changing manually the global settings on UNIX and Linux operating systems .... 283
Running Database and Index Cleanup Scripts .................................................. 323
Error trying to encrypt information when saving your configuration .......... 326
CAM-CRP-1315 error when saving configuration ............................................. 327
CAM-CRP-0221 error when logging into the portal ......................................... 327
Manually changing the installation directory name affects installations running under an application server .............................. 328
Configuration data is locked by another instance of IBM Cognos Configuration ................................................................. 328
Unable to exit a tab sequence when using keyboard-only navigation in IBM Cognos Configuration ............................................. 329
Unable to save your configuration ................................................................. 329
Java error when starting IBM Cognos Configuration ...................................... 329
Cryptographic error when starting IBM Cognos Configuration ..................... 330
Restarting the IBM Cognos service to apply configuration settings ............... 330
CM-CFG-029 error when trying to save a configuration that specifies a Microsoft SQL Server content store ................................. 331
DB2 not found error for Linux on System z .................................................... 331
DPR-ERR-2079 when Content Manager configured for failover .................... 331
Importing a large content store in Solaris using JRE 1.5 fails ....................... 332
Importing a large deployment in Windows crashes the Java virtual machine . 332
DPR-ERR-2008 error when you open a report .................................................. 332
Cannot load TM1 Cubeviewer or WebSheet iWidget in Business Insight ........ 332
Users are prompted for Active Directory credentials ................................... 333
Font on UNIX not found when starting IBM Cognos Configuration ............... 333
ESSBASEPATH cannot be detected ................................................................. 334
Query fails when using Oracle Essbase Server .............................................. 334
Group membership is missing from Active Directory namespace .............. 335
Errors displayed when deploying to Oracle 10G Application Server ............. 336
CGI timeout error while connected to IBM Cognos Business Intelligence through a Web browser .................................................. 337
Servlet class fails to load in WebLogic .......................................................... 337
Desktop icons or IBM Cognos Configuration window flicker on Windows ... 338
Migration Does Not Work .............................................................................. 339
Missing translations for object names in some locales ................................. 339

Notices ................. 341
Glossary ........................................ 345

A ........................................................................................................ 345
B ........................................................................................................ 345
C ........................................................................................................ 345
D ........................................................................................................ 347
E ........................................................................................................ 347
F ........................................................................................................ 347
G ........................................................................................................ 347
H ........................................................................................................ 348
I ........................................................................................................ 348
J ........................................................................................................ 348
L ........................................................................................................ 348
M ........................................................................................................ 349
N ........................................................................................................ 349
O ........................................................................................................ 349
P ........................................................................................................ 349
Q ........................................................................................................ 350
R ........................................................................................................ 350
S ........................................................................................................ 351
T ........................................................................................................ 351
U ........................................................................................................ 351
W ........................................................................................................ 352

Index ........................................... 353
Introduction

This guide contains instructions about installing, configuring, and testing IBM® Cognos® PowerPlay®.

For information about migration and about the differences between IBM Cognos Series 7 PowerPlay and IBM Cognos PowerPlay, see the IBM Cognos PowerPlay Migration and Administration Guide.

Audience

To use this guide, you should be familiar with

- IBM Cognos Series 7 PowerPlay
- installing software on a Microsoft Windows or UNIX operating system
- your information technology and security infrastructure
- database, directory server, and application server administration

Finding information

To find IBM Cognos product documentation on the web, including all translated documentation, access one of the IBM Cognos Information Centers (http://pic.dhe.ibm.com/infocenter/cogic/v1r0m0/index.jsp). Release Notes are published directly to Information Centers, and include links to the latest technotes and APARs.

You can also read PDF versions of the product release notes and installation guides directly from IBM Cognos product disks.

Accessibility Features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products. This product has accessibility features. For information on these features, see "Keyboard Shortcuts for the Installation Wizard" on page 291. IBM Cognos HTML documentation has accessibility features. PDF documents are supplemental and, as such, include no added accessibility features.

Forward-looking statements

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

Samples disclaimer

The Sample Outdoors Company, Great Outdoors Company, GO Sales, any variation of the Sample Outdoors or Great Outdoors names, and Planning Sample depict fictitious business operations with sample data used to develop sample applications for IBM and IBM customers. These fictitious records include sample
data for sales transactions, product distribution, finance, and human resources. Any resemblance to actual names, addresses, contact numbers, or transaction values is coincidental. Other sample files may contain fictional data manually or machine generated, factual data compiled from academic or public sources, or data used with permission of the copyright holder, for use as sample data to develop sample applications. Product names referenced may be the trademarks of their respective owners. Unauthorized duplication is prohibited.
Chapter 1. What's New?

This section contains a list of new, changed, and removed features for this release. It will help you plan your upgrade and application deployment strategies and the training requirements for your users.

What's New information for past releases is available by accessing one of the IBM Cognos Information Centers (http://pic.dhe.ibm.com/infocenter/cogic/v1r0m0/index.jsp).

To review an up-to-date list of environments that are supported by IBM Cognos Business Intelligence products, including information on operating systems, patches, browsers, web servers, directory servers, database servers, and application servers, see the IBM Software Product Compatibility Reports (SPCR) page (www.ibm.com/support/docview.wss?uid=swg27037784).

New features in version 10.2.1

The following topics describe the new features for 10.2.1.

New security standards in IBM Cognos BI

By default, IBM Cognos version 10.2.1 is qualified for the NIST SP800-131a standard as the product's cryptographic functions are configured for this standard.

You can configure IBM Cognos BI to comply with other standards or remove cryptographic components that are associated with older standards by using the ThirdPartyCertificateTool.

For more information, see "Change the security standard compliance for IBM Cognos trust stores" on page 204.

Store reports in an external object store

You can configure the Content Manager to store report output to a local drive or network share instead of in the content store database by configuring an external object store.

An external object store offers improved read and write performance by reducing the load on the Content Manager.

Related information:

"Use an external object store for report output" on page 200

You can configure Content Manager to store report output to a local drive or network share by defining an external object store. Report output is available through IBM Cognos Connection and IBM Cognos SDK, but the report output is not stored in the content store database.

New Features in Version 10.2.0

Listed are new features since the last release. Links to directly-related topics are included.
Option to initialize Cognos Configuration from a different file

You can use the -startupfile path/filename.xml option to specify a startup file other than the cogstartup.xml file when starting the IBM Cognos configuration tool.

The cogstartup.xml file must still exist in the Configuration directory.

For example, the following command runs the installation program in silent mode using the test.xml file located in the Configuration directory to set the configuration parameters.

cogconfig.sh -s -startupfile <c10_location>/configuration/test.xml

Related information:

“Use an unattended configuration” on page 268
To use an unattended configuration, you must export a configuration from an existing installation that has the same IBM Cognos BI components installed. You can then run IBM Cognos Configuration in silent mode.

Option to view the status of silent installations on the screen

You can use the -displayLog option to view the status of the silent installation on the screen in a UNIX or Linux environment.

For example, the following command runs the installation program in silent mode. The installation program uses the test.ats as the response file and displays the status of the installation on the screen.

./issetup -s test.ats -displayLog

Related information:

“Modifying a response file” on page 267
Generate and modify a response file to specify and record your installation preferences. You can also modify the response file template that is provided.

Predefined LDAP configurations

In IBM Cognos Configuration, you can configure your environment by selecting from a number of predefined LDAP authentication namespace configurations.

The following is a list of predefined LDAP configurations:

- LDAP - Active Directory
- LDAP - IBM Tivoli®
- LDAP - OracleSunOne

New Features in Version 10.1.0

Listed are new features since the last release. Links to directly-related topics are included.

Access to Software Development Kit Installation and Configuration Guide

In Version 10.1.0, the IBM Cognos Software Development Kit Installation and Configuration Guide is available from the IBM Cognos Information Center
Changed Features in Version 10.1.0

Listed are changes to features since the last release. Links to directly-related topics are included.

Default Installation Location and Web Alias

The path for the default installation directory is changed in IBM Cognos Business Intelligence, Version 10.1.0.

The default location, represented by `c10_location` in this guide, is as follows:

- **Microsoft Windows operating system**
  
  `C:\Program Files\IBM\cognos\c10`

- **UNIX and Linux operating systems**
  
  `/usr/IBM/cognos/c10`

The default Web alias in IBM Cognos Configuration is changed from `cognos8` to `ibmcognos`.

PowerPlay Batch Administration

In the previous release, the IBM Cognos PowerPlay Batch Administration utility was available only as a separate download. For this release the utility is included with the PowerPlay installation.

For more information about the utility, see the *PowerPlay Migration and Administration Guide*.

IBM Cognos Go! Dashboard is Merged with Features from IBM Cognos Viewer into One User Interface

In earlier releases, an interactive dashboard application was available by installing IBM Cognos Go! Dashboard with your IBM Cognos BI server product. In addition, IBM Cognos Viewer provided the basic report consumption experience.

IBM Cognos Go! Dashboard and features from IBM Cognos Viewer are now merged into one user interface. This brings the information consumption, rather than viewing and opening folders, to the forefront of the experience. However, IBM Cognos Viewer is still available and maintained in this release.

Enhanced Support for Authentication Using a RACF Provider

In earlier releases, if you wanted to use a Resource Access Control Facility (RACF®) provider for authentication with IBM Cognos Business Intelligence server, you created a custom Java™ provider and then configured a Custom Java Provider namespace in IBM Cognos Configuration to use it. In IBM Cognos Business Intelligence server, Version 10.1.0, you can configure a RACF namespace directly in IBM Cognos Configuration on AIX® or on Linux for System z® operating systems.

Secure Access When Monitoring System Metrics Externally

In earlier releases, you could monitor system metrics externally to IBM Cognos Administration by using Java Management Extensions (JMX), a technology that supplies tools to manage and monitor applications and service-oriented networks.
In IBM Cognos Business Intelligence Server, Version 10.1.0, IBM Cognos Configuration provides two new properties that you can use to enable secure access to the metrics in the Java environment.

**Removed Features in Version 10.1.0**

Listed are features that are removed since the last release. Links to directly-related topics are included.

**Managing Memory for the IBM Cognos Service**

In earlier releases, you had two options in IBM Cognos Configuration for configuring the maximum amount of memory for the IBM Cognos service. You could adjust the maximum memory value or you could delete the Cognos service and then select a new service that used a small, medium, or large configuration template. In IBM Cognos BI server, Version 10.1.0, you have the single option of adjusting the maximum memory value.
Chapter 2. Distribution options

Before implementing IBM Cognos PowerPlay, decide how you will install it in your environment. You can install all PowerPlay components on one computer, or distribute them across a network. The best distribution option depends on your reporting or scorecarding requirements, resources, and preferences. Configuration requirements differ depending on whether you install all components on one computer or more than one computer.

IBM Cognos PowerPlay is compatible with other IBM Cognos products. If your environment includes other IBM Cognos products, you must consider how IBM Cognos PowerPlay will fit into that environment.

For some distributed installations that include both IBM Cognos PowerPlay and IBM Cognos BI components, you must complete additional tasks in IBM Cognos Administration after you complete the installation and configuration. For information about required administration tasks, see the IBM Cognos PowerPlay Migration and Administration Guide.

Product components

IBM Cognos PowerPlay is a web-based business intelligence solution with integrated reporting and data exploration features.

IBM Cognos PowerPlay integrates easily into your existing infrastructure by using resources that are in your environment. Some of these existing resources are required, such as using a database for the content store. Other resources are optional, such as using a security provider for authentication, or using an application server.

By default, IBM Cognos BI uses Apache Tomcat as an application server. You can configure IBM Cognos BI products to run on supported application servers that you currently use in your environment.

Server components

The server components for IBM Cognos Business Intelligence are separated into three tiers.

The server components provide the user interfaces for reporting and data exploration, as well as the server functionality for routing and processing user requests.

In the installation program, you can select to install the following server components:

- Gateway
- Application Tier Components
- Content Manager
Web communication - gateway
Web communication in IBM Cognos Business Intelligence is typically through gateways, which reside on one or more Web servers. A gateway is an extension of a Web server program that transfers information from the Web server to another server.

Gateways are often CGI programs, but may follow other standards, such as Internet Server Application Program Interface (ISAPI), Apache Modules (apache_mod), or as a servlet implementation.

Application Tier Components
The IBM Cognos Business Intelligence applications tier contains one or more IBM Cognos BI servers. An IBM Cognos BI server runs requests, such as reports, analyses, and queries, that are forwarded by a gateway. An IBM Cognos BI server also renders the IBM Cognos Connection and studio interfaces.

Configuring and managing the product - IBM Cognos Configuration
IBM Cognos Configuration is a tool that you use to configure IBM Cognos BI, and to start and stop its services.

Publishing, managing, and viewing content - IBM Cognos Connection
IBM Cognos Connection is a Web portal provided with IBM Cognos Business Intelligence, providing a single access point to the corporate data available for its products. It provides a single point of entry for querying, analyzing, and organizing data, and for creating reports, scorecards, and events. Users can run all their Web-based IBM Cognos BI applications through IBM Cognos Connection. Other business intelligence applications, and web addresses to other applications, can be integrated with IBM Cognos Connection.

Central administration - IBM Cognos Administration
IBM Cognos Administration is a central management interface that contains the administrative tasks for IBM Cognos BI. It provides easy access to the overall management of the IBM Cognos environment and is accessible through IBM Cognos Connection.

IBM Cognos Administration also provides access to cube and report settings for PowerPlay.

IBM Cognos PowerPlay Studio
IBM Cognos PowerPlay Studio lets users view, explore, and distribute reports using a web browser.

Viewing and interacting with published content - Cognos Viewer
Cognos Viewer is a portlet in which you can view and interact with any type of published IBM Cognos content. It is accessible through IBM Cognos Connection and any existing enterprise portal.
Exploring, analyzing, and comparing dimensional data - Analysis Studio

In Analysis Studio, users can explore, analyze, and compare dimensional data. Analysis Studio provides access to dimensional, OLAP (online analytical processing), and dimensionally modeled relational data sources. Analyses created in Analysis Studio can be opened in Report Studio and used to build professional reports.

Facilitating decision-making - IBM Cognos Workspace

You can create sophisticated interactive workspaces using IBM Cognos content, as well as external data sources such as TM1® Websheets and CubeViews, according to your specific information needs. You can view and open favorite workspaces and reports, manipulate the content, and e-mail your findings. You can also use comments and activities for collaborative decision making.

Managing Application Data - Content Manager

Content Manager is the IBM Cognos Business Intelligence service that manages the storage of customer application data, including security, configuration data, models, metrics, report specifications, and report output. Content Manager is needed to publish packages, retrieve or store report specifications, manage scheduling information, and manage the Cognos namespace.

Content Manager stores information in a content store database.

Optional server components

The following optional components are available to install on the server to extend the functionality of IBM Cognos Business Intelligence.

Preconfigured application database - Cognos Content Database

Cognos Content Database is an instance of an Apache Derby database. It is a selectable installation component, and is not installed by default. If you install Cognos Content Database, it is preconfigured as the default content store for IBM Cognos Business Intelligence.

Do not use Cognos Content Database for the content store in a production environment. Cognos Content Database is provided to help you quickly set up a test or proof-of-concept system.

Apache Derby is open source software whose license terms can be found on the Apache Derby web site. Modifying the Apache Derby database or using it with other products is not supported. Any modifications that you make to the Apache Derby database are at your own risk.

You can use Cognos Content Database as a content store or notification database, but not as a query database.

Learning and troubleshooting using sample data - IBM Cognos BI Samples

The IBM Cognos BI samples illustrate product features and technical and business best practices using data from a fictitious company, The Sample Outdoors Company. You can also use them for experimenting with and sharing report design techniques, and for troubleshooting.
Migration Components

The IBM Cognos Business Intelligence migration components are used to migrate content from IBM Cognos Series 7 to IBM Cognos BI.

For more information about the migration components, see the *IBM Cognos PowerPlay Migration and Administration Guide*.

The migration components include the following:

**Migration Assistant**

Administrators use the Migration Assistant to migrate IBM Cognos Series 7 PowerPlay content from PowerPlay Enterprise Server, Upfront, and IBM Cognos Connection to IBM Cognos PowerPlay.

**Migration Services**

Migration services support the migration of PowerPlay content from IBM Cognos Series 7 to IBM Cognos PowerPlay. An IBM Cognos PowerPlay installation includes the migration service by default. The IBM Cognos PowerPlay CD also includes the migration service that you install on the IBM Cognos Series 7 computer.

**Bookmark Conversion Utility**

The bookmark conversion utility converts PowerPlay Enterprise Server bookmarks into a format that can be read by IBM Cognos PowerPlay Studio.

**Report Conversion Macro**

IBM Cognos PowerPlay does not support ppr format reports created with IBM Cognos Series 7. IBM Cognos PowerPlay provides a macro named ppr2ppx.mac to allow you to convert ppr format reports to ppx format.

**Report Upgrade Macro**

If you have local .ppx files that access remote cubes, IBM Cognos PowerPlay provides a macro you can use to change the cube reference in the report to an IBM Cognos BI package reference. Also, the macro converts the report encoding to UTF-8.

Client Components

Client components provide functionality to users without the requirement of a full server installation and may depend on the server to perform some operations. IBM Cognos PowerPlay provides the following client.

**IBM Cognos PowerPlay Client**

PowerPlay Client lets users view, explore, format, and distribute reports.

**Required database components**

In addition to the tools that are provided, IBM Cognos PowerPlay requires the following components that are created using other resources.
Content store

The content store is a relational database that contains data that your IBM Cognos BI product needs to operate, such as report specifications, published models, and the packages that contain them; connection information for data sources; information about the external namespace, and the Cognos namespace itself; and information about scheduling and bursting reports.

Your IBM Cognos BI product includes an embedded database, Cognos Content Database, that you can use to get your product running quickly in a test or proof-of-concept system. When you are ready to set up a production environment with your IBM Cognos BI product, set up the content store to use a supported database that can be secured and tuned for performance and stability. The administration portal provides features that you can use to back up and archive the data from Cognos Content Database before moving to the new content store database in your production environment. For more information, see the topic about deploying the entire content store in the IBM Cognos Business Intelligence Administration and Security Guide.

Design models and log files are not stored in the content store.

The IBM Cognos service that uses the content store is named Content Manager.

Data sources

Data sources, also known as query databases, are relational databases, dimensional or OLAP cubes, files, or other physical data stores that can be accessed through IBM Cognos BI. Application Tier Components use data source connections to access data sources.

IBM Cognos PowerPlay supports PowerCube data sources. For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.

Distributing components

When you install IBM Cognos PowerPlay server components, you specify where to place the gateways, Application Tier Components, and Content Manager. You can install these components using any of these options:

- Install all components on one computer.
  This option is typically used for a demonstration or in a proof of concept environment.
- Install the gateway on a separate computer.
  In this option, the gateway and Web server are on one computer, and the remaining IBM Cognos components are on other computers. You may choose this option if you have existing Web servers available to handle IBM Cognos component requests.
- Install Application Tier Components and Content Manager on separate computers.
  Choose this option to maximize performance, availability, capacity, or security based on the processing characteristics of your organization.

If you plan to install Cognos Content Database, install it on the same computer as Content Manager. Cognos Content Database is automatically configured for use as your content store.
• Install IBM Cognos PowerPlay server components in the same location as other IBM Cognos BI products.
  Different IBM Cognos BI products share components, such as the Content Manager. If you plan to install the IBM Cognos BI reporting and scorecarding components on the same computer, for example, install them in the same installation location. This conserves resources such as disk space and memory consumption by services.

• Install components on 64-bit systems
  Some IBM Cognos BI components are available for 64-bit systems. Whether you are installing all server components together on a single server or on multiple servers, 32-bit and 64-bit components must be in separate directories.

After installing IBM Cognos BI server components, you must configure them so they can communicate with each other.

In addition to installing the Content Manager, Application Tier Components, and gateway components, you must install Framework Manager, the metadata modeling application for business intelligence. You can also choose to install Transformer, the modeling and building tool for creating PowerCubes for use with IBM Cognos BI. No matter which IBM Cognos installation scenario you follow, you can install all modeling components in separate locations.

For more information about installing Framework Manager or Transformer, see the IBM Cognos Business Intelligence Installation and Configuration Guide.

All server components on one computer

You can install all the IBM Cognos PowerPlay server components on one computer. Choose this scenario for proof of concept or demonstration environments where the user load is small

Because the gateway must be located with the Web server, the single computer must also be running a Web server.

If your web server is on UNIX or Linux, you must install the PowerPlay Client on a separate computer that runs on a Microsoft Windows operating system.

In a single-computer installation, all server components for PowerPlay are installed on one computer. The content store and data sources can be on one or more computers.

Configuration requirements

If you install all server components for IBM Cognos PowerPlay on the same computer, you must then
• configure your Web server to host IBM Cognos Web content
• specify connection information to the content store
• set up an email account for notifications (if you intend to email reports)

Gateways on separate computers

The gateway passes queries from the Web server and clients to the dispatcher. It can reside on one or more Web servers.
You can install the gateway and a Web server on one computer, and install the remaining IBM Cognos PowerPlay server components on other computers. If you have a Web farm, you may want to install a gateway on each Web server. Using multiple Web servers to manage incoming requests provides a better level of service.

If you install only the gateway component on the same computer as the Web server, your Web server manages the core Web services and does not process user requests. This separation of processing may be required if you have a firewall between the Web server and your Application Tier Components computers.

In the following diagram, two Web servers each have a gateway installed. Incoming requests are passed to either gateway and forwarded to the Application Tier Components computer.

![Diagram of two gateways and Application Tier Components]

**Figure 1. Installation with two gateways**

**Configuration requirements**

If you install one or more gateways on separate computers, you must ensure that you can view IBM Cognos content and that the gateways can communicate with other IBM Cognos components. On each computer where the gateway is installed you must:

- configure your Web server to host IBM Cognos Web content
- configure the Dispatcher URIs

**Application Tier Components and Content Managers on separate computers**

Application Tier Components use the IBM Cognos Connection interface to balance loads, access data, perform queries, schedule jobs, and render reports. Content Manager stores all report specifications, results, packages, folders, and jobs in the content store.
You can install the Application Tier Components and Content Manager on the same computer, or on different computers. Installing on different computers can improve performance, availability, and capacity.

**More than one Content Manager**

You can install any number of installations of Content Manager, although only one is active at any time. The other installations each act as a standby Content Manager. One becomes active only if a failure occurs that affects the active Content Manager computer. For failover support, it is advisable to install Content Manager on two or more computers.

**Install multiple Content Managers**

Content Manager stores data that IBM Cognos BI needs to operate, such as report specifications, published models, and the packages that use them; connection information for data sources; information about the external namespace and the Cognos namespace itself; and information about scheduling and bursting reports. The content store is a relational database management system (RDBMS). There is only one content store for each IBM Cognos installation.

You may choose to install Content Manager separately from the Application Tier Components. For example, you may want Content Manager in your data tier instead of in the applications tier.

When an active Content Manager fails, unsaved session data is lost. When the new active Content Manager takes over, users may be prompted to logon.

**Configuration requirements**

On each computer where you install Content Manager, you must
- specify connection information to the content store
- specify the Dispatcher URIs
- specify all Content Manager URIs
- set up a connection to an email account for notifications (if you want to email reports)

**More than one Application Tier Components computer**

To improve scalability in an environment in which there is typically a large volume of report requests to process, you can install the Application Tier Components on multiple computers dedicated to processing incoming requests. By installing the Application Tier Components on multiple computers, you distribute and balance loads among the computers. You also have better accessibility and throughput than on a single computer, as well as failover support.

In an installation with multiple IBM Cognos PowerPlay servers, incoming requests are routed through a gateway to a dispatcher. The dispatcher forwards the request to one of the PowerPlay servers. The PowerPlay server forwards the request to the Content Manager, which queries the content store for metadata to query the PowerCube. Query results are returned to the PowerPlay server for rendering.
Configuration requirements

If you install one or more Application Tier Components on a separate computer, to ensure that they can communicate with other IBM Cognos PowerPlay components, do the following:

- specify all Content Manager URIs
- specify the Dispatcher URIs
- specify the Dispatcher URI for external applications

Installing 64-bit versions of IBM Cognos BI products

Some IBM Cognos BI components are available for 64-bit systems. When installing on a 64-bit system, the components must be installed in the appropriate directories.

Like previous releases, IBM Cognos PowerPlay components remain 32-bit. However, PowerPlay provides an installation to support integration with 64-bit IBM Cognos BI installations. This integration allows you to take advantage of the performance benefits offered by the 64-bit IBM Cognos BI components.

The default installation directory that is used by the IBM Cognos BI components depends on the version that you install.

Table 1. Default paths for 32-bit installations

<table>
<thead>
<tr>
<th>For a 32-bit Installation on</th>
<th>Default path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows operating systems</td>
<td>C:\Program Files\IBM\Cognos\c10</td>
</tr>
<tr>
<td>64-bit Microsoft Windows operating systems</td>
<td>C:\Program Files (x86)\IBM\Cognos\c10</td>
</tr>
<tr>
<td>UNIX operating systems</td>
<td>/usr/IBM/cognos/c10</td>
</tr>
<tr>
<td>Linux operating systems</td>
<td>/opt/IBM/cognos/c10</td>
</tr>
</tbody>
</table>

Table 2. Default paths for 64-bit installations

<table>
<thead>
<tr>
<th>For a 64-bit Installation on</th>
<th>Default path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows operating systems</td>
<td>C:\Program Files\IBM\Cognos\c10_64</td>
</tr>
<tr>
<td>UNIX operating systems</td>
<td>/usr/IBM/cognos/c10_64</td>
</tr>
<tr>
<td>Linux operating systems</td>
<td>/opt/IBM/cognos/c10_64</td>
</tr>
</tbody>
</table>

Whether you are installing all server components together on a single server or on multiple servers, the 32-bit and 64-bit components must be in separate directories.

Server components that can be installed together in the c10_64 directory

The following components can be installed together on one 64-bit server or installed separately on multiple 64-bit servers. When installing the components, ensure that you start from the appropriate download directory or disk:

- IBM Cognos BI Server and IBM Cognos PowerPlay (Content Manager, Application Tier Components, Gateway)
- IBM Cognos BI Supplementary Language Documentation (32-bit and 64-bit versions available on one disk)
- IBM Cognos BI Samples (32-bit and 64-bit versions available on one disk)
Components that must be installed to a separate directory than the 64-bit components

The following components can be installed together on the 64-bit server, but they must be installed to a separate directory from the 64-bit components. For example, the default installation location for these components is the Program Files (x86) directory on a 64-bit Windows computer, while the 64-bit server components are installed to the Program Files directory. They can also be installed on a separate 32-bit system:

- Framework Manager (Windows only)
- IBM Cognos PowerPlay Client (Windows only)
- IBM Cognos Transformer (UNIX and Linux utility for building PowerCubes)
- IBM Cognos Transformer (Windows modeling tool)
- IBM Cognos BI for Microsoft Office (Windows only)

Accessing product documentation in an integrated environment

The documentation for IBM Cognos Business Intelligence components is installed with the gateway component. If you integrate different IBM Cognos BI products, you either use the same gateway or use separate gateways. If you want to use the same gateway, all gateway components must be of the same product version, and you should install the IBM Cognos BI gateway component for each product into the same location on the same computer. This ensures that all of the product documentation is available to all users. If you want to use separate gateways for each product, you can install the IBM Cognos BI gateway component for each product on separate computers, but the product documentation on each gateway is specific for the IBM Cognos BI product you installed.

If you want users to access each IBM Cognos BI product through separate gateways, yet still be able to access documentation for all components, you can install each product’s gateway component into the same location as your other IBM Cognos BI gateway components.

IBM Cognos PowerPlay with Other IBM Cognos Products

You can install IBM Cognos PowerPlay in an environment that includes other IBM Cognos Business Intelligence products. The installation wizard for PowerPlay can recognize compatible directories and shows a warning when conflicts occur. After PowerPlay is installed, you can access objects that are created in other IBM Cognos BI products. The requirements for access depend on how you choose to run the two products.

IBM Cognos Series 7 Products That Can Be Migrated to IBM Cognos PowerPlay

You can completely migrate IBM Cognos Series 7 PowerPlay applications to IBM Cognos PowerPlay. For more information, see the PowerPlay Migration and Administration Guide.

You can also migrate metadata and applications from other IBM Cognos Series 7 products to IBM Cognos Business Intelligence. Content that can be migrated includes Architect models, Impromptu® client reports and catalogs, and Impromptu Web Reports content.
**PowerPlay Enterprise Server**

The data analysis and exploration capabilities of IBM Cognos Series 7 PowerPlay are now available with IBM Cognos PowerPlay. The IBM Cognos BI service-oriented architecture makes possible the integration of PowerPlay Web, PowerPlay Enterprise Server Administration, and the PowerPlay Enterprise Server service.

You use the Migration Assistant to migrate IBM Cognos Series 7 PowerPlay content from
- PowerPlay Enterprise Server
- Upfront
- Cognos Connection (content published from IBM Cognos Series 7 PowerPlay Enterprise Server)

You can also migrate bookmarks and PowerPlay Client reports to Cognos PowerPlay. For details about what you can migrate from IBM Cognos Series 7 PowerPlay to IBM Cognos PowerPlay, see the PowerPlay Migration and Administration Guide.

To migrate content from IBM Cognos Series 7 to IBM Cognos PowerPlay, you must install IBM Cognos PowerPlay Server and IBM Cognos Series 7 Migration Components.

**Architect**

You can migrate Architect models for use as a metadata source for Framework Manager.

**Impromptu**

You can migrate Impromptu catalogs and reports to IBM Cognos BI. You use migrated catalogs as a metadata source for Framework Manager. After completing the catalog migration process, you can migrate and deploy Impromptu reports.

**Impromptu Web Reports**

You can migrate Impromptu Web Reports content, such as schedules and events, to IBM Cognos BI. You migrate Impromptu Web Reports content using an IBM Cognos Series 7 Deployment Manager package as the migration source. Before you migrate Impromptu Web Reports you must migrate the Impromptu catalog metadata used by the reports.

You cannot migrate Impromptu query definition files (.iqd), but you can continue to use existing .iqd files to build cubes in IBM Cognos BI Transformer 8.4. To do so, you must install the optional component, Series 7 IQD Bridge, which is available to install with IBM Cognos BI on IBM Cognos Series 7 supported platforms.

PowerPrompts are not migrated, but you can implement similar functionality using either the built-in administrator functionality or the IBM Cognos Software Development Kit.
IBM Cognos Products That Interoperate with IBM Cognos PowerPlay

Some IBM Cognos Business Intelligence products provide functionality that is not available in IBM Cognos PowerPlay. You can use these products in the same environment as IBM Cognos PowerPlay.

IBM Cognos BI Server

To use modeling tools, such as Framework Manager and IBM Cognos Transformer, with PowerPlay, you must install IBM Cognos BI. If you also want to use Report Studio, Analysis Studio, or Query Studio, you need IBM Cognos BI Server.

If you are installing PowerPlay in an existing IBM Cognos BI environment, backup your IBM Cognos BI configuration before installing PowerPlay.

For a single-computer installation, install components for both products in the same directory, as follows:
1. Install both IBM Cognos BI Server and IBM Cognos PowerPlay.
2. Configure the installed components.
3. Install IBM Cognos Series 7 Migration Components on the IBM Cognos Series 7 PowerPlay server.

For a distributed installation, install and configure components as follows:
1. Install, configure, and test all components for IBM Cognos BI Server: Content Manager, application tier, and gateway.
   For instructions about installing and configuring IBM Cognos BI Server, see the IBM Cognos BI Installation and Configuration Guide.
2. On each computer that includes the IBM Cognos BI Application Tier Components, install PowerPlay Administration. You can also install PowerPlay Server on the same computer as the IBM Cognos BI Application Tier Components.
3. If you install PowerPlay Application Tier Components on a separate computer from the IBM Cognos BI Application Tier Components, you must disable some services. On the computer where you installed the PowerPlay Application Tier Components, open Cognos Configuration and under IBM Cognos Services, disable the presentation service and report service. Optionally, to reduce demand on system resources, you can disable the query service.
4. On the computer that includes the IBM Cognos BI Content Manager components, install the PowerPlay Content Manager components.
5. On the computer that includes the IBM Cognos BI gateway components, install the PowerPlay gateway components.
6. If you plan to migrate content from IBM Cognos Series 7, install the IBM Cognos Series 7 Migration Components on the IBM Cognos Series 7 PowerPlay Enterprise Server computer, and if required, the IBM Cognos Series 7 Upfront computer.

For some distributed installation scenarios, you must complete additional tasks in IBM Cognos Administration after you complete the installation and configuration to ensure PowerPlay content works correctly. For information about required administration tasks, see the IBM Cognos PowerPlay Migration and Administration Guide.
**Cognos Planning - Analyst**

You can access published plan data in IBM Cognos BI by using the Generate Framework Manager Model wizard, which requires IBM Cognos Planning - Analyst 7.3 MR1 or later.

If you want to use this product with the IBM Cognos BI server, you must ensure that both products are the same version.

For more information, see the *IBM Cognos Analyst User Guide*.

**Cognos Planning - Contributor**

You can access unpublished (real-time) Contributor cubes in IBM Cognos BI by custom installing the IBM Cognos BI - Contributor Data Server component that is included with IBM Cognos Planning - Contributor 7.3 MR1 release or later. You can access published plan data in IBM Cognos BI by using the Generate Framework Manager Model administration extension in Contributor, which requires IBM Cognos Planning - Contributor 7.3 MR1 or later.

If you want to use this product with the IBM Cognos BI server, you must ensure that both products are the same version. You cannot install IBM Cognos Planning in the same path as 64-bit IBM Cognos BI.

For more information, see the *IBM Cognos Contributor Administration Guide*.

**Cognos Finance**

You can access IBM Cognos Finance cubes that are secured against a Series 7 namespace by using the IBM Cognos Finance Network API Service. You can also export data and metadata from IBM Cognos Finance for use in Framework Manager.

**Cognos Controller**

You can access IBM Cognos BI to create IBM Cognos Controller Standard Reports by using a predefined Framework Manager model that is created when IBM Cognos Controller is installed. You can also access published Controller data and structures in Framework Manager for custom reporting and analysis.

If you want to use this product with the IBM Cognos BI server, you must ensure that both products are the same version.

**Cognos Transformer**

You can use IBM Cognos PowerCubes and Transformer models that were generated by Transformer 7.3 or later directly in IBM Cognos BI. The cubes and models are upwards compatible and require no migration or upgrade tools. You can run reports and analyses in IBM Cognos BI against the IBM Cognos PowerCubes.

If you want to use the new integration features of Transformer with IBM Cognos BI, you can upgrade IBM Cognos Series 7.x Transformer models to IBM Cognos BI Transformer 8.4 or later. This allows you to use IBM Cognos BI data sources (such
as published packages), list reports authored in Query Studio or Report Studio, authenticate using IBM Cognos BI security, and publish directly to IBM Cognos Connection.

Before you load the model, the IBM Cognos Series 7 namespace must be configured in IBM Cognos BI and the name ID that is used to configure it in IBM Cognos BI must match the name used in IBM Cognos Series 7.

For more information about upgrading IBM Cognos Series 7 secured PowerCubes, see the IBM Cognos Business Intelligence Transformer User Guide.

For IBM Cognos Series 7 PowerCubes to be used in IBM Cognos BI, optimize the cubes for use in IBM Cognos BI by using the pcoptimizer utility, which is supplied with IBM Cognos BI. Otherwise, PowerCubes that were created with previous versions of Transformer may take too long to open in the IBM Cognos BI Web studios. This optimization utility is suitable for older PowerCubes created before Transformer 8.4 and does not require access to the model or data source. It is not necessary to run this command line utility for cubes created in Transformer 8.4 or later. For more information about optimizing PowerCubes, see the Transformer User Guide.

You can publish PowerCubes using Transformer 8.4, Framework Manager, or directly in the IBM Cognos BI portal. You can publish single PowerCube data sources and packages to IBM Cognos Connection interactively in Transformer or in the command line. You can also publish silently using batch scripts after building a PowerCube. A user who has privileges to create data sources and packages in IBM Cognos Connection can publish PowerCubes in IBM Cognos Connection as well. The MDC file must be in a secured location that the IBM Cognos BI dispatcher and the report server process can access. Packages that use multiple PowerCubes from different PowerCube definitions or PowerCubes mixed with other data sources must be published using Framework Manager.

If you use an IBM Cognos Series 7 PowerCube as a data source, IBM Cognos BI converts the cube data from the encoding that was used on the system where the PowerCube was created. For a successful conversion, IBM Cognos Series 7 PowerCubes must be created with a system locale set to match the data in the PowerCube.

**Cognos Data Manager**

Data Manager is used to create data warehouses and data repositories for reporting, analysis, and performance management. When Data Manager is installed in your IBM Cognos BI environment, you can use the Data Movement Service to run builds and JobStreams in IBM Cognos Connection. You must install the Data Manager engine in the same location as your IBM Cognos BI Application Tier Components. Both Data Manager and IBM Cognos BI must be the same version.

**Cognos Mobile**

With IBM Cognos Mobile, you can access reports authored with Analysis Studio, Report Studio, Query Studio, and workspaces created in IBM Cognos Workspace on a mobile device (such as a Blackberry) or a tablet computer.

To download, view, and interact with reports, IBM Cognos Mobile devices are either web-based, require the download of a native client or require the installation
of a rich client, in addition to the installation of IBM Cognos BI components on the server. Both IBM Cognos Mobile and IBM Cognos BI server must be at the same version.

For more information, see the *IBM Cognos Mobile Installation and Administration Guide*.

**IBM Cognos Series 7 content that can be recreated in IBM Cognos Business Intelligence**

Some IBM Cognos products cannot be programmatically migrated with the migration tools for IBM Cognos BI. IBM Cognos BI offers two options for duplicating content or functionality for the products described: use the Upfront portal within the IBM Cognos BI portal or use IBM Cognos BI studios to duplicate queries, visualizations, or objects.

The last release of the migration tools was version 10.1.1. You can use these tools to migrate to IBM Cognos Business Intelligence version 10.1.1 (Report Studio or Analysis Studio), and then upgrade the migrated content to IBM Cognos BI version 10.2.0.

**Cognos Query**

You can use IBM Cognos Migration Assistant to identify IBM Cognos Query objects in the IBM Cognos Series 7 migration source. You can then duplicate most IBM Cognos Query functionality in IBM Cognos BI. Foundation queries are available in IBM Cognos BI when you migrate an Architect model to Framework Manager. You can also manually replicate saved queries using SQL components in Report Studio.

**Cognos Visualizer**

You can duplicate some functionality by using the charting, layout, and formatting options in Report Studio and Analysis Studio.

**Cognos NoticeCast**

You can duplicate alert and notification functionality by using Event Studio and other IBM Cognos BI components.

**Cognos Web Services**

You can duplicate most IBM Cognos Web Services functionality using the IBM Cognos Software Development Kit.

**CognosScript**

You can duplicate automation functionality using the IBM Cognos Software Development Kit.

**Cognos Portal Services**

You can duplicate most IBM Cognos Portal Services functionality using IBM Cognos Connection.
Chapter 3. Preparing to install

Before you install IBM Cognos PowerPlay, you must set up resources in your environment so that the components can operate. For example, you must create a database for the content store, configure Web browsers, and create a user account for IBM Cognos Business Intelligence.

If you want to use Cognos Content Database as your content store, you do not have to create a database or set up a database client. A database is created during the installation and IBM Cognos BI is configured to use it.

When you select the Cognos Content Database in the installation wizard, a database is created during the installation and PowerPlay is configured to use it.

Use the following checklist to guide you through the setup process:

- Review the Release Notes
- Review supported environments
- Verify system requirements
- Review the default port settings
- Create the database for the content store
- Configure a user or network server account for IBM Cognos BI.
- Configure Web browsers

Review the Release Notes Before You Install

Before you install your IBM Cognos product, it is important to be aware of all issues that may affect your installation strategy.

There may be late-breaking issues that were not known when this installation guide was created.

Review the Release Notes before you install your product. The Release Notes contains late-breaking information about known issues, and documentation updates and deprecation notices. The Release Notes are available from the first page of the installation wizard or from the product disc. Release notes are also available from Information Centers IBM Cognos Information Centers (http://pic.dhe.ibm.com/infocenter/cogic/v1r0m0/index.jsp).

Review supported environments

To ensure that your product works properly, apply all minimum required operating system patches, and use only the supported versions of third-party software.

To review an up-to-date list of environments that are supported by IBM Cognos Business Intelligence products, including information on operating systems, patches, browsers, web servers, directory servers, database servers, and application servers, see the IBM Software Product Compatibility Reports (SPCR) page (www.ibm.com/support/docview.wss?uid=swg27037784).
Unless otherwise indicated, IBM Cognos products are compatible with later versions of patches and service packs from the versions stated.

It is important to note that the Linux operating system is available in a number of distributions and supports a number of hardware platforms. Ensure that the combination of the operating system and hardware that you are using is supported.

**Cognos products and virtualization environments**

The [IBM virtualization policy](http://www.ibm.com/software/support/virtualization_policy.html) describes IBM support for virtualization environments.

For more information, search [supported server virtualization environments by product](http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/vesForProduct.html).

### Verify system requirements

Use the following tables to check the minimum hardware and software requirements to install and run IBM Cognos Business Intelligence components on one computer. Additional resources may be required for distributed or production environments.

The following table lists the hardware requirements and specifications for a single computer installation.

**Hardware requirements**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Microsoft Windows</td>
</tr>
<tr>
<td></td>
<td>UNIX</td>
</tr>
<tr>
<td></td>
<td>Linux</td>
</tr>
<tr>
<td></td>
<td>Some IBM Cognos BI components are not supported on Linux.</td>
</tr>
<tr>
<td>RAM</td>
<td>For more information, see <strong>Memory settings</strong> on page 23.</td>
</tr>
<tr>
<td>Operating system specifications</td>
<td>File descriptor limit set to 2048 on UNIX and Linux</td>
</tr>
<tr>
<td>Disk space</td>
<td>A minimum of 3.5 GB of free space is required to install the software and 4 GB of free space on the drive that contains the temporary directory used by IBM Cognos components. For all databases, the size will increase over time. Ensure that you have sufficient disk space for future requirements.</td>
</tr>
<tr>
<td>Printer</td>
<td>To ensure that reports print properly on Windows, Adobe Reader requires that you configure at least one printer on the computer where you install the Application Tier Components. All reports, regardless of the print format that you choose, are sent as temporary PDF files to Adobe Reader for printing.</td>
</tr>
</tbody>
</table>
Table 3. Hardware requirements for a single computer installation (continued)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td>To email reports, the system requires the ability to use and access a mail server.</td>
</tr>
</tbody>
</table>

Software requirements

The following table lists the software requirements and specifications for a single computer installation.

Table 4. Software requirements for a single computer installation

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web server</td>
<td>A Web server must be installed and started.</td>
</tr>
<tr>
<td>Java Runtime Environment (JRE)</td>
<td>An IBM JRE is installed automatically with IBM Cognos BI on Windows. If you are using an application server, use the JRE that is installed with it, if it is supported in IBM Cognos BI.</td>
</tr>
</tbody>
</table>
| Database                  | Cognos Content Database can be installed and configured as the default content store database in a test or proof-of-concept system. You must have one of the following databases available to store IBM Cognos data in a production environment:  
  - Oracle  
  - DB2®  
  - Microsoft SQL Server  
  - Sybase  
  - Informix®  
  TCP/IP connectivity is required for all database types. |
| Web browser               | For all Web browsers, the following must be enabled:  
  - cookies  
  - JavaScript  
  For Microsoft Internet Explorer only, the following must be enabled:  
  - Run ActiveX controls and plug-ins  
  - Script ActiveX controls marked safe for scripting  
  - Active scripting  
  - Allow META REFRESH  
  For Microsoft Internet Explorer version 10, ensure that Automatically recover from page layout errors with Compatibility Mode is enabled on the Advanced tab of Internet Option. |

Memory settings

Memory settings depend on many factors, such as the level of activity expected on the server, the complexity of the IBM Cognos applications, the number of users and requests, and acceptable response times.
If your environment supports more than 100 named users, is complex, experiences high peak usage periods, or includes any combination of these factors, consider completing a capacity plan. For more information, see IBM Software Services for Cognos (www.ibm.com/software/analytics/cognos/services/).

To determine the settings that are best suited for your environment, performance testing is advised.

Use the following memory settings as a starting point and adjust them based on the memory usage of your system.

- 2 GB for the base operating system and accompanying software, such as antivirus, back up, and enterprise management software
- 4 GB for a 64-bit Content Manager JVM
- 4 GB for a 64-bit Application Tier JVM
- 2 GB for the graphics JVM (IBM Cognos Workspace)
- 2-4 GB for the query service (dynamic query mode) JVM
- 1 GB per core for the report services processes (dynamic query mode) (JVM)
- 2 GB per core for the report services processes (compatible query mode) (BIBuS)

The following table shows the suggested memory settings by architectural tier for a 64-bit operating system.

Table 5. Suggested memory settings by architectural tier

<table>
<thead>
<tr>
<th>Architectural Tier</th>
<th>Memory settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Cognos Gateway Tier</td>
<td>2 GB</td>
</tr>
<tr>
<td>IBM Cognos Application Tier (compatible query mode)</td>
<td>2 GB per core</td>
</tr>
<tr>
<td>IBM Cognos Application Tier (dynamic query mode)</td>
<td>4 GB + 1 GB per core</td>
</tr>
<tr>
<td>IBM Cognos Content Manager Tier</td>
<td>4 GB</td>
</tr>
</tbody>
</table>

More resources might be required when installing additional software.

Java requirements

To support the cryptographic services in IBM Cognos Business Intelligence, you may be required to update your version of Java or set a JAVA_HOME environment variable. Depending on your security policy requirements, you may also have to install the unrestricted Java Cryptography Extension (JCE) policy file.

You can use an existing Java Runtime Environment (JRE) or the JRE that is provided with IBM Cognos BI.

Cryptographic standards

By default, IBM Cognos BI is configured to support the NIST SP800-131a security standard. To be compliant with this security standard, you must use a JRE that also supports this standard.

The JRE that is provided for installations on Microsoft Windows operating system does support this standard. If you are using another JRE, and you want to use the NIST SP800-131a security standard, you must ensure that the JRE supports the standard.
For more information about the supported Java versions for IBM Cognos BI, see the IBM Software Product Compatibility Reports (SPCR) page (www.ibm.com/support/docview.wss?uid=swg27037784).

For more information about this security standard, see the IBM Java Information Center (publib.boulder.ibm.com/infocenter/java7sdk/v7r0/index.jsp?topic=%2Fcom.ibm.java.security.component.doc%2Fsecurity-component%2Fjsse2Docs%2Fsp800-131a.html).

JAVA_HOME

Set a JAVA_HOME environment variable if:

- You are installing on a UNIX or Linux operating systems.
- You are installing on Microsoft Windows operating systems and you want to use your own Java or a Java bundled with other software. For example, if you are installing IBM Cognos BI on WebSphere® Application Server.

Ensure that the JRE version is supported by IBM Cognos products.

On Microsoft Windows operating systems, if you do not have a JAVA_HOME variable, the JRE files that are provided with the installation are used.

To verify that your JRE is supported, go to the IBM Software Product Compatibility Reports (SPCR) page (www.ibm.com/support/docview.wss?uid=swg27037784). Click the link for your version of Cognos BI and locate the Java Run Time Libraries information.

Unrestricted JCE Policy File

JREs include a restricted policy file that limits you to certain cryptographic algorithms and cipher suites. If you require a wider range of cryptographic algorithms and cipher suites than are shown in IBM Cognos Configuration, you can download and install the unrestricted JCE policy file.

For Java that is provided by IBM, the unrestricted JCE policy file is available on the IBM website (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcSDK).

Review the Default Port Settings for IBM Cognos Business Intelligence

After installation, you can use the configuration tool to change the settings. You can also change them by editing the cogstartup.xml file.

Default Port Settings for IBM Cognos BI Components

The following table lists the default ports and URI settings for IBM Cognos Business Intelligence.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Manager URI</td>
<td><a href="http://localhost:9300/p2pd/servlet">http://localhost:9300/p2pd/servlet</a></td>
<td>The URI to Content Manager</td>
</tr>
<tr>
<td>Gateway URI</td>
<td><a href="http://localhost:80/ibmcognos/cgi-bin/cognos.cgi">http://localhost:80/ibmcognos/cgi-bin/cognos.cgi</a></td>
<td>The URI to the gateway</td>
</tr>
</tbody>
</table>
Table 6. Default Port Settings for IBM Cognos BI Components (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dispatcher URI</td>
<td><a href="http://localhost:9300/p2pd/servlet/dispatch">http://localhost:9300/p2pd/servlet/dispatch</a></td>
<td>The URI to the dispatcher</td>
</tr>
<tr>
<td>(Internal, External)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dispatcher URI for external</td>
<td><a href="http://localhost:9300/p2pd/servlet/dispatch">http://localhost:9300/p2pd/servlet/dispatch</a></td>
<td>The URI to the dispatcher</td>
</tr>
<tr>
<td>applications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dispatcher URIs for Gateway</td>
<td><a href="http://localhost:9300/p2pd/servlet/dispatch/ext">http://localhost:9300/p2pd/servlet/dispatch/ext</a></td>
<td>The URI to the primary dispatcher used by the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>gateway</td>
</tr>
<tr>
<td>Log server port</td>
<td>9362</td>
<td>The port used by the local log server</td>
</tr>
<tr>
<td>Listening port number</td>
<td>1527</td>
<td>The port used by Cognos Content Database.</td>
</tr>
</tbody>
</table>

Default Port Settings for Tomcat

The following table lists the default settings used by IBM Cognos BI for Tomcat. The non-SSL and SSL connectors are automatically updated in the server.xml file when you use IBM Cognos Configuration to change the dispatcher port or to enable the SSL protocol. You can directly update the shutdown port using IBM Cognos Configuration.

Table 7. Default Port Settings for Tomcat

<table>
<thead>
<tr>
<th>Setting</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-SSL Coyote HTTP/1.1</td>
<td>9300</td>
<td>The port Tomcat uses to pass requests from the Web server to IBM Cognos BI</td>
</tr>
<tr>
<td>Connector</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL Coyote HTTP/1.1</td>
<td>9334</td>
<td>The port Tomcat uses to listen for secure connections</td>
</tr>
<tr>
<td>connector</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shutdown port</td>
<td>9399</td>
<td>The port Tomcat uses to listen for a shutdown command</td>
</tr>
</tbody>
</table>

Default Port Settings for Migration

The following table lists the default settings used in migration from IBM Cognos Series 7 to IBM Cognos BI PowerPlay.

Table 8. Default Port Settings for Migration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration Service Port</td>
<td>21567</td>
<td>The port used for communications between IBM Cognos Series 7 migration</td>
</tr>
<tr>
<td>Number</td>
<td></td>
<td>service and IBM Cognos BI migration service</td>
</tr>
<tr>
<td>PPBOOKMARKTOOL_PORT</td>
<td>7777</td>
<td>The port used for bookmark migration</td>
</tr>
</tbody>
</table>
Guidelines for creating the content store

The content store is a database that Content Manager uses to store global configuration data, global settings (such as the language and currency formats shown in the user interface), connections to data sources, and product-specific content. You must use one of the supported enterprise-level databases as the content store in a production environment.

Do not use Cognos Content Database for the content store in a production environment. Cognos Content Database is provided to help you quickly set up a test or proof-of-concept system.

Design models and log files are not stored in the content store.

You must create the content store before you can use your IBM Cognos Business Intelligence product.

If you are using IBM DB2 for your content store, you can generate a DDL to allow your database administrator to create a DB2 database suitable for the content store. For more information, see “Generating a script file to create a database for a DB2 content store” on page 61.

Database properties

You must create the content store database using one of the databases listed in the following table.

The following table shows the character encoding and protocol that is used by the different types of databases.

Table 9. Character encoding and protocols for the content store database

<table>
<thead>
<tr>
<th>Database</th>
<th>Character encoding</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2</td>
<td>UTF-8</td>
<td>TCP/IP</td>
</tr>
<tr>
<td>Oracle</td>
<td>AL32UTF8 or AL32UTF16</td>
<td>TCP/IP</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>UTF-8 or UTF-16</td>
<td>TCP/IP</td>
</tr>
<tr>
<td>Informix</td>
<td>UTF-8</td>
<td>TCP/IP</td>
</tr>
<tr>
<td>Sybase</td>
<td>UTF-8</td>
<td>TCP/IP</td>
</tr>
<tr>
<td>Cognos Content Database</td>
<td>preconfigured</td>
<td>preconfigured</td>
</tr>
</tbody>
</table>

If you plan to use the Cognos Content Database as your content store, a database is created and preconfigured when the installation is complete.

Collation sequence

Cognos BI uses a single sort order that specifies the rules used by the database to interpret, collect, compare, and present character data. For example, a sort order defines whether the letter A is less than, equal to, or greater than the letter B; whether the collation is case sensitive; and whether the collation is accent sensitive. For more information about collation and collation sequences, see the [ICU](http://site.icu-project.org/) web site, select the User Guide, and search for Collation.
Suggested settings for creating the content store in DB2 on Linux, Windows, and UNIX operating systems

The database you create on the Microsoft Windows, Linux, or UNIX operating system for the content store must contain the specified configuration settings.

To ensure a successful installation, use the following guidelines when creating the content store. Use the same guidelines to create a database for log messages.

Library files for DB2

Ensure that you use the appropriate library files for the version of the IBM Cognos Business Intelligence server that you install. IBM Cognos BI requires 32-bit library files when running in a 32-bit application server and it requires 64-bit library files when running in a 64-bit application server. Depending on the version of DB2 that installed, you may have to change the library files or change the order in which the library files are listed so that IBM Cognos BI server can find the correct files. Whichever version of library files is needed must be listed first.

Guidelines for creating the content store

Use the following checklist to help you set up the content store on DB2.

- Set the appropriate environment variables for DB2, which are as shown in the following table.

Table 10. Environment variables for DB2

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2PATH</td>
<td>The top-level directory that contains the database client software or the entire database installation.</td>
</tr>
<tr>
<td>LD_LIBRARY_PATH</td>
<td>The load library path. You must add the driver location and indicate the 32-bit or 64-bit library files as appropriate for your application server.</td>
</tr>
<tr>
<td></td>
<td>For example (replace the double hash symbol with the library file value, either 32-bit or 64-bit), LD_LIBRARY_PATH= $DB2_location/sqllib/lib##: $LD_LIBRARY_PATH</td>
</tr>
<tr>
<td></td>
<td>Examples (replace ## with 32 or 64 as appropriate):</td>
</tr>
<tr>
<td></td>
<td>For Solaris and Linux:</td>
</tr>
<tr>
<td></td>
<td>LD_LIBRARY_PATH= $DB2DIR/lib##: $LD_LIBRARY_PATH</td>
</tr>
<tr>
<td></td>
<td>For AIX:</td>
</tr>
<tr>
<td></td>
<td>LIBPATH=$DB2DIR/lib##$LIBPATH</td>
</tr>
<tr>
<td></td>
<td>For HP-UX:</td>
</tr>
<tr>
<td></td>
<td>SHLIB_PATH=$DB2DIR/ \lib##$SHLIB_PATH</td>
</tr>
<tr>
<td>DB2INSTANCE</td>
<td>The default database server connection.</td>
</tr>
</tbody>
</table>
Table 10. Environment variables for DB2 (continued)

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2CODEPAGE</td>
<td>Setting this optional environment variable to a value of 1208 provides support for multilingual databases. For information about whether to use this environment variable, see the DB2 documentation.</td>
</tr>
</tbody>
</table>

- Use **UTF-8** as the code set value when you create the database. To check that your database has the correct code set, using the command-line interface, and type the following at the command prompt:
  
  `db2 get database configuration for database_name`
  
  The code set value is UTF-8 and the code page value is 1208.

- Ensure that you set the configuration parameters as shown in the following table.

Table 11. Configuration parameters for DB2

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application heap size</td>
<td>AUTOMATIC or at least 1024 KB</td>
</tr>
<tr>
<td>(applheapsz)</td>
<td>If the application heap size value is too small, out of memory errors may occur when there are many users.</td>
</tr>
<tr>
<td>Lock timeout (locktimeout)</td>
<td>240 seconds</td>
</tr>
<tr>
<td></td>
<td>Do not set this to an infinite timeout value.</td>
</tr>
<tr>
<td>DB2 registry variable</td>
<td>YES</td>
</tr>
<tr>
<td>(DB2_INLIST_TO_NLJN)</td>
<td>Setting this variable to YES improves performance.</td>
</tr>
</tbody>
</table>

- Create a buffer pool with a page size of 32 KB, and a second one with a page size of 8 KB.
- Create a system temporary tablespace using the 32 KB buffer pool you created in the previous step.
- Create a user temporary tablespace using the 8 KB buffer pool you created. Global temporary tables will be created in the user temporary tablespace.
- Create a regular user tablespace using the 8 KB buffer pool you created. If you are also creating a logging database, create an additional regular user tablespace with a page size of 8 KB.
- Grant the following database privileges for the user account IBM Cognos BI will use to access the database:
  - Connect to database
  - Create tables
  - Create schemas implicitly

**Tip:** If you want to host more than one content store on your DB2 instance and you use both at the same time, use a different user account for each content store to ensure that each IBM Cognos BI instance is fully isolated from the other.
• Ensure that the user account has use privileges for the user temporary tablespace and other appropriate tablespaces associated with the database.
• Create a schema for the user account IBM Cognos BI that you will use to access the database, and ensure the user has create, drop, and alter permissions for the schema.
• Create a profile that sources the sqllib/db2profile from the DB2 user's home directory. For example, the content of your profile will be similar to the following:

```
if [ -f /home/db2user/sqllib/db2profile ]; then
  ./home/db2user/sqllib/db2profile
fi
```
• Your database administrator must back up IBM Cognos BI databases regularly because they contain the IBM Cognos data. To ensure the security and integrity of databases, protect them from unauthorized or inappropriate access.

### Suggested settings for creating the content store in DB2 on z/OS

The database you create for the content store must contain the specified configuration settings.

To ensure a successful installation, use the following guidelines when creating the content store.

Use the following checklist to help you set up the content store in DB2 on z/OS.

- Log on to the z/OS system as a user with System Administrator (SYSADM) or System Control (SYSCtrl) privileges in DB2 to create the database.
- Create a database instance, storage group, and a user account for the content store.
- Ensure that you reserve a buffer pool with a page size of 32 KB, and a second one with a page size of 4 KB for the database instance.
- Administrators must run a script to create table spaces to hold Large Objects and other data for the content store and grant user rights to the table spaces. For information about running the script, see "Creating tablespaces for a content store on DB2 for z/OS" on page 61.
- Your database administrator must back up the content store regularly because it contains the IBM Cognos data application and security information. To ensure the security and integrity of the content store database, protect it from unauthorized or inappropriate access.

### Suggested settings for creating the content store in Oracle

The database you create for the content store must contain the specified configuration settings.

To ensure a successful installation, use the following guidelines when creating the content store. Use the same guidelines to create a database for log messages.

Use the following list to help you set up the content store on Oracle.

- Ensure that the parameter for the database instance compatibility level of the content store database is set to 9.0.1 or higher.
For example, you can check the COMPATIBLE initialization parameter setting by issuing the following SQL statement:

```
SELECT name, value, description FROM v$parameter WHERE name='compatible';
```

For information about changing an instance configuration parameter, see the Oracle documentation.

- Determine if the database is Unicode.

**Tip:** One method is to type the following select statement:

```
select * from NLS_DATABASE_PARAMETERS
```

If the result set returns an NLS_CHARACTERSET that is not Unicode, create a new database and specify AL32UTF8 for the database character set parameters.

- Determine which user account is to access the database.

**Tip:** If you want to host more than one content store on your Oracle instance and you will use both at the same time, use a different user account for each content store to ensure that each IBM Cognos Business Intelligence instance is fully isolated from the others.

- Ensure that the user account that accesses the database has permission to do the following:
  - Connect to the database
  - Create, alter, and drop triggers, views, procedures, and sequences
  - Create and alter tables
  - Insert, update, and delete data in the database tables

- Your database administrator must back up IBM Cognos BI databases regularly because they contain the Cognos data. To ensure the security and integrity of databases, protect them from unauthorized or inappropriate access.

### Suggested settings for creating the content store in Microsoft SQL Server

The database you create for the content store must contain the specified configuration settings.

To ensure a successful installation, use the following guidelines when creating the content store. Use the same guidelines to create a database for log messages.

Use the following checklist to help you set up the content store on Microsoft SQL Server.

- Ensure that the collation sequence is case-insensitive.

  In a Custom installation, you choose a collation, which includes character sets and sort order, during the Microsoft SQL Server setup. In a Typical installation, the installation uses the locale identified by the installation program for the collation. This setting cannot be changed later.

- When connecting to Microsoft SQL Server Management Studio to create the database, use Microsoft SQL Server authentication.

  If you connect using Microsoft Windows operating system authentication, the database that you create will also use Windows authentication. In this situation, you must configure the database connection using a database type of **SQL Server database (Windows Authentication)** in IBM Cognos Configuration.

- For the user account that will be used to access the database, create a new login under **Security** and use the following settings:
  - Select **SQL Server authentication**.
– Clear the Enforce password policy check box.

**Tip:** If you want to host more than one content store on your Microsoft SQL Server instance and you will use both at the same time, use a different user account for each content store to ensure that each IBM Cognos Business Intelligence instance is fully isolated from the others.

- For Microsoft SQL Server 2008, grant EXECUTE permission to the user account that accesses the database.
- For the content store database, create a new database under Databases.
- Under Security for the new database, create a new schema and assign a name to it.
- Under Security for the new database, create a new user with the following settings:
  - For Login name, specify the new login that you created for the user account.
  - For Default schema, specify the new schema.
  - For Owned Schemas, select the new schema.
  - For Role Members, select db_datareader, db_datawriter, and db_ddladmin.

**Suggested settings for creating the content store in IBM Informix Dynamic Server**

The database that you create for the content store must contain specific configuration settings.

Use the following guidelines when creating the content store. Use the same guidelines to create a database for log messages.

Use the following checklist to help you set up the content store on the IBM Informix Dynamic Server database.

- Set the following environment variables:
  - GL_USEGLU - To enable International Components for Unicode (ICU) functionality in Informix Dynamic Server, set the value to 1.
  - DB_LOCALE - To set the database locale to Unicode, specify en_us.utf8.
- In the file ONCONFIG.instance_name, set the property SHMBASE to 0x14000000L.
- Create a database in mode ANSI and with logging turned on.
- For the user account that you use to access the database, grant the DBA database privilege.

**Important:** If you host more than one database on your Informix instance and use them at the same time, use a different user account for each database. You must also define the user account in each instance of the IBM Cognos Configuration application by creating an advanced property parameter and specifying the user account as the value. For multiple content store databases, name the property CMSCRIPT_CS_ID. For multiple logging databases, name the property IPFSCRIPTIDX.

**Suggested settings for creating the content store in Sybase**

The database you create for the content store must contain the specified configuration settings.
To ensure a successful installation, use the following guidelines when creating the content store. Use the same guidelines to create a database for log messages.

Use the following checklist to help you set up the content store on Sybase.
- On the Sybase server, create a server instance with an 8 KB server page size.
  For instructions, see the Sybase documentation.
- If required, install jConnect 6.
  This tool sets up the communication between the JDBC driver and the Sybase Adaptive Server instance.
  For instructions, see the Sybase documentation.
  If your version of Sybase does not include JConnect 6, you must download the installer from Sybase's Web site.
- Add the UTF-8 character set to the server instance.
- If required, make UTF-8 the default character set on the server.
- Create a database device.

  **Tip:** Set log segment to a minimum of 10 MB.
- Set the new database device as the default.
  Information about the new database will be stored in the new database device.
  Keep a backup of the database device for recovery purposes.
- Create the database.
- Determine which user account will be used to access the database.

  **Tip:** If you want to host more than one content store on your Sybase instance and you will use them at the same time, use a different user account for each content store to ensure that each IBM Cognos Business Intelligence instance is fully isolated from the others.
- Ensure that the user account has the following privileges for the database: create default, create procedure, create rule, create table, and create view.
- Ensure that the database has the following settings and is restarted:
  - create and drop table privileges for the user account
  - Select into property is set to True

### Configure a User Account or Network Service Account for IBM Cognos Business Intelligence

You can configure either a user account or a network service account for IBM Cognos Business Intelligence.

The user or network service account under which IBM Cognos BI runs must:
- have access to all required resources, such as printers
- have the rights to log on as a service and act as part of the operating system

In addition, the user account must be a member of the local administrator group.

For example, to print reports using a network printer, the account must have access to the network printer, or you must assign a logon account to the IBM Cognos service.
**Configure a User Account**

For Microsoft Windows operating system, assign a logon account to the IBM Cognos service. You can configure the IBM Cognos service to use a special user account by selecting the IBM Cognos service from the list of services shown in the Services window in Windows. You can then define the user account properties.

For UNIX or Linux operating system, create a new UNIX or Linux group named cognos, for example. This group must contain the user that owns the IBM Cognos files. Change the group ownership of the IBM Cognos files to the cognos group and change the file permissions for all IBM Cognos files to GROUP READABLE/WRITABLE/EXECUTABLE.

You must configure the Web Server to use aliases. For more information, see the IBM Cognos BI Installation and Configuration Guide.

**Configure a Network Service Account**

The network service account is the built in account NT AUTHORITY\NetworkService in the operating system. Administrators do not need to manage a password or maintain the account.

Use an account with administrator privileges if you are installing on Windows Server 2008.

You must configure the Web server to use the application pool. For more information, see the IBM Cognos Business Intelligence Installation and Configuration Guide. You also need the appropriate write permissions to install to the directory.

**Configure Web Browsers**

IBM Cognos Business Intelligence products use default browser configurations. Additional required settings are specific to the browser.

**Browser Settings Required for IBM Cognos BI Portal**

The following table shows the settings that must be enabled.

*Table 12. Enabled Browser Settings for IBM Cognos BI Portal*

<table>
<thead>
<tr>
<th>Browser</th>
<th>Setting</th>
<th>IBM Cognos component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer (settings for studios and portals)</td>
<td>Allow Cookies</td>
<td>IBM Cognos Connection</td>
</tr>
<tr>
<td></td>
<td>Active Scripting</td>
<td>IBM Cognos Administration</td>
</tr>
<tr>
<td></td>
<td>Allow META REFRESH</td>
<td>Cognos Viewer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Studio</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerPlay Studio</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IBM Cognos Workspace</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IBM Cognos Workspace Advanced</td>
</tr>
</tbody>
</table>
Table 12. Enabled Browser Settings for IBM Cognos BI Portal (continued)

<table>
<thead>
<tr>
<th>Browser</th>
<th>Setting</th>
<th>IBM Cognos component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefox</td>
<td>Allow Cookies</td>
<td>IBM Cognos Connection</td>
</tr>
<tr>
<td></td>
<td>Enable Java</td>
<td>IBM Cognos Administration</td>
</tr>
<tr>
<td></td>
<td>Enable JavaScript</td>
<td>Cognos Viewer</td>
</tr>
<tr>
<td></td>
<td>Load Images</td>
<td>Report Studio</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Analysis Studio</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerPlay Studio</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IBM Cognos Workspace</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IBM Cognos Workspace Advanced</td>
</tr>
<tr>
<td>Safari 5</td>
<td>Enable Java</td>
<td>IBM Cognos Connection</td>
</tr>
<tr>
<td></td>
<td>Enable JavaScript</td>
<td>Cognos Viewer</td>
</tr>
<tr>
<td></td>
<td>Do not Block Popup Windows</td>
<td>IBM Cognos Workspace</td>
</tr>
<tr>
<td></td>
<td>Block Cookies: Never</td>
<td></td>
</tr>
<tr>
<td>Google Chrome</td>
<td>Cookies: Allow local data to be set</td>
<td>IBM Cognos Connection</td>
</tr>
<tr>
<td></td>
<td>Images: Show all images</td>
<td>Cognos Viewer</td>
</tr>
<tr>
<td></td>
<td>JavaScript: Allow all sites to run JavaScript</td>
<td>IBM Cognos Workspace</td>
</tr>
<tr>
<td></td>
<td>Pop-ups: Allow all sites to show pop-ups</td>
<td></td>
</tr>
</tbody>
</table>

If Adblock Plus is installed with Firefox, disable it using the per-page option. Adblock Plus prevents some IBM Cognos Connection resources from working properly.

If you use Microsoft Internet Explorer Version 8, you may receive Adobe link errors when you open PDF documents in the IBM Cognos portal. To prevent these errors, in Internet Explorer, from the Tools menu, select Manage Add-ons, and disable Adobe PDF Reader Link Helper.

If you use a Microsoft Internet Explorer Web browser, then you can add the URL for your gateway(s) to the list of Trusted sites. For example, http://<server_name>::<port_number>/ibmcognos. This enables automatic prompting for file downloads.

For more information, see "IBM Cognos Application Firewall" on page 190.

For more information, see the topic about configuring IBM Cognos Application Firewall in the IBM Cognos Business Intelligence Installation and Configuration Guide.
Cookies Used by IBM Cognos BI Components

IBM Cognos BI uses the following cookies to store user information.

<table>
<thead>
<tr>
<th>Cookie</th>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS_TICKET</td>
<td>Session temporary</td>
<td>Created if IBM Cognos BI is configured to use an IBM Cognos Series 7 namespace</td>
</tr>
<tr>
<td>caf</td>
<td>Session temporary</td>
<td>Contains security state information</td>
</tr>
<tr>
<td>Cam_passport</td>
<td>Session temporary</td>
<td>Stores a reference to a user session stored on the Content Manager server. Administrators can set the HTTPOnly attribute to block scripts from reading or manipulating the CAM passport cookie during a user’s session with their web browser. For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.</td>
</tr>
<tr>
<td>cc_session</td>
<td>Session temporary</td>
<td>Holds session information that is specific to IBM Cognos Connection</td>
</tr>
<tr>
<td>cc_state</td>
<td>Session temporary</td>
<td>Holds information during edit operations, such as cut, copy, and paste</td>
</tr>
<tr>
<td>CRN</td>
<td>Session temporary</td>
<td>Contains the content and product locale information, and is set for all IBM Cognos users</td>
</tr>
<tr>
<td>CRN_RS</td>
<td>Persistent</td>
<td>Stores the choice that the user makes for the view members folder in Report Studio</td>
</tr>
<tr>
<td>PAT_CURRENT_FOLDER</td>
<td>Persistent</td>
<td>Stores the current folder path if local file access is used, and is updated after the Open or Save dialog box is used</td>
</tr>
<tr>
<td>pp_session</td>
<td>Session temporary</td>
<td>Stores session information that is specific to PowerPlay Studio</td>
</tr>
<tr>
<td>qs</td>
<td>Persistent</td>
<td>Stores the settings that the user makes for user interface elements such as menus and toolbars</td>
</tr>
<tr>
<td>userCapabilities</td>
<td>Session temporary</td>
<td>Contains all capabilities and the signature for the current user</td>
</tr>
<tr>
<td>Cookie</td>
<td>Type</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>usersessionid</td>
<td>Session temporary</td>
<td>Contains a unique user session identifier, valid for the duration of the browser session.</td>
</tr>
<tr>
<td>FrameBorder</td>
<td>Session temporary</td>
<td>These cookies store the preferences for export to PDF.</td>
</tr>
<tr>
<td>PageOrientation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PageSize</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDFLayerDimension</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDFOPTS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DimTreeToolbarVisible</td>
<td>Persistent</td>
<td>Stores the setting that determines whether to show or hide the dimension viewer toolbar.</td>
</tr>
<tr>
<td>cea-ssa</td>
<td>Session temporary</td>
<td>Stores the setting that determines whether the user session information is shared with other IBM Cognos BI components.</td>
</tr>
<tr>
<td>BRes</td>
<td>Session temporary</td>
<td>Stores information used to determine the screen resolution to use to render charts.</td>
</tr>
</tbody>
</table>

After upgrading or installing new software, restart the Web browser and advise users to clear their browser cache.
Chapter 4. Upgrade IBM Cognos Business Intelligence

The enhancements in new versions of IBM Cognos Business Intelligence (BI) can affect many parts of your business intelligence environment. Therefore it is best to perform the upgrade in stages. To ensure success, treat upgrading as an IT project that requires careful planning, adequate time, and adequate resources.

**Cognos Upgrade Central website**

The [Cognos Upgrade Central website](http://www.ibm.com/software/analytics/cognos/customercenter/upgrade.html) provides additional information to help you upgrade. For example, frequently asked questions, demonstration videos, and links to additional resources are available on the website.

**Upgrade process**

Every upgrade requires a plan, and each plan follows the same basic upgrade process.

You must plan your upgrade so that you know what to expect at each stage of the process. In the planning stage, you can review the upgrade documentation for information about expected behavior, new features, deprecated features, compatibility between versions, and requirements for preparing your production environment. When you finish the review, you can then conduct a site survey to identify the BI infrastructure, applications, reports, and custom configuration settings. Finally, you can test the upgrade on a subset of your data so that you can fine-tune your reports and data before committing to the full upgrade.

When planning your upgrade, ensure that you perform the following tasks:

- Gather the necessary information, such as the required inputs and expected outputs for each phase.
- Assess the applications in your reporting environment and group similar reports together.
- Install the new software in a test environment and deploy the content to the test environment.
- Test the upgraded applications to ensure that your reports run as expected.
  
  You can use Lifecycle Manager to compare reports from a different version of IBM Cognos BI. For more information, see the Lifecycle Manager documentation.

Deployment and testing is usually an iterative process. Assess any differences between the source and target environments. Move to your production environment when you are satisfied that the deployed applications meet your business requirements.

The following diagram shows a general upgrade workflow and the stages in the upgrade process. The process includes the following stages:

- Creating an upgrade plan, which includes the following activities:
  - Reviewing resources, such as documentation and the [Cognos Upgrade Central website](http://www.ibm.com/software/analytics/cognos/customercenter/upgrade.html)
- Verifying the supported environments to ensure compatibility with your other software by going to the IBM Software Product Compatibility Reports (SPCR) page (www.ibm.com/support/docview.wss?uid=swg27037784). You may also want to check this page if you are thinking of upgrading your operating system.

- Evaluating your existing system to determine what you want to move to your new version of the product.

- Creating a detailed plan to implement your upgrade strategy.
  - Creating a development or test system with the new version of the product.
  - Using the information learned from the development or test system and applying it as you create your QA or production systems.

### Figure 2. Upgrade process

#### A) Prepare: Create an upgrade plan

1. Review resources
   - FAQs
   - Documentation
   - Supported environments

2. Evaluate existing system
   - Audits
   - Surveys
   - Available resources

3. Detailed upgrade plan
   - Milestones
   - Testing
   - Resources

#### B) Validate: Create a test or development system

1. Prepare the environment

2. Upgrade the content store

3. Test applications
   - Validate reports

4. Resolve validation or configuration issues

5. Retest report content

6. Revise upgrade plan

#### C) Execute: Create a QA or production system

1. Prepare the environment

2. Upgrade the content store

3. Test applications
   - Validate reports

4. Resolve validation or configuration issues

5. Retest report content
   - Perform comparison tests

6. Go Live

#### D) Leverage: Adopt new features

- Review new features documentation

---

**Reviewing the documentation**

Documentation is provided from various sources to help you achieve a successful upgrade.
All the documentation is available online at the IBM Cognos Information Center (http://pic.dhe.ibm.com/infocenter/cogic/v1r0m0/index.jsp).

**Procedure**

1. Read the What’s New section in this guide.
   - It contains a list of new, changed, deprecated, and removed features for this release.
2. Read the rest of the Upgrade information in this document.
3. From the IBM Cognos Information Center (http://pic.dhe.ibm.com/infocenter/cogic/v1r0m0/index.jsp), review the latest versions of the documentation listed in the following table.

<table>
<thead>
<tr>
<th>Document</th>
<th>Information to search for</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Cognos PowerPlay Release Notes</td>
<td>Recent issues that can affect an upgrade</td>
</tr>
<tr>
<td>IBM Cognos Business Intelligence New Features</td>
<td>New features that can affect the behavior of existing content</td>
</tr>
<tr>
<td>IBM Cognos Framework Manager User Guide</td>
<td>Upgrading models</td>
</tr>
<tr>
<td>IBM Cognos Transformer User Guide</td>
<td>Upgrading user views and upgrading IBM Cognos Series 7 models</td>
</tr>
<tr>
<td>IBM Cognos Migration Assistant User Guide</td>
<td>Moving content from IBM Cognos Series 7 to IBM Cognos BI.</td>
</tr>
<tr>
<td></td>
<td>The last release of the migration tools was version 10.1.1. You can use these tools to migrate to IBM Cognos Business Intelligence version 10.1.1 (Report Studio or Analysis Studio), and then upgrade the migrated content to IBM Cognos BI version 10.2.0.</td>
</tr>
<tr>
<td></td>
<td>You can also use the migration tools to migrate Series 7 PowerPlay content to IBM Cognos BI PowerPlay version 10.2.0.</td>
</tr>
<tr>
<td>IBM Cognos Lifecycle Manager User Guide</td>
<td>Using Lifecycle Manager to audit trial upgrades.</td>
</tr>
</tbody>
</table>

**Assess applications in your environment before you upgrade**

Preparing to upgrade provides an opportunity to review your existing applications and clean up your source environment.

For example, you might have many applications in your environment. However, it is not uncommon to find that a number of applications are not used or no longer meet your requirements.

Assessing your applications is a useful exercise because it can reduce the number of applications to consider during an upgrade.

An audit of your existing applications can include the following tasks:
- Do a site survey to assess the current production environment and identify areas that require attention during the upgrade. The site survey includes information about the infrastructure, applications, users, and configuration settings.
• Assess the software that you use in your environment and create a list of the software, such as operating systems, web servers, security providers, and databases.

To review an up-to-date list of environments that are supported by IBM Cognos Business Intelligence products, including information on operating systems, patches, browsers, web servers, directory servers, database servers, and application servers, see the IBM Software Product Compatibility Reports (SPCR) page (www.ibm.com/support/docview.wss?uid=swg27037784).

• Complete a detailed assessment of your applications. The usage, age, size, and complexity of your applications are important factors to consider when planning the upgrade. The total size of the applications can have an impact on the time required to complete the upgrade.

• List the following information about your configuration:
  – Configuration settings that you enabled in IBM Cognos Configuration
    Installing the new version of the product in a different location than the existing version lets you compare the settings between the two version. To run the two versions you must ensure that you use unique port numbers, web server aliases, and unique content store databases.
  – Changes to other configuration files
    You must manually change other configuration files during the upgrade. If you changed other configuration files, you must assess the changes that you want to preserve in the upgraded environment. This might include .xml, .txt, and .css files in the configuration, templates, webapps, and webcontent directories.

  Note: If you have modified .ini files, please contact Customer Support to determine whether the changes are supported in the new version of the software.

• Back up your content store database.

After your audit is complete, you can create an upgrade plan.

**Guidelines when upgrading your operating system**

You might want to consider the following guidelines before you upgrade to a later version of the operating system on the computers where IBM Cognos BI is installed:

• Check the IBM Software Product Compatibility Reports (SPCR) page (www.ibm.com/support/docview.wss?uid=swg27037784) to ensure that the IBM Cognos BI version supports the version of the operating system you are thinking of moving to.

• Ensure that the third-party software that is used by IBM Cognos BI is supported on the proposed operating system version. Third-party software would include components, such as database and database drivers, application servers, web servers, and browsers.

• Determine whether you must recompile IBM Cognos BI SDK applications.

• Determine whether you must re-create web deployments, which include web archive (.war) files and enterprise archive (.ear) files.

**Access content from a previous version in the portal**

You can view content from a previous version of IBM Cognos BI in the new version by enabling multi-version coexistence.
Enabling multi-version coexistence can help provide a more seamless experience through the upgrade process by staging the upgrade. You can provide IT with the ability to address business demands for features in the new version. And, at the same time, provide the flexibility to plan an application upgrade to the capacity of your IT department.

For more information, see [How to access content from previous IBM Cognos release from within the IBM Cognos 10 portal on the IBM website](https://www.ibm.com/support/docview.wss?uid=swg21459041).

**Upgrade tasks**

When you upgrade, you perform the following tasks:
1. Install and configure the new version of the product.
2. Move your content to the new version of the product.
3. Upgrade your report specifications.
4. Compare your upgraded content to your existing content to ensure consistency.

**Install and configure a new version of the product**

Install the new version of the product to a new location. The location can be on the same computer as your existing version of the product or on another computer.

Installing to a new location allows you to maintain your existing version of the product and run it in addition to the new version of the product. This can help you test your new version without affecting your existing version. You can compare the configuration settings between version and compare the appearance and functionality of the reports in both environments to ensure equivalency.

**Considerations for running multiple versions or instances of IBM Cognos BI on the same computer**

To have multiple versions or instances of IBM Cognos Business Intelligence on the same computer you must change the configuration to ensure that the versions do not share port numbers or other resources.

**Required configuration changes for running multiple versions on the same computer**

To run multiple versions of IBM Cognos Business Intelligence on the same computer, ensure that each installation is distinct. The versions or instances must be installed in different directories. The configuration settings for each version must use different settings for the following configuration properties.

**Ports and URI settings**

If you are using Tomcat, you must use different port numbers to avoid port conflicts. Because IBM Cognos BI reserves a port range, ensure that you use an offset of 100 for the ports. Change the following ports.

- Dispatcher URIs for gateway
- External dispatcher URI
- Internal dispatcher URI
- Dispatcher URI for external applications
- Content Manager URIs
- Local log server port number
- Shutdown port number
The default port numbers for Tomcat start at 9300. If you are installing another version of the product, ensure that you do not use the same values for your second version.

If you are installing the product on an application server other than Tomcat, ensure that you install the new version to a new profile or a separate instance than your existing version.

**Content store**

Use a different content store or schema for each installation. When the content store is upgraded you cannot revert the content. You can use a restored copy of your existing content store as the content store for the newer version of IBM Cognos Business Intelligence. The newer version of the product upgrades the content store when you start the services.

**Web server virtual directories**

To view static content for IBM Cognos Business Intelligence, the virtual directories for the web server must be different for each version. Ensure that you update the Gateway URI in Cognos Configuration to reflect the names of the virtual directories.

For example, the default virtual directory is `http://servername/ibmcognos`. If you have two gateways installed on the same computer, you must change the `ibmcognos` virtual directory for one of the gateways.

**Application pools (Microsoft IIS web server)**

If you use `cognosisap.dll`, each gateway must use a separate application pool.

**User account that starts the service (optional)**

Changing the user account might be helpful when you are troubleshooting. For example, you can troubleshoot Java processes by owner.

**Configuration settings that are the same for multiple versions on the same server**

Multiple instances or versions of IBM Cognos Business Intelligence running on the same computer use the same resources, such as memory, network, and disk space.

Multiple versions of IBM Cognos can use the same authentication source for both versions. You can configure identical properties for the namespace.

**Customized configuration files**

If you manually edited any configuration files, you must reapply the changes. Keep a record of any customizations to ensure that they can be reapplied after upgrading. Also, back up these files so that the original version can be restored if necessary.

The IBM Cognos BI presentation service supports automatic upgrade of some `system.xml` files. If you made many customization changes to `system.xml` files, you can use this automatic upgrade feature instead of reapplying the changes manually after upgrading. By replacing the `system.xml` files with those from your earlier version of the product, the files can be upgraded by the new version of the product. The automatic upgrade is applied when you start the IBM Cognos service.

The `system.xml` files for which automatic upgrade is supported are in the following directories:
Configuring a second instance of IBM Cognos BI on one computer

To have more than one instance of IBM Cognos Business Intelligence on one computer, you must configure each instance with unique values for ports, the web server virtual directory, and content store database.

Before you begin

For the new version of the product, you require a new content store. If you are upgrading your entire content store, create a content store from a backup of your existing content store. If you are moving your content with deployment archives you can create a blank content store database.

Ensure that you have your new content store database in place before you configure the new version of the product.

Important: If you are connecting to a backup of your content store, the first time you start your IBM Cognos services, you are prompted to upgrade your reports. Upgrading your reports can take a long time, and it is better to upgrade them after you have the new version running. You can upgrade your reports afterwards using IBM Cognos Administration.

Procedure

1. For the new instance of IBM Cognos BI, start IBM Cognos Configuration.
2. In the Explorer window, click Environment.
3. Ensure that the port numbers for the following settings do not conflict with your other instance or version of IBM Cognos BI:
   - Dispatcher URIs for gateway
   - External dispatcher URI
   - Internal dispatcher URI
   - Dispatcher URI for external applications
   - Content Manager URIs
4. Ensure that the Gateway URI uses a different virtual directory or alias than your other instance or version of IBM Cognos BI.
5. Click Logging, and ensure that the Local log server port number is unique.
6. If you are using Tomcat as the application server, click IBM Cognos, and ensure that the Shutdown port number is unique.
   - If you are using another application server, such as WebSphere, this value is not used.
7. If you are using Portal Services, update the applications.xml file location:
   - In the Explorer window, click Environment > Portal Services.
   - In the Properties window, ensure that the port number for the Location of applications.xml property matches the port number for the other URI properties.
8. In the Explorer window, under Data Access > Content Manager, ensure that you do not use the same content store that is used for your other instance or version of IBM Cognos BI.
9. Save the configuration, and start IBM Cognos BI.

Move your content to the new version of the product

There are two methods for moving your content.

Move your entire content store

This method requires you to make a backup of your existing content store, and then restore the backup to a new content store. You then connect your new version of the product to the restored content store, and the product upgrades the content store to the new version.

This method maintains all of your security and user preferences, but it does require a new content store database.

When configuring security, ensure that you set the unique identifier to the same value as it was in the release that you are upgrading from, otherwise the security settings will be lost. For more information, see “Enable Security” on page 67.

Run a consistency check on your content store before you upgrade to ensure that there are no inconsistencies. For more information, see the “Create a Content Store Maintenance Task” topic in the IBM Cognos Business Intelligence Administration and Security Guide.

Important: When you use this method, the first time you start your IBM Cognos services, you are prompted to upgrade your reports. Upgrading your reports can take a long time, and it is better to upgrade them after you have the new version running. Additionally, if you have Software Development Kit applications that create, modify, or save report specifications, do not select the option to upgrade your report specifications. You can upgrade your reports afterwards using IBM Cognos Administration.

Also, you must ensure you unregister any dispatchers from your previous version of the product. You can do so using IBM Cognos Administration after you have started the services.

Move content by creating deployment archives

You can move content by creating deployment archives.

This method lets you move specific content, but it can be time consuming for a large content store.

If you are changing content store database vendors, you must create deployments to move your content. For example, if you are changing your content store from Microsoft SQL Server to IBM DB2, you must do so with deployment archives.

Considerations for both methods

NC tables must be completely empty before performing the upgrade. Run the appropriate NC DROP Database Type.sql before you upgrade. For more information, see “Running Database and Index Cleanup Scripts” on page 323.

As part of the upgrade process, ensure that your applications work as expected in the new version. Sometimes, changes can introduce unexpected results. It is
important to test your applications with the new version of the product before you move them to your production environment.

**Upgrade your content store**

IBM Cognos BI upgrades the content store database to the new version of the product when you start the services for the first time.

The process for upgrading your content store to the new version of the product includes the following steps:

1. Make a backup of your existing content store database.
2. Create a database from the backup.
   - If your content store is on DB2 on z/OS, you must run a script to upgrade the content store before you start the services in IBM Cognos Configuration.
3. Connect the new version of the product to the content store that you created from the backup in IBM Cognos Configuration.
4. Start your services.
   - The content store is upgraded during the startup process.

**Important:** When you use this method, the first time you start your IBM Cognos services, you are prompted to upgrade your reports. Upgrading your reports can take a long time, and it is better to upgrade them after you have the new version running. You can upgrade your reports afterwards using IBM Cognos Administration. Additionally, if you have Software Development Kit applications that create, modify, or save report specifications, do not select the option to upgrade your report specifications.

This process lets you use the old and new versions of the product at the same time, where each version has its own content store.

**Important:** When you connect the new version of the product to the content store you created from the backup, the content store database is upgraded, and can no longer be used with your older version of the product.

**Upgrading a content store on IBM DB2 on z/OS:**

To upgrade the content store on DB2 on z/OS, run a script that creates new tablespaces and grants Content Manager the rights to use the tablespaces.

**Before you begin**

To run the script, you must have permission to create tablespaces. Run the script before you save the configuration for the new version.

**Procedure**

1. Go to the `c10_location\configuration\schemas\content\db2zOS` directory and open `tablespaceUpgrade_db2zOS.sql` in a text editor.
2. Follow the instructions in the script file to replace the placeholder values in the file with the values for your database.
3. Save and run the file.

**Unregister previous version dispatchers from your content store:**

If you use a backup of your existing content store with a new version of the product, you must unregister the dispatchers from your previous version.
Procedure
1. Open IBM Cognos Connection in your web browser.
2. In the upper-right corner, click Launch, IBM Cognos Administration.
3. Click Configuration, and then click Dispatchers and Services.
4. Click More for the dispatchers belonging to your previous version.
5. Click Unregister, and then click OK.
   The dispatcher information is removed from the content store.

Upgrading a logging database on IBM DB2 on z/OS:
To upgrade the logging database on DB2 on z/OS, run a script that creates new tablespaces and grants the rights to use the tablespaces.

Before you begin
To run the script, you must have permission to create tablespaces. Run the script before you save the configuration for the new version.

Procedure
1. Go to the \configuration\schemas\logging\db2zOS directory and open LS_tablespaceUpgrade_db2zOS.sql in a text editor.
2. Follow the instructions in the script file to replace the placeholder values in the file with the values for your database.
3. Save and run the file.

Moving your content with a deployment archive
To move specific content from your content store you can use deployment archives. Deployment archives are compressed files that you can then import into your new version of the product.

Important: If you have moved your content by restoring your existing content store, you do not need to move your content using deployment archives.

Moving your content with deployment archives involves the following steps:
1. Creating the archive.
2. Copying the archive to the new version of the product.
3. Importing the content.

Creating a deployment archive:
Use the following task to create a deployment archive.

Procedure
1. In IBM Cognos Administration, on the Configuration tab, click Content Administration.
2. On the toolbar, click the New Export icon.
3. Enter Name for the archive.
4. Select the content you want to include in the archive:
   • To export specific folders and directory content, click Select public folders and directory content.
• To export the entire content store, click Select the entire content store. If you select the entire content store, you can also select Include user account information.

5. Click Next.

6. If you clicked Select the entire content store, enter a password to be used when you import the content, and then click OK.

7. If you clicked Select public folders and directory content:
   a. On the Select the Public folders content panel, click Add.
   b. On the Select entries panel, in the Available Entries box, select the packages or folders that you want to export.
      You can browse the Public Folders hierarchy and choose the packages and folders that you want. Click the Add icon to move the selected items to the Selected entries box, and click OK.
   c. For each package and folder that you export, do the following, and then click Next:
      • If you want to make any changes to the package or folder in the target environment, click the Edit icon, make your changes, and click OK.
      • To restrict access to the package or folder and its entries, select the check box in the Disable after import column. This is useful when you want to test the reports before you make them available in the target environment.
      • Under Options, select whether you want to include the report output versions, run history, and schedules and what to do with entries when there is a conflict.
   d. On the Select the directory content panel, select the options that you want, and click Next.
   e. On the Specify the general options panel, select the options that you want, and click Next.
   f. On the Specify a deployment archive panel, select an existing deployment archive from the list, or create one.
      If you are typing a new name for the deployment archive, do not use spaces in the name. If the name of the new deployment specification matches the name of an existing deployment archive, the existing deployment archive is overwritten.

8. Review the summary information and click Next.

9. Under Actions, select Save and run once.

10. On the Run with options panel, select Now and click Run.

Results

A deployment archive is created in the deployment directory where you installed IBM Cognos BI.

Copying the deployment archive to your new version:

You must manually copy the deployment archives from the instance where they were created to your new instance.
Procedure

Copy the deployment archives you created from the old_version_install_location/deployment directory to the new_version_install_location/deployment directory.

Note: The deployment directory is configurable in IBM Cognos Configuration. By default, the location is install_location/deployment. If you are using a different location, ensure that you copy the deployment archives to the appropriate directory.

Including configuration objects when you import a deployment archive of the entire content store:

You can include configuration objects when importing an entire content store. For example, you might want to import the configuration because you have a series of advanced settings for your services that you want from the source environment.

By default, configuration objects are excluded when you import an entire content store, even though they are included in the export. Configuration objects include dispatchers and configuration folders used to group dispatchers.

Procedure

1. In IBM Cognos Administration, on the Configuration tab, click Dispatchers and Services.
2. Click the dispatcher you want.
3. Next to ContentManagerService, click the set properties icon.
4. Click the Settings tab.
5. In the Value column, click Edit.
6. Select the Override the settings acquired from the parent entry check box.
7. In the Parameter column, type the following uppercase text:
   CM.DEPLOYMENTINCLUDECONFIGURATION
8. In the Value column, type true.
9. Click OK to finish.

Importing a deployment archive:

To import the entries, you create an import deployment specification.

When you import, you select from entries that were exported. You can either accept the default options set during the export, or change them. You can select options that were included in the deployment archive during the export.

If you do a partial deployment of specific public folders and directory content, the import wizard shows whether packages and folders exist in the target environment and the date and time that they were last modified. You can use this information to help you decide how to resolve conflicts. When you redeploy, the wizard also shows whether the packages and folders were in the original deployment.

Before you begin

Ensure that you have copied the deployment archive to the c10_location/deployment directory for your new version of the product.
Procedure

1. For your new version of the product, in IBM Cognos Administration, on the Configuration tab, click Content Administration.

2. On the toolbar, click the new import icon.

3. In the Deployment archive box, select the deployment archive that you want to import, and click Next.

4. If your deployment archive is of your entire content store, type the password entered during the export, and click OK.

5. Type a name for the import and select the folder where you want to save it, and then click Next.

6. Select the content that you want to include in the import, select the options, and click Next.

   Tip: Click the edit icon next to the package if you want to change the target location for the imported content.

7. On the Specify the general options panel, select the options that you want, and click Next.

8. Review the summary information, and click Next.

9. Under Actions, select Save and run once, and click Finish.

10. On the Run with options panel, do the following:

    a. Select Upgrade all report specifications to the latest version if you want to upgrade the report specifications during the import. You can also perform this task after you import the content.

    b. Click Run.

Upgrade your report specifications

Report specifications will have changed from one version of IBM Cognos BI to another. You must upgrade any report specifications created in previous versions of the product.

If you are upgrading from a backup of your existing content store, you should upgrade the report specifications after you have started the services.

If you are moving content to a new version using deployment archives, you can choose to upgrade the import specifications during the import.

If you moved your content using deployment archive you may have selected the option to upgrade your report specifications. If you upgraded the report specifications during the import, you do not have to do it again.

Before you begin

Important: Do not upgrade your report specifications if you have Software Development Kit applications that create, modify, or save report specifications. You must first update your Software Development Kit applications to comply with the IBM Cognos report specifications schema. Otherwise, your Software Development Kit applications may not be able to access the upgraded report specifications. For information about upgrading report specifications, see the IBM Cognos Software Development Kit Developer Guide.
**Procedure**

1. In the upper-right corner, click **Launch, IBM Cognos Administration**.
2. On the **Configuration** tab, click **Content Administration**.

3. Click the arrow on the new content maintenance button on the toolbar, and then click **New Report Upgrade**

4. Type a name for the upgrade task and, if you want, a description and screen tip. Click **Next**.

5. Select the packages and locations for the report specification you want to upgrade. Click **Next**.
   If you upgrade report specifications by package, all reports in the content store that are based on the model in the package will be upgraded. If you upgrade report specifications by folder, all reports in the folder will be upgraded.

6. Choose one of the following:
   - **Save and run once** opens the run with options page.
   - **Save and schedule** opens the scheduling tool.
   - **Save only** allows you to save the upgrade so that you can run it at a later time.

**Use Lifecycle Manager to compare reports between your versions of the product**

Lifecycle Manager lets you verify your upgraded content by comparing reports in your old environment with the reports in your new version of the product.

For more information, see the IBM Cognos Lifecycle Manager documentation.
Chapter 5. Installing and Configuring Product Components on One Computer

You can install all IBM Cognos PowerPlay components on one computer. This is useful when you are setting up a test or evaluation environment, or for small production environments. You can also distribute the installation of IBM Cognos PowerPlay on different computers. After installation, you can customize the components for use in your environment by changing other settings in IBM Cognos Configuration.

To migrate content from IBM Cognos Series 7 to IBM Cognos BI migration components are required on both the IBM Cognos PowerPlay computer and the IBM Cognos Series 7 computers. When you install IBM Cognos PowerPlay the installation automatically includes migration components. You must complete a separate installation to add migration components to IBM Cognos Series 7 computers.

For uninstallation instructions, see Chapter 15, “Uninstalling IBM Cognos BI,” on page 289.

Install the server components

Use the installation wizard to select the server components that you want to install and the location on your computer where you want to install them. Only the components that you choose to install are copied from the disk to your computer.

To use IBM Cognos PowerPlay on one computer, you must install all components that are selected by default in the installation wizard.

If you are installing IBM Cognos PowerPlay with IBM Cognos Business Intelligence Server, install and configure IBM Cognos BI server first. Both products must be the same version.

Application samples for your IBM Cognos BI product are on a separate disk. If you want to use the samples, you must install them from the IBM Cognos Business Intelligence Samples disk.

Stopping the service

If you need to stop the IBM Cognos service, it is important to also stop the following:

- applications that are related to the IBM Cognos service, such as Framework Manager, IBM Cognos Transformer, IBM Cognos Connection, IBM Cognos Administration, and Metric Designer
- any Software Development Kit applications that are running

Upgrading your installation

If you are upgrading from a previous release of IBM Cognos PowerPlay, you must use the upgrading steps.
If you are upgrading from a previous release of IBM Cognos products, see Chapter 4, “Upgrade IBM Cognos Business Intelligence,” on page 39.

If you are upgrading from an earlier version of IBM Cognos BI, all the distributed components must be the same version of IBM Cognos BI. If you install IBM Cognos BI on additional or alternate hosts, you must update location-specific properties in IBM Cognos Configuration.

If you will be using PowerCubes that are secured against an IBM Cognos Series 7 namespace, you must install IBM Cognos PowerPlay on a computer that supports IBM Cognos Series 7.

If you are upgrading IBM Cognos BI in an environment that includes earlier versions of other IBM Cognos BI products, such as IBM Cognos BI Controller Version 8.x, IBM Cognos BI Planning Version 8.x, or IBM Cognos BI Analysis for Microsoft Excel Version 8.x, install the new version of IBM Cognos BI in a separate location from the other IBM Cognos BI product and configure the new version of IBM Cognos BI to operate independently of that product. After you upgrade the other product to a compatible version with IBM Cognos BI, you can then configure the two products to operate together.

64-bit installations

The IBM Cognos BI gateway provides 32-bit libraries, whether you install on a 64-bit server or a 32-bit server. Some Web servers, such as Apache Web Server, cannot load a 32-bit compiled library in a 64-bit compiled server. In that situation, install the 32-bit version of the IBM Cognos gateway on a 32-bit Web server.

The report server component, included with the Application Tier Components, is provided in both 32- and 64-bit versions. Selecting which version you use is done using IBM Cognos Configuration after installation. By default, the report server component is set to use the 32-bit mode, even on a 64-bit computer. The 32-bit mode allows you to run all reports, whereas the 64-bit mode allows you to run only reports created for dynamic query mode.

If you are upgrading IBM Cognos BI in an environment that includes earlier versions of other IBM Cognos BI products, such as IBM Cognos BI Controller Version 8.x, IBM Cognos BI Planning Version 8.x, or IBM Cognos BI Analysis for Microsoft Excel Version 8.x, install the new version of IBM Cognos BI in a separate location from the other IBM Cognos BI product and configure the new version of IBM Cognos BI to operate independently of that product. After you upgrade the other product to a compatible version with IBM Cognos BI, you can then configure the two products to operate together.

Windows installations

For Microsoft Windows operating system installations, ensure that you have administrator privileges for the Windows computer you are installing on. Also ensure that your computer has a TEMP system variable that points to the directory where you want to store temporary files. During installation, files from the disk are temporarily copied to this directory.
UNIX installations

For UNIX operating system installations, you can install server components using a graphical user interface or by running a silent installation. To run graphical-mode installation, the console attached to your UNIX computer must support a Java-based graphical user interface.

Also, IBM Cognos BI respects the file mode creation mask (umask) of the account running the installation program. This affects only the installation directories. It does not affect the file permissions within the directories. However, run-time generated files, such as logs, respect the mask. Use umask 022 on the installation directory.

Cognos Content Database as content store

If you want to use Cognos Content Database as your content store, you must select it in the installation wizard. If you are installing components on several computers, you need to only install Cognos Content Database once.

Printer requirements

To ensure that reports print properly on Windows, Adobe Reader requires that you configure at least one printer on the operating system where Application Tier Components are installed. All reports, regardless of the print format that you choose, are sent as temporary PDF files to Adobe Reader for printing.

Installing server components on UNIX or Linux operating systems

Use the installation wizard to select the server components that you want to install and the location on your computer where you want to install them. Only the components that you choose to install are copied from the disk to your computer.

Before you begin

Go to the IBM Software Product Compatibility Reports (SPCR) page (www.ibm.com/support/docview.wss?uid=swg27037784). Verify that you have the required patches installed on your computer before you install the product.

Procedure

1. If you are installing to a directory with other IBM Cognos BI components, stop the IBM Cognos service.
2. Set the JAVA_HOME environment variable to point to the installation location of your Java Runtime Environment (JRE).
   
   An example of the installation location of a Java Runtime Environment is /directory/java/java_version/jre.
   
   IBM Cognos BI requires a JVM, such as the one that is provided by IBM, to run on Linux operating system.
   
   If you are installing in a location with other IBM Cognos BI components, use the existing JAVA_HOME environment variable.
3. On HP-UX, set the _M_ARENA_OPTS environment variable as follows:
   
   _M_ARENA_OPTS 1:4
   
   This increases the memory allocation for HP-UX to more closely match that of other UNIX platforms.
4. On AIX, if you are using a servlet gateway, set the AIXTHREAD_SCOPE environment variable as follows:

   AIXTHREAD_SCOPE=S

   This sets the contention scope for user threads to system-wide, which supports more efficient scheduling of user threads.

5. If installing from a download, go to the location where the installation files were downloaded and extracted.

6. If installing from a disk, mount the disk using Rock Ridge file extensions.
   To mount the disk on HP-UX, do the following:
   • Add the pfs_mount directory in your path.
     For example,
     
     PATH=/usr/sbin/:$PATH
     export PATH
   • To start the required NFS daemons and run the daemons in the background, type bg pfs_mountd and then type bg pfsd
   • To mount the drive, type
     
     pfs_mount -t rrip <device><mount_dir> -o xlat=unix
     For example,
     pfs_mount /dev/dsk/c0t2d0 /cdrom -o xlat=unix
     You can now install or copy files as a non-root user using an IBM Cognos disk from this drive.
   • When the installation is complete, type pfs_umount /cdrom and kill the pfsd and pfs_mountd daemons to unmount the disk.

7. To start the installation wizard, go to the operating system directory and then type
   ./issetup

    **Note:** When you use the issetup command with XWindows, Japanese characters in messages and log files may be corrupted. When installing in Japanese on UNIX or Linux, first set environment variables LANG=C and LC_ALL=C (where C is the language code, for example ja_JP.PCK on Solaris), and then start the installation wizard.

    If you do not use XWindows, run an unattended installation (see Chapter 12 “Using an unattended installation and configuration,” on page 269).

    If you do not use XWindows, run an unattended installation. For more information, see the Installation and Configuration Guide.

    If you are installing on Linux operating systems, and you receive error messages about missing openmotif libraries, you can use an unattended installation with the issetupnx command.

8. Follow the directions in the installation wizard and copy the required files to your computer.
   Install IBM Cognos BI components in a directory that contains only ASCII characters in the path name. Some UNIX and Linux Web servers do not support non-ASCII characters in directory names.

9. When you are prompted about installing non-English product documentation, click OK to continue.

10. In the Finish page of the installation wizard, do the following:
    • If you want to see the log files, click **View** for the appropriate log file.
• If you want to see late-breaking information about the product, select the check box for IBM Cognos Release Notes.
• Do not configure IBM Cognos BI immediately because you must do other tasks first to ensure that your environment is properly set up. Ensure that the IBM Cognos Configuration check box is clear.
  You can later configure IBM Cognos BI using IBM Cognos Configuration by typing cogconfig.sh in the c10_location/bin64 directory.
• Click Finish.

1. Append the c10_location/bin directory to the appropriate library path environment variable.
   • For Solaris and Linux, LD_LIBRARY_PATH
   • For AIX, LIBPATH
   • For HP-UX, SHLIB_PATH

Results

If you want users to see product documentation in a language other than English, you must install the Supplementary Language Documentation component in the location where you installed the Gateway components. For more information, see “Installing translated product documentation” on page 59.

You must also update your Java security framework (see “Java requirements” on page 24) before you can configure IBM Cognos BI. Otherwise, you may receive the following error:

[Cryptography]
1. [ ERROR ] java.lang.NoClassDefFoundError: java/net/ServerSocketFactory:

Related tasks:
“Cannot run issetup on Linux operating systems” on page 304

You run issetup to install IBM Cognos BI but you receive the following error message:

Installing server components on Windows operating systems

Use the installation wizard to select the server components that you want to install and the location on your computer where you want to install them. Only the components that you choose to install are copied from the disk to your computer.

For Windows Vista, Windows 7, or Windows 2008 computers, the default installation location uses the Program Files (x86) directory. If you install to this location, ensure that you run IBM Cognos Configuration as an Administrator. Alternatively, you can install the product outside of the Program Files (x86) directory. For example, you can change the installation directory to something like C:\IBM\cognos\c10.

Procedure
1. If you are installing in a directory with other IBM Cognos BI components, stop the IBM Cognos service.
2. Do one of the following:
   • Insert the IBM Cognos product disk.
     If the installation wizard does not open automatically, go to the operating system directory, and double-click issetup.exe.
3. Select the language to use for the installation.

   The language that you select determines the language of the user interface. All supported languages are installed. You can change the user interface to any of the installed languages after installation.

4. Follow the directions in the installation wizard to copy the required files to your computer.

   Install IBM Cognos BI components in a directory that contains only ASCII characters in the path name. Some Windows Web servers do not support non-ASCII characters in directory names.

5. When you are prompted about installing non-English product documentation, click OK to continue.

6. In the Finish page of the installation wizard, do the following:

   • If you want to see the log files, click View for the appropriate log file.
   • If you want to see late-breaking information about the product, select the check box for IBM Cognos Release Notes.
   • If you start IBM Cognos Configuration from the installation wizard, ensure that you follow the additional tasks in this section to ensure that your environment is properly set up before you start the services.

   You can start IBM Cognos Configuration using the IBM Cognos Configuration shortcut from the Start menu.

   • Click Finish.

   If you want users to see product documentation in a language other than English, you must install the Supplementary Language Documentation component in the location where you installed the Gateway components. For more information, see “Installing translated product documentation” on page 59.

---

**Installing fix packs**

IBM provides interim maintenance packages that contain updates to one or more components in your IBM Cognos product. If a fix pack is available when you are installing or upgrading your product, you must install it after you install the IBM Cognos components.

Fix packs are cumulative. When you install the latest fix pack, it includes updates from all the previous fix packs. Fix packs are available for download from [IBM Support](http://www.ibm.com/support/entry/portal/overview).

**Note:** Fix packs are not standalone installations. You must install them on computers that have IBM Cognos components installed. Install the fix packs that are appropriate for your product version. To check your version, open the component list file at `c10_location\cmp\list.txt` and check the line that starts with `C8PPCLIENT_version=` for the PowerPlay Client and `C8PPES_version=` for the PowerPlay server version.

### Installing IBM Cognos fix packs on UNIX or Linux operating systems

Fix packs are product updates that contain cumulative code fixes that were made since the last release of the product. IBM Cognos fix packs are installed in the same location as the existing product.
Procedure
1. Go to the location where the installation files are downloaded, or insert the disc if you have one.
2. To start the installation wizard, type the following command.
   ```bash
   ./issetup
   ```
3. Follow the directions in the installation wizard to install the fix pack files to the same location as the existing IBM Cognos components.
4. If required, update the new installation files with any changes from the backup copies of your customized files.
   To prevent errors, before copying the customized files, compare both versions of the files. This validation determines whether you can replace the file.
5. If you have a distributed environment, repeat these steps for all remaining IBM Cognos servers.

Installing Fix Packs on Windows operating systems
Fix packs are product updates that contain cumulative code fixes that were made since the last release of the product. IBM Cognos fix packs are installed in the same location as the existing product.

Procedure
1. Insert the fix pack disk for the Windows operating system or go to the location where you downloaded and extracted the files, and double-click the `issetup.exe` file.
2. Follow the directions in the installation wizard to install the fix pack files to the same location as the existing IBM Cognos components.
3. If required, update the new installation files with any changes from the backup copies of your customized files.
   To prevent errors, before copying the customized files, compare both versions of the files. This validation determines whether you can replace the file.
4. If you have a distributed environment, repeat these steps for all remaining IBM Cognos servers.

Installing translated product documentation
The product installation includes a limited set of translated documentation for some languages, such as installation guides and release notes. To access a complete set of translated documentation, you must install it from IBM Cognos BI Supplementary Language Documentation.

Before you begin
Before installing the Supplementary Language Documentation, ensure that:
- IBM Cognos BI is installed and configured correctly
- adequate disk space is available to install supplementary language documentation
  You need at least 220 MB of disk space.
- your software environment is supported
**Procedure**

1. In the location where the Gateway component is installed, insert the IBM Supplementary Language Documentation disk or go to the directory where the installation files were downloaded and extracted.
   
   On UNIX or Linux operating systems, mount the disk using Rock Ridge file extensions.
   
   On Windows, the installation wizard starts automatically from the product disk.
   
2. To manually start the installation wizard, go to the operating system directory and do the following:
   
   - On Windows, if no Welcome page appears, double-click the issetup.exe file.
   - On UNIX or Linux, type `./issetup`

   **Note:** When you use the issetup command with XWindows, Japanese characters may be corrupted.

3. Follow the instructions in the installation wizard to copy the required files to the same location where you installed gateway components for IBM Cognos BI.
   
   Install in a directory that contains only ASCII characters in the path name. Some Web servers do not support non-ASCII characters in directory names. The supplementary languages documentation components is selected by default.

4. Choose the option you want in the **Finish** page of the installation wizard.

---

**Set up database connectivity for the content store database**

If you are using a database other than Cognos Content Database or Microsoft SQL Server as the content store, you may have to install database client software, or Java Database Connectivity (JDBC) drivers, or both, on each computer where you install Content Manager. Doing this allows Content Manager to access the content store database.

**Set up database connectivity for an IBM DB2 content store**

This procedure describes how to set up database connectivity for a DB2 content store. You must perform this procedure on each computer where you install Content Manager.

You must use a type 4 Java Database Connectivity (JDBC) driver to connect to your content store if you are using IBM DB2.

The type 4 driver is considered an independent product. It does not require the DB2 client to be installed.

**Procedure**

Copy the following files from `DB2_installation\sql1ib\java` directory to the `c10_location\webapps\p2pd\WEB-INF\lib` directory:

- The universal driver file, `db2jcc.jar`
- The license file:
  - For DB2 on Linux, UNIX, or Windows operating systems, use `db2jcc_license_cu.jar`.
  - For DB2 on z/OS, use `db2jcc_license_cisuz.jar`. 
If you are connecting to DB2 on z/OS, use the driver version from Linux, UNIX, or Windows version 9.1 fix pack 5 or version 9.5 fix pack 2.

Tip: To check the driver version, run the following command:
```
java -cp path\db2jcc.jar com.ibm.db2.jcc.DB2Jcc -version
```

Generating a script file to create a database for a DB2 content store
You can generate a script file to automatically create the content store in IBM DB2 on all platforms. The script file is called a DDL file.

Procedure
1. Start IBM Cognos Configuration.
2. In the Explorer window, under Data Access > Content Manager, click Content Store.
   The default configuration is for an IBM DB2 database. Ensure that the Type is DB2 database.
3. In the Database server and port number field, enter the name of your computer and port number on which DB2 is running. For example, localhost:50000. Where, 50000 is the default port number that is used by IBM DB2. If you are using a different port number, ensure you use that value.
4. Click the Value field next to the User ID and password property and then click the edit icon. Type the appropriate values and click OK.
5. In the Properties window, for the Database name property, type the name for your content store database.
   Important: Do not use a name longer than eight characters and use only letters, numbers, underscores, and hyphens in the name.
6. Right-click Content Store, and click Generate DDL.
7. Click Details to record the location of the generated DDL file.
   The DDL file named createDB.sql is created. The script is created in the $c10_location\configuration\schemas\content\db2 directory.

What to do next
Use this script to create a database in IBM DB2. For more information about using a DDL file, see your IBM DB2 documentation.

If you use the IBM DB2 command-line interface, you can run the script by entering the following command:
```
db2 -tvf createDB.sql
```

Creating tablespaces for a content store on DB2 for z/OS
A database administrator must run scripts to create a set of tablespaces required for the content store database. Modify the scripts to replace the placeholder parameters with ones that are appropriate for your environment.

By default, the content store is used for notifications, human tasks, and annotations. You can create separate databases for each.
About this task

Ensure that you use the naming conventions for DB2 on z/OS. For example, all names of parameters must start with a letter and the length must not exceed eight characters. There are two exceptions to the character length limit:

- CMSCRIPT_CS_ID is no more than 2 characters.
- CMSCRIPT_TABLESPACE is no more than 6 characters.

The reason for the exception is that when the two parameters are concatenated the character length can be no more than 8.

For more information, see the IBM DB2 Information Center.

Procedure

1. Connect to the database as a user that has privileges to create and drop tablespaces and to allow execution of SQL statements.
2. Go to the directory that contains the scripts:
   
   `c10_location/configuration/schemas/content/db2zOS`

3. Make a backup copy of the `tablespace_db2zOS.sql` script file and save the file to another location.
4. Open the original `tablespace_db2zOS.sql` script file.
   a. Add a connection statement to the beginning of the script.
      
      For example,
      
      `connect to databasename;`
   b. Use the following table to help you to replace the generic parameters with ones appropriate for your environment.
      
      Not all of the parameters listed are in the script, but some might be added in the future.


<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMSCRIPT_STOGROUP</td>
<td>Specifies the name of the storage group.</td>
</tr>
<tr>
<td>CMSCRIPT_DATABASE</td>
<td>Specifies the name of the content store database.</td>
</tr>
<tr>
<td>CMSCRIPT_CS_ID</td>
<td>Specifies the subsystem identification for the content store database.</td>
</tr>
<tr>
<td>CMSCRIPT_TABLESPACE</td>
<td>Specifies the name of the tablespace that contains all of the base tables in the content store. Auxiliary tables are not included. The name cannot be longer than 6 characters.</td>
</tr>
<tr>
<td>CMSCRIPT_LARGE_BP</td>
<td>Specifies the name of the large buffer pool allocated for especially large objects. This bufferpool is the 32 KB buffer pool that was created when the database administrator created the content store database on the z/OS system.</td>
</tr>
</tbody>
</table>
Table 15. Parameter names and description for the content store tablespace script (continued)

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMSCRIPT_REGULAR_BP</td>
<td>Specifies the name of the regular size buffer pool allocated for regular and</td>
</tr>
<tr>
<td></td>
<td>large objects. This bufferpool is the 16 KB buffer pool that was created</td>
</tr>
<tr>
<td></td>
<td>when the database administrator created the content store database on the z/OS</td>
</tr>
<tr>
<td>CMSCRIPT_USERNAME</td>
<td>Specifies the user account that accesses the content store database.</td>
</tr>
</tbody>
</table>

5. Save and run the script.
   For example, if you set up your clp.properties file and your DB2 alias in your profile or tcshrc script file, type the following command to run the script:
   `db2 -tvf tablespace_db2zOS.sql`

6. Grant the IBM Cognos user rights to the tablespaces that were created when you ran the tablespace_db2zOS.sql file script:
   a. Make a copy of the rightsGrant_db2zOS.sql script file and store it in another location.
   b. In the remote access tool, open the original rightsGrant_db2zOS.sql script file and replace the placeholder parameters with values that are appropriate for your environment.
   Ensure that you use the same values that you used when you allocated resources to the buffer pools and user account.
   c. Add a connection statement to the beginning of the script.
   For example,
   `connect to databasename user username using password;`
   d. Save and then run the script.
   For example,
   `db2 -tvf rightsGrant_db2zOS.sql`

7. To create the notification tablespaces, go to the cl0_location/configuration/schemas/delivery/zosdb2 directory.
   a. Make a backup copy of the NC_TABLESPACES.sql script file and save the file to another location.
   b. Open the original NC_TABLESPACES.sql script file and use the following table to help you to replace the placeholder parameters with ones appropriate for your environment.

Table 16. Tablespace parameter names and descriptions for the DB2 notification database on z/OS

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCCOG</td>
<td>Specifies the name of the notification database.</td>
</tr>
<tr>
<td>DSN8G810</td>
<td>Specifies the name of the storage group.</td>
</tr>
<tr>
<td>BP32K</td>
<td>Specifies the name of the buffer pool.</td>
</tr>
</tbody>
</table>

Not all of the parameters listed are in the script, but might be added in the future.

   c. Save and run the script.
For example,
```
db2 -tvf NC_TABLESPACES.sql
```

**d.** Open the `NC_CREATE_DB2.sql` script file and replace the NCCOG placeholder parameter with the name of the notification database.

**e.** Save the script.

The Job and Scheduling Monitor services will automatically run the script. However, you may choose to run it yourself.

8. To create the human tasks tablespaces, go to the `cil0_location/configuration/schemas/hts/zosdb2` directory.

   **a.** Make a backup copy of the `HTS_tablespaces.sql` script file and save the file to another location.

   **b.** Open the original `HTS_TABLESPACES.sql` script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

   **Table 17. Tablespace parameter names and descriptions for human tasks on DB2 for z/OS**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCCOG</td>
<td>Specifies the name of the database.</td>
</tr>
<tr>
<td>DSN8G810</td>
<td>Specifies the name of the storage group.</td>
</tr>
<tr>
<td>BP32K</td>
<td>Specifies name of the 32 k buffer pool.</td>
</tr>
</tbody>
</table>

   See the script for a complete list of the parameters required.

   **c.** Save and run the script.

   **d.** Open the `HTS2_CREATE_Db2zos.sql` script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

   **Table 18. Tablespace parameter names and descriptions for human tasks on DB2 for z/OS**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCCOG</td>
<td>The name of the database.</td>
</tr>
</tbody>
</table>

   See the script for a complete list of the parameters required.

   **e.** Save and run the script.

9. To create the annotations tablespaces, go to the `cil0_location/configuration/schemas/ans/zosdb2` directory.

   **a.** Make a backup copy of the `ANN_TABLESPACES.sql` script file and save the file to another location.

   **b.** Open the original `ANN_TABLESPACES.sql` script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

   **Table 19. Tablespace parameter names and descriptions for annotations on DB2 for z/OS**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCCOG</td>
<td>The name of the database.</td>
</tr>
<tr>
<td>DSN8G810</td>
<td>The name of the storage group.</td>
</tr>
<tr>
<td>BP32K</td>
<td>The name of the 32 k buffer pool.</td>
</tr>
</tbody>
</table>

   See the script for a complete list of the parameters required.

   **c.** Save and run the script.
d. Open the `ANS2_CREATE_Db2zos.sql` script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCCOG</td>
<td>The name of the database.</td>
</tr>
</tbody>
</table>

See the script for a complete list of the parameters required.

e. Save and run the script.

Set up database connectivity for an Oracle content store

This procedure describes how to set up database connectivity for an Oracle content store. You must perform this procedure on each computer where you install Content Manager.

**Procedure**

1. On the computer where the Oracle client is installed, go to the `ORACLE_HOME/jdbc/lib` directory.
2. Copy the correct library file for your version of the Oracle client to the `c10_location/webapps/p2pd/WEB-INF/lib` directory on the computer where Content Manager is installed and where notification is sent to an Oracle database.
   - If you are using Oracle 10g, you must have `ojdbc14.jar`.
   - If you are using Oracle 11g, you must have `ojdbc5.jar`.

The files are available from an Oracle client or server install, and can also be downloaded from the Oracle technology Web site.

Set up database connectivity for an Informix content store

This procedure describes how to set up database connectivity for an Informix content store. You must perform this procedure on each computer where you install Content Manager.

**Procedure**

1. On the computer where Informix is installed, go to the `Informix_location/sqllib/java` directory.
2. Copy the following files to the `c10_location/webapps/p2pd/WEB-INF/lib` directory on every computer where Content Manager is installed.
   - the universal driver file, `db2jcc.jar`
   - the license file, `db2jcc_license_cisuz.jar`

Set up database connectivity for a Sybase content store

This procedure describes how to set up database connectivity for a Sybase content store. You must perform this procedure on each computer where you install Content Manager.

**Procedure**

1. On the computer where Sybase is installed, go to the `Sybase_location/jConnect-6/classes` directory.
2. Copy the jconn3.jar file to the c10_location/webapps/p2pd/WEB-INF/lib directory on every computer where Content Manager is installed and where notification is sent to a Sybase database.

Start IBM Cognos Configuration

Use IBM Cognos Configuration to configure IBM Cognos Business Intelligence components and to start and stop IBM Cognos services if you are using the default Tomcat servlet container.

Before you begin

Before starting IBM Cognos Configuration, ensure that the operating environment is properly set up. For example, ensure that all environment variables have been set.

On a Microsoft Windows operating system, you can start IBM Cognos Configuration in the last page of the installation wizard only if additional setup is not required. For example, if you use a database server other than Microsoft SQL or Cognos Content Database for the content store, copy the Java Database Connectivity (JDBC) drivers to the appropriate location before you start the configuration tool.

On UNIX or Linux operating systems, do not start IBM Cognos Configuration in the last page of the installation wizard. Additional setup is required before you can configure IBM Cognos BI. For example, you must update your Java environment.

Ensure that user or service account used to run IBM Cognos has been set up.

Procedure

1. On Microsoft Windows, click Start > IBM Cognos Configuration.
   If you are using a Windows Vista, Windows 7, or Windows 2008 computer, and have installed the product to the Program Files (x86) directory, start IBM Cognos Configuration as an Administrator.

2. On UNIX or Linux operating systems, go to the c10_location/bin64 directory and then type the following command:
   ./cogconfig.sh

   If IBM Cognos Configuration does not open, ensure that you set the DISPLAY environment variable.

   If you see a JAVA.Lang.unsatisfied link message, verify that you are using a supported version of Java.

   If you see a Java.lang.unsupportedClassVersionError message, ensure that you are using a 64-bit version of Java.

Configure Environment Properties in IBM Cognos Configuration

Specify the server name or an IP address in the URI properties that are used by IBM Cognos Business Intelligence. This will ensure that users in different locations can connect to reports and workspaces that are sent by e-mail. By default, the URI properties specify the localhost.

Procedure

1. Start IBM Cognos Configuration.

2. In the Explorer window, click Environment.
3. In the **Properties** window, change the **localhost** portion of all URI properties to the name or IP address of your IBM Cognos BI server by doing the following:
   - For **Content Manager URIs**, click the value and then click the edit icon. Change the value and then click **OK**.
   - For all other URI properties, click the value to change it.
4. In the **Explorer** window, under **Security > Cryptography**, click **Cognos**, the default cryptographic provider.
5. Under the **Certificate Authority settings** property group, set the **Password** property. Record the password in a secure location.
6. From the **File** menu, click **Save**.

### Enable Security

By default, IBM Cognos Business Intelligence allows anonymous access. If you want to use security in your IBM Cognos BI environment, you must disable anonymous access and configure IBM Cognos BI to use an authentication provider.

**Procedure**

1. In the IBM Cognos Configuration **Explorer** window, click **Security >Authentication > Cognos**.
2. Click the **Value** box for **Allow Anonymous Access**, and select **False**.
3. Right-click **Authentication**, and click **New Resource > Namespace**.
4. In the **Name** box, type a name for your authentication namespace.
5. In the **Type** list, click the appropriate namespace type and then click **OK**.
   
The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.
6. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
7. From the **File** menu, click **Save**.

### Set Database Connection Properties for the Content Store

You must specify the database server information to ensure that Content Manager can connect to the database you use for the content store. Content Manager uses the database logon to access the content store. After you set the database connection properties, you can test the connection between Content Manager and the content store.

If you installed Cognos Content Database, the database connection properties use the Cognos Content Database by default. You do not have to change the default connection properties. However, Cognos Content Database is for test or proof-of-concept systems only. When you move to a production environment, you must use an enterprise-level database for your content store.

If you are upgrading from an earlier version of IBM Cognos BI, configure IBM Cognos BI to point to a copy of the existing content store database. After you save the configuration and start the IBM Cognos service, the data in the content store is automatically upgraded and cannot be used by the earlier version. By using a copy of the original database with the new version, you can keep the earlier version running with the original data.
Setting database connection properties for a DB2 content store

You must specify the database server information to ensure that Content Manager can connect to the database you use for the content store.

Procedure
1. In the location where you installed Content Manager, start IBM Cognos Configuration.
2. In the Explorer window, under Data Access, Content Manager, click Content Store.
3. In the Properties window, for the Database name property, type the name of the database or the database alias.
4. Change the logon credentials to specify a valid user ID and password:
   • Click the Value box next to the User ID and password property and then click the edit button when it appears.
   If you are connecting to a database on DB2 on z/OS, ensure that you specify the same user ID as the value you specified for CMSCRIPT_USERNAME when you created the tablespaces.
   • Type the appropriate values and click OK.
5. In the Database server and port number field, enter the name of your computer and port number on which DB2 is running. For example, localhost:50000. 50000 is the default port number used by DB2. If you are using a different port number, ensure you use that value.
6. If you are connecting to a database on DB2 on z/OS:
   a. In the Explorer window, click Local Configuration.
   b. In the Properties window, next to Advanced properties, click inside the Value box, and then click the edit icon.
   c. Click Add to add the parameters that you used to create the tablespaces. Add all of the parameters except CMSCRIPT_USERNAME.
7. From the File menu, click Save.

Setting database connection properties for a Microsoft SQL Server, Oracle, Informix, or Sybase content store

You must specify the database server information to ensure that Content Manager can connect to the database you use for the content store.

Procedure
1. Start IBM Cognos Configuration.
2. In the Explorer window, under Data Access, Content Manager, right-click Content Store and click Delete.
   This step deletes the connection to the default resource. Content Manager can access only one content store.
3. Right-click Content Manager, and then click New resource, Database.
4. In the Name box, type a name for the resource.
5. In the Type box, select the type of database and click OK.

   Tip: If you want to use an Oracle Net8 keyword-value pair to manage the database connection, select Oracle database (Advanced).
6. In the Properties window, provide the values for your database type:
• If you use a Microsoft SQL Server database, type the appropriate values for the **Database server with port number or instance name** and **Database name** properties.

For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property.

For the **Database server with port number or instance name** property, include the instance name if there are multiple instances of Microsoft SQL Server.

To connect to a named instance, you must specify the instance name as a Java Database Connectivity (JDBC) URL property or a data source property. For example, you can type localhost\instance1. If no instance name property is specified, a connection to the default instance is created.

The properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

```
jdbc:JSQLConnect://localhost\instance1/user=sa/
more properties as required
```

To connect to a named instance, you must specify the instance name. For example, you can type localhost\instance1. If an instance name is not specified, a connection to the default instance is created.

• If you use an Oracle database, type the appropriate values for the **Database server and port number** and **SID** properties.

• If you use an advanced Oracle database, for the **Database specifier** property, type the Oracle Net8 keyword-value pair for the connection.

Here is an example:

```
(description=(address=(host=myhost)(protocol=tcp)(port=1521)
     (connect_data=(sid=(orcl))))))
```

When you select the advanced Oracle database, IBM Cognos BI uses enterprise-oriented Oracle features to select a listener, switch to another listener if the first listener fails, automatically reconnect to the database if the connection fails, balance connection requests among listeners, and balance connection requests among dispatchers.

• If you use an Informix database, type the appropriate values for the **Database server and port number** and **Database name** properties.

• If you use a Sybase database, type the appropriate values for the **Database server and port number** and **Database name** properties.

7. To configure logon credentials, specify a user ID and password:

• Click the Value box next to the **User ID and password** property and then click the edit icon when it appears.

• Type the appropriate values and click **OK**.

8. If you host more than one content store database on an Informix instance, create the advanced property CMSCRIPT_CS_ID and specify the account under which the instance runs:

• In the Explorer window, click **Local Configuration**.

• In the Properties window, click the Value column for **Advanced properties** and then click the edit icon.

• In the **Value - Advanced properties** dialog box, click **Add**.

• In the Name column, type CMSCRIPT_CS_ID

• In the Value column, type the user ID of the account under which the instance of the content store runs.
Use a different user account for each instance of Informix content store database.

9. From the File menu, click Save.
   The logon credentials are immediately encrypted.

Results

Content Manager can now create the required tables in the content store when you start the IBM Cognos service for the first time. If the connection properties are not specified correctly, you cannot start the IBM Cognos services.

Specify a Connection to a Mail Server Account

If you want to send reports by email, you must configure a connection to a mail server account.

You must also change the host name portion of the Gateway URI from localhost to either the IP address of the computer or the computer name. Otherwise the URL in the email will contain localhost and remote users will not be able to open the report.

Procedure

1. In the location where Content Manager is installed, start IBM Cognos Configuration.
2. In the Explorer window, under Data Access, click Notification.
3. In the Properties window, for the SMTP mail server property, type the host name and port of your SMTP (outgoing) mail server.
   
   Tip: To be able to open reports that are sent as links, ensure that the Gateway URI on report servers and notification servers specifies an accessible Web server hosting IBM Cognos content. If you have mobile users accessing links remotely, consider using an external URI.
4. Click the Value box next to the Account and password property and then click the edit button when it appears.
5. Type the appropriate values in the Value - Account and password dialog box and then click OK.
   
   Tip: If logon credentials are not required for the SMTP server, remove the default information for the Account and password property. When you are prompted for confirmation to leave this property blank, click OK. Ensure that the default user name has been removed. Otherwise, the default account is used and notifications will not work properly.
6. In the Properties window, type the appropriate value for the default sender account.
7. Test the mail server connections. In the Explorer window right-click Notification and click Test.
   IBM Cognos Business Intelligence tests the mail server connection.

Results

If you do not plan to send reports by email, or do not want to set up a mail server account immediately, you are not required. However, when you save the configuration and then you start the services in IBM Cognos Configuration, you
will see a warning message when the mail server connection is tested. You can safely ignore the warning.

**Configure an IBM Cognos Series 7 Namespace in IBM Cognos BI**

If you want to migrate security information or secured content from IBM Cognos Series 7 to IBM Cognos Business Intelligence, you must configure a namespace in IBM Cognos BI that is identical to the IBM Cognos Series 7 namespace.

You can configure multiple namespaces for authentication in IBM Cognos BI. For more information, see Chapter 8, “Configuring IBM Cognos Components to Use an Authentication Provider,” on page 141.

**Note:** You cannot use an IBM Cognos Series 7 Local Authentication Export (LAE) file for authentication with IBM Cognos BI components.

We recommend that all IBM Cognos Series 7 namespaces use the same primary IBM Cognos Series 7 Ticket Server. Otherwise, you may receive errors or be prompted for authentication more than once.

If you change the configuration information stored in the directory server used for IBM Cognos Series 7, you must restart the IBM Cognos BI service before the changes take effect in the IBM Cognos installation.

A user must be in at least one Access Manager user class to be able to log on to IBM Cognos BI components.

**Procedure**

1. Start IBM Cognos Configuration.
2. In the Explorer window, under Security, Authentication, click Cognos.
3. Click the Value box for Allow Anonymous Access, and select False.
5. In the Name box, type a name for the authentication namespace.
6. In the Type list, click IBM Cognos Series 7 and then click OK.
   The new authentication provider resource appears in the Explorer window, under the Authentication component.
7. In the Resource Properties window, specify the mandatory values.
   Certain values must match the values you used when you configured the IBM Cognos Series 7 namespace in Configuration Manager. In Configuration Manager, the properties are located in Services, Access Manager - Runtime, Directory Server.
   • For Namespace ID, specify a unique identifier for the namespace.
   • For Host and port, type the same value that you used for the Computer property in Configuration Manager.
   The format must be identical. If you use an IP address in IBM Cognos Series 7, type the same IP address. If you use a network host name in IBM Cognos Series 7, type the same network host name.
   • For Base Distinguished Name, type the same value that you used for the Base Distinguished Name (DN) property in Configuration Manager.
   • For Namespace name, type the same value that you used for the Default Namespace property in Configuration Manager.
This value is case sensitive and must match exactly.

8. Specify the values for all other required properties to ensure that IBM Cognos BI components can locate and use your existing authentication provider.

   If your IBM Cognos Series 7 namespace version is 16.0, ensure that the `Data encoding` property is set to `UTF-8`. In addition, the computers where Content Manager is installed must use the same locale as the data in the IBM Cognos Series 7 namespace.

9. If your namespace environment includes version 15.2 of the IBM Cognos Series 7 namespace, you must disable the `Series7NamespacesAreUnicode` setting.

   - In the `Properties` window, in the `Advanced Properties` value, click the `edit` icon.
   - In the `Value - Advanced properties` window, click `Add`.
   - In the `Name` box, type `Series7NamespacesAreUnicode`.
   - In the `Value` box, type `False`, and then click `OK`.

10. In the `Properties` window, under `Cookie settings`, ensure that the `Path`, `Domain`, and `Secure flag enabled` properties match the settings configured for IBM Cognos Series 7.

11. From the `File` menu, click `Save`.

---

### Start the IBM Cognos services

To register the IBM Cognos Business Intelligence service so that users can access it through IBM Cognos Connection, you must start the services. Before you start the services, test the configuration by using the test feature in IBM Cognos Configuration.

#### Before you begin

Before you begin, ensure that a user or service account is set up. For information, see "Configure a User Account or Network Service Account for IBM Cognos Business Intelligence" on page 33.

#### Procedure

1. Start IBM Cognos Configuration.
   
   If you are upgrading, a message appears indicating that configuration files were detected and upgraded to the new version.

2. Ensure that you save your configuration, otherwise you cannot start the IBM Cognos service.

3. From the `Actions` menu, click `Test`.

   IBM Cognos Configuration checks the common symmetric keys (CSK) availability, tests the namespace configuration, and tests the connections to the content store and other resources.

   **Tip:** If `Test` is not available for selection, in the `Explorer` window, click `Local Configuration`.

4. If the test fails, reconfigure the affected properties and then test again.

   You can test some components individually by right-clicking the component in the `Explorer` panel and selecting `Test`.

   Do not start the service until all tests pass.
5. From the **Actions** menu, click **Start**.
   It may take a few minutes for the IBM Cognos service to start.
   This action starts all installed services that are not running and registers the
   IBM Cognos service on Windows.

---

**Configuring the web server**

You must configure your Web server before users can connect to the IBM Cognos
BI portal.

For IBM Cognos BI for reporting, you must also set the content expiry for the
images directory in your Web server so that the Web browser does not check
image status after the first access.

On UNIX and Linux operating systems, the account under which the Web server
runs must have read access to the `cogstartup.xml` file in the `c10_location/
configuration` directory. By default the `cogstartup.xml` file has read permission for
others. If you run your Web server under a specific group, you can change the
`cogstartup.xml` file permissions to ensure that it belongs to the same group as the
Web server. You can then remove the read permission for others.

---

**Use compiled gateways for production systems**

For production systems, you can improve performance by changing the gateway
from the default CGI gateway.

The compiled gateways include:

- Microsoft Internet Server Application Programming Interface (ISAPI) for
  Microsoft Internet Information Services (IIS)
- Apache module for Apache Web Server or IBM HTTP Server
- Servlet Gateway Java application if you use an application server other than the
default Apache Tomcat

**Use Apache modules on Apache Server or IBM HTTP Server**

You can use Apache modules for Apache Server 2.2.x or Apache Server 2.0.x or for
IBM HTTP Server 8, 7, or 6.1.

**Important:** You cannot use the Apache modules with the version of Apache Server
2.2 that is supplied with Red Hat Enterprise Linux version 5.3 and later.

**Procedure**

1. Append the `c10_location/cgi-bin` directory to the appropriate environment
   variable:
   - On Solaris or Linux, `LD_LIBRARY_PATH`
   - On HP-UX, `SHLIB_PATH` and `LD_LIBRARY_PATH`
   - On AIX, `LIBPATH`

2. Go to the `Webserver_installation/conf` directory.

3. Open the `httpd.conf` file in an editor.

4. Ensure that both the server name and web server port number values are
   specified for the `ServerName` property.

5. Add the following to the end of the load module list:

   ```
   LoadModule cognos_module "c10_location/cgi-bin/mod2_2_cognos.suffix"
   ```
   Where `suffix` is as listed in the following table.
Table 21. Module suffix for your operating system

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Suffix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>dll</td>
</tr>
<tr>
<td>Solaris, AIX, IA®, Linux</td>
<td>so</td>
</tr>
</tbody>
</table>

Apache modules are provided for different versions of Apache Server or IBM HTTP Server:

- Use the mod2_2_cognos module for Apache Server 2.2.x or IBM HTTP Server 8 and 7.
- Use the mod2_cognos module for Apache Server 2.0.x and IBM HTTP Server 6.1.

6. Add the following:

```xml
ScriptAlias /ibmcognos/cgi-bin "c10_location/cgi-bin"
<Directory "c10_location/cgi-bin">
  AllowOverride None
  Options None
  Order allow,deny
  Allow from all
</Directory>

Alias /ibmcognos "c10_location/webcontent"
<Directory "c10_location/webcontent">
  Options Indexes MultiViews
  AllowOverride None
  Order allow,deny
  Allow from all
</Directory>
```

The `<Directory>` directive is optional.

**Note:** Ensure that you define the `/ibmcognos/cgi-bin` alias before the `/ibmcognos` alias.

**Important:** `ibmcognos` is the default value that is used in the Gateway URI and Controller URI for gateway values in IBM Cognos Configuration. If you do not use `ibmcognos` for the ScriptAlias and Alias values, ensure that you change the Gateway URI and Controller URI for gateway values to match the values you use. Also, ensure that you use the same value for the `ibmcognos` part of the ScriptAlias and Alias values as shown in the examples.

7. Add the following to the server status reports section:

```xml
<Location /ibmcognos/cgi-bin/module_alias>
  SetHandler cognos-handler
  Order allow,deny
  Allow from all
</Location>
```

Where `module_alias` is a name that you can choose.

8. To enable the gateway diagnostic page, add the following to the server status reports section:

```xml
<Location /ibmcognos/cgi-bin/diag_module_alias>
  SetHandler cognos-handler
  Order allow,deny
  Allow from all
</Location>
```

Where `diag_module_alias` is a name that you can choose.

9. Add the following to the user directory section:
Apache module files are provided for different versions of Apache Server or IBM HTTP Server:

- Use `mod2_2_cognos.c` for Apache Server 2.2.x or IBM HTTP Server 8 and 7.
- Use `mod2_cognos.c` for Apache Server 2.0.x and IBM HTTP Server 6.1.

10. Save and close the file.

11. On HP-UX, enable searching for `SHLIB_PATH` by running the following command in the `Apache_installation/bin` directory:

   ```
   chatr +s enable +b enable httpd
   ```

12. Restart the web server.


14. In the **Explorer** panel, click **Local Configuration > Environment**.

15. In the **Gateway URI** box, change the `cognos.cgi` part of the URI to `module_alias`.

   For example, `http://host_name:port/ibmcognos/cgi-bin/module_alias`.

16. Save your changes.

**Results**

Users can access the server by entering the Apache module URI in their browser.

For example,

`http://servername:port/ibmcognos/cgi-bin/module_alias`.

**Use the ISAPI gateway on Microsoft Internet Information Services (IIS) version 7 or 8**

If you are using a Microsoft Internet Information Services (IIS) web server, configure IBM Cognos to use the ISAPI gateway rather that the default CGI gateway.

**About this task**

If you are using Microsoft IIS as your web server and you plan to run more than one IBM Cognos BI product, or several instances of the same product, on one computer, you must create a separate application pool for each product or instance and then associate the aliases for that product or instance to the application pool.

For more information about creating an application pool, see your web server documentation.

**Important:** If you are using the 32-bit version of the ISAPI gateway, you must enable 32-bit application for the application pool that is used for the IBM Cognos gateway. In the Internet Information Services (IIS) Manager, select the application pool that is used for IBM Cognos, and click **Advanced Settings**. Change the value for **Enable 32-Bit Applications** to **True**.

**Procedure**

1. In the Microsoft Windows **Control Panel**, click **Programs > Programs and Features**.

   If you are using Microsoft Windows 8 or 2012 Server, **Programs and Features** is available directly from the **Control Panel**.
2. Click Turn Windows features on or off.
3. If you are using Microsoft Windows 2008 Server, use the following steps:
   a. Click Server Manager > Roles > Web Server (IIS).
   b. Ensure that Common HTTP Features, or the features you require are enabled.
   c. If ISAPI extensions is set to Not installed, select ISAPI extensions and click Add Role Service.
4. If you are using Microsoft Windows 2012 Server, use the following steps:
   a. In the Add Roles and Features Wizard, click Role-based or feature-based installation, and click Next.
   b. Select your server, and click Next.
   c. Select Web Server (IIS), if it is not already installed, ensure that Common HTTP Features is selected, and click Next until you get to the Role Services section of the wizard.
   d. Expand Application Development.
   e. Select ISAPI extensions if it is not already selected, and click Next.
   f. Click Install.
5. If you are using Microsoft Windows 7 or 8, use the following steps:
   a. Select Internet Information Services if it is not already selected.
   b. Expand Internet Information Services > World Wide Web Services.
   c. Ensure that Common HTTP Features, or the features you require are enabled.
   d. Expand Application Development Features.
   e. If ISAPI extensions is not selected, select ISAPI extensions.
   f. Click OK.
6. In the Internet Information Services (IIS) Manager console, under Connections, select your server name.
   • If you are using Microsoft Windows 2012 Server, in Server Manager, select IIS, and then right-click your server name, and click Internet Information Services (IIS) Manager.
   • If you are using Microsoft Windows 2008 Server, in Server Manager, expand Roles > Web Server (IIS), and then click Internet Information Services (IIS) Manager.
   • If you are using Microsoft Windows 8, from the Control Panel, click Administrative Tools to access the Internet Information Services (IIS) Manager console.
   • If you are using Microsoft Windows 7, from the Control Panel, click System and Security > Administrative Tools to access the Internet Information Services (IIS) Manager console.
7. Expand Sites, and under your website, add the virtual directories as shown in the table:

<table>
<thead>
<tr>
<th>Alias</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibmcognos</td>
<td>c10_location/webcontent</td>
</tr>
<tr>
<td>ibmcognos/cgi-bin</td>
<td>c10_location/cgi-bin</td>
</tr>
</tbody>
</table>
Important: \texttt{ibmcognos} is the default value that is used in the \texttt{Gateway URI} and \texttt{Controller URI for gateway} values in IBM Cognos Configuration. If you do not use \texttt{ibmcognos} for the Alias values, ensure that you change the \texttt{Gateway URI} and \texttt{Controller URI for gateway} values to match the values you use.

8. Select the cgi-bin virtual directory that you created.
9. Double-click \texttt{Handler Mappings}.
10. Under \texttt{Actions}, click \texttt{Add Module Mapping}.
   a. In \texttt{Request Path}, type \texttt{cognosisapi.dll}.
   b. In \texttt{Module}, select \texttt{IsapiModule}.
   c. In \texttt{Executable}, enter the path to the \texttt{cognosisapi.dll} file.
      For example, enter: \texttt{C:\Program Files\ibm\cognos\c10\cgi-bin\cognosisapi.dll}
   d. In \texttt{Name}, enter a name for the entry, such as \texttt{CognosISAPI}.
   e. Click \texttt{OK}.
   f. Click \texttt{Yes} in the dialog box to allow the ISAPI extension.
11. Start IBM Cognos Configuration.
12. In the \texttt{Explorer} panel, click \texttt{Local Configuration > Environment}.
13. In the \texttt{Gateway URI} box, change the \texttt{cognos.cgi} part of the URI to \texttt{cognosisapi.dll}.

\textbf{Results}

Users can access the ISAPI gateway by entering \texttt{http://servername/ibmcognos/isapi} in their web browsers.

\textbf{Configure the servlet gateway for an application server}

If you deploy IBM Cognos to an application server other than Tomcat, you can use the servlet gateway to serve the portal pages rather than using a web server.

\textbf{Before you begin}

Ensure the following tasks are complete:

\begin{itemize}
  \item The application server is installed and running on each computer where the servlet gateway is to be installed.
  \item IBM Cognos BI gateway components are installed on the same system as the application server.
  \item The IBM Cognos BI Application Tier Components and Content Manager are installed and running in the environment.
  \item The application server user account has full access permission for the IBM Cognos installation.
\end{itemize}

\textbf{About this task}

Instead of routing requests directly to the dispatcher, you deploy the servlet gateway to a different JVM instance than the JVM instances that run the IBM Cognos BI Application Tier Components and Content Manager servlets. Doing this type of deployment separates the load for serving static content from the main applications.
Procedure
1. Create a separate JVM instance, if necessary.
   If you plan to run IBM Cognos BI and the IBM Cognos Servlet Gateway on the same application server, the servlet gateway must be deployed to a separate JVM instance.
2. Check that IBM Cognos components are properly set up
3. Set environment variables
4. Configure IBM Cognos Servlet Gateway to run on the application server
5. Change the application server startup script, if necessary.
6. Configure application server properties and deploy IBM Cognos Servlet Gateway
7. Enable SSL, if required.

Results
You can now access IBM Cognos components using the servlet gateway by entering the gateway URI. For example, http[s]:host_name:port/ServletGateway.

The IBM Cognos Servlet Gateway URI is case-sensitive.

Use CGI gateways
You can use the CGI gateway on IBM HTTP Server, Apache Web Server, or Microsoft Internet Information Services (IIS) Server.

Use the CGI gateway on Apache Server or IBM HTTP Server
The default gateway configured in IBM Cognos Configuration is the CGI gateway. To use the CGI gateway, you must configure aliases for Apache Server or IBM HTTP Server.

Procedure
1. Go to the Webserver_installation/conf directory.
2. Open the httpd.conf file in an editor.
3. Ensure that both the server name and web server port number values are specified for the ServerName property.
4. Add the following:
   ScriptAlias /ibmcognos/cgi-bin "c10_location/cgi-bin"
   <Directory "c10_location/cgi-bin">
      AllowOverride None
      Options None
      Order allow,deny
      Allow from all
   </Directory>
   Alias /ibmcognos "c10_location/webcontent"
   <Directory "c10_location/webcontent">
      Options Indexes MultiViews
      AllowOverride None
      Order allow,deny
      Allow from all
   </Directory>
   The <Directory> directive is optional.
Note: Ensure that you define the /ibmcognos/cgi-bin alias before the /ibmcognos alias.

Important: ibmcognos is the default value that is used in the Gateway URI and Controller URI for gateway values in IBM Cognos Configuration. If you do not use ibmcognos for the ScriptAlias and Alias values, ensure that you change the Gateway URI and Controller URI for gateway values to match the values you use. Also, ensure that you use the same value for the ibmcognos part of the ScriptAlias and Alias values as shown in the examples.

5. Save and close the file.
6. Restart the web server.

Results

Users can access the portal at http://servername:port/ibmcognos.

Use the CGI gateway on Microsoft Internet Information Services (IIS) version 7 or 8

If you are using Microsoft Internet Information Services (IIS) version 7 or later, use the following task to configure the CGI gateway.

The CGI gateway is provided for both 32-bit and 64-bit web servers.

About this task

If you are using Microsoft IIS as your web server and you plan to run more than one IBM Cognos BI product, or several instances of the same product, on one computer, you must create a separate application pool for each product or instance and then associate the aliases for that product or instance to the application pool.

For more information about creating an application pool, see your web server documentation.

Procedure

1. In the Microsoft Windows Control Panel, click Programs > Programs and Features.
   If you are using Microsoft Windows 8 or 2012 Server, Programs and Features is available directly from the Control Panel.
2. Click Turn Windows features on or off.
3. If you are using Microsoft Windows 2008 Server, use the following steps:
   a. Click Server Manager > Roles > Web Server (IIS).
   b. Ensure that Common HTTP Features, or the features you require are enabled.
   c. If CGI is set to Not installed, select CGI and click Add Role Service.
4. If you are using Microsoft Windows 2012 Server, use the following steps:
   a. In the Add Roles and Features Wizard, click Role-based or feature-based installation, and click Next.
   b. Select your server, and click Next.
   c. Select Web Server (IIS), if it is not already installed, ensure that Common HTTP Features is selected, and click Next until you get to the Role Services section of the wizard.
   d. Expand Application Development.
e. Select CGI if it is not already selected, and click Next.
f. Click Install.

5. If you are using Microsoft Windows 7 or 8, use the following steps:
   a. Select Internet Information Services if it is not already selected.
   b. Expand Internet Information Services > World Wide Web Services.
   c. Ensure that Common HTTP Features, or the features you require are enabled.
   d. Expand Application Development Features.
   e. If CGI is not selected, select CGI.
   f. Click OK.

6. In the Internet Information Services (IIS) Manager console, under Connections, select your server name.
   - If you are using Microsoft Windows 2012 Server, in Server Manager, select IIS, and then right-click your server name, and click Internet Information Services (IIS) Manager.
   - If you are using Microsoft Windows 2008 Server, in Server Manager, expand Roles > Web Server (IIS), and then click Internet Information Services (IIS) Manager.
   - If you are using Microsoft Windows 8, from the Control Panel, click Administrative Tools to access the Internet Information Services (IIS) Manager console.
   - If you are using Microsoft Windows 7, from the Control Panel, click System and Security > Administrative Tools to access the Internet Information Services (IIS) Manager console.

7. Double-click ISAPI and CGI Restrictions.

8. Under Actions, click Add.

9. Enter the path to the cognos.cgi file. The file is in the c10_location\cgi-bin directory.
   You must enter the full path, including the file name. If the path includes spaces, ensure you use quotation marks around the path. For example, enter: “C:\Program Files\ibm\cognos\c10\cgi-bin\cognos.cgi”

10. Enter a Description, such as CognosCGI.

11. Select Allow extension path to execute, and click OK.

12. Under Connections, expand Sites, and under your website, add the virtual directories as shown in the table:

<table>
<thead>
<tr>
<th>Alias</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibmcognos</td>
<td>c10_location/webcontent</td>
</tr>
<tr>
<td>ibmcognos/cgi-bin</td>
<td>c10_location/cgi-bin</td>
</tr>
</tbody>
</table>

13. Select the cgi-bin virtual directory that you created.


   a. In Request Path, type cognos.cgi.
   b. In Module, select CgiModule.
   c. Leave Executable (optional) blank.
   d. In Name, enter a name for the entry, such as CognosCGI.
Results

Users can access the CGI gateway by entering http://servername/ibmcognos in their web browsers.

**Use the CGI gateway on older versions of Microsoft IIS**

For versions of Microsoft Internet Information Services (IIS) earlier than version 7, use these steps to configure the CGI gateway.

**Procedure**

Create the virtual directories shown in the following table:

<table>
<thead>
<tr>
<th>Alias</th>
<th>Location</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibmcognos</td>
<td>c10_location/webcontent</td>
<td>Read</td>
</tr>
<tr>
<td>ibmcognos/cgi-bin</td>
<td>c10_location/cgi-bin</td>
<td>Execute</td>
</tr>
</tbody>
</table>

**Important:** ibmcognos is the default value that is used in the Gateway URI and Controller URI for gateway values in IBM Cognos Configuration. If you do not use ibmcognos for the ScriptAlias and Alias values, ensure that you change the Gateway URI and Controller URI for gateway values to match the values you use.

**Configuring WebDAV to view and browse images**

To view and browse images in the Report Studio, configure Web Distributed Authoring and Versioning (WebDAV) on your web server. Report authors can browse for images to include in reports in a way that is similar to browsing a file system.

**Configuring WebDAV on Microsoft IIS web servers**

On Microsoft Internet Information Services (IIS) web servers, you must first enable the WebDAV feature, and then configure your web server to access the image location.

**Procedure**

1. In the Microsoft Windows Control Panel, click Programs > Programs and Features.
   
   If you are using Microsoft Windows 8 or 2012 Server, Programs and Features is available directly from the Control Panel.
2. Click Turn Windows features on or off.
3. If you are using Microsoft Windows 2008 Server, use the following steps:
   a. Click Server Manager > Roles > Web Server (IIS).
   b. In the Role Services section, select Add Role Services.
   c. Under Web Server > Common HTTP Features, select WebDAV Publishing.
   d. Click Next, and then click Install.
4. If you are using Microsoft Windows 2012 Server, use the following steps:
   a. In the Add Roles and Features Wizard, click Role-based or feature-based installation, and click Next.
b. Select your server, and click Next.
d. Click Next > Next, and then click Install.

5. If you are using Microsoft Windows 7 or 8, use the following steps:
a. Expand Internet Information Services > World Wide Web Services > Common HTTP Features.
b. Select WebDAV Publishing, and click OK.

6. In the Internet Information Services (IIS) Manager console, under Connections, select your server name.
   - If you are using Microsoft Windows 2012 Server, in Server Manager, select IIS, and then right-click your server name, and click Internet Information Services (IIS) Manager.
   - If you are using Microsoft Windows 2008 Server, in Server Manager, expand Roles > Web Server (IIS), and then click Internet Information Services (IIS) Manager.
   - If you are using Microsoft Windows 8, from the Control Panel, click Administrative Tools to access the Internet Information Services (IIS) Manager console.
   - If you are using Microsoft Windows 7, from the Control Panel, click System and Security > Administrative Tools to access the Internet Information Services (IIS) Manager console.

7. Under Connections, expand your web server, Sites, and select your website. For example, select Default Web Site.


9. Click Enable WebDAV.

10. Click WebDAV Settings.

11. If you have anonymous access enabled, select True for Allow Anonymous Property Queries, and click Apply.

12. Select the directory or virtual directory to which you want to allow WebDAV access.


14. Click Add Authoring Rule, and add the appropriate rules for your environment. For example, if you installed the samples and you want to use the default path, under the ibmcognos virtual directory, expand samples, and select images, and add an authoring rule for the image files.

15. Right-click the directory or virtual directory you added authoring rules to, and click Edit Permissions.

16. Click Security, and add the appropriate permissions. For example, if you allow anonymous access to your web server, add permissions for the anonymous access user. You can find that user by select the website, double-clicking Authentication, and viewing the properties for the displayed users.

Results

With WebDAV enabled, Report Studio users can add images to their reports. When users click Browse in the image browser, the default location for browsing is http://servername/ibmcognos/samples/images. If you created another location, users can enter that location.
Test the Installation and Configuration

You can test your configuration settings by running the test feature as you configure IBM Cognos Business Intelligence. After you have completed the configuration and started the services, you can test the installation by connecting to the IBM Cognos BI portal.

Procedure
1. Open a Web browser.
2. Test that Content Manager is running by typing the Content Manager URIs value from IBM Cognos Configuration. For example, http://host_name:port/p2pd/servlet The default value for host_name:port is localhost:9300.
3. Test the availability of the dispatcher by typing the Internal dispatcher URI value from IBM Cognos Configuration. For example, http://host_name:port/p2pd/servlet/dispatch The default value for host_name:port is localhost:9300. If the response shows a list of content in Public Folders, the dispatcher is available.
4. Test the gateway by typing the Gateway URI value from IBM Cognos Configuration in your Web browser. It may take a few minutes for the Web page to open. If you see the Welcome page in the IBM Cognos BI portal, your installation is working.

Installing and Configuring Migration on IBM Cognos Series 7

Before you can use the Migration Assistant in IBM Cognos PowerPlay to migrate IBM Cognos Series 7 content from PowerPlay Enterprise Server, Upfront, or IBM Cognos Connection, you must install migration components on IBM Cognos Series 7 computers. The IBM Cognos Series 7 migration components are available on Microsoft Windows and UNIX, on the IBM Cognos PowerPlay Server CD.

Use the following checklist to guide you through the tasks to install and configure IBM Cognos Migration

• Install IBM Cognos Series 7 migration components.
• Configure the IBM Cognos Series 7 migration components, if required.
• Start the IBM Cognos Series 7 migration service.

For information about migrating content from IBM Cognos Series 7 to IBM Cognos BI, including configuration recommendations for the migration process, see the IBM Cognos PowerPlay Migration and Administration Guide.

Install IBM Cognos Series 7 Migration Components

Ensure that your IBM Cognos Series 7 installations are working correctly before installing the IBM Cognos Series 7 migration components. This includes ensuring that the IBM Cognos Series 7 PowerPlay Enterprise Server service and the Upfront services, including the IBM Cognos Upfront Administration Service, IBM Cognos Upfront Data Store and the IBM Cognos Upfront Dispatcher services, are running.

You install IBM Cognos Series 7 migration components on the IBM Cognos Series 7 computers.
• To migrate content from a PowerPlay Enterprise Server you must install IBM Cognos Series 7 migration components on the PowerPlay Enterprise Server computer. If Upfront is located on the same computer you can also migrate content from Upfront. Installing migration components on the PowerPlay Enterprise Server computer also supports the migration of PowerPlay content that was published to Cognos Connection.

• To migrate content from Upfront you must install IBM Cognos Series 7 migration components on the Upfront computer. When Upfront and PowerPlay Enterprise Server are installed on separate computers, you must install IBM Cognos Series 7 migration components on the both the PowerPlay Enterprise Server computer and the Upfront computer. Also, you must set up and configure a shared network location to support migration processing.

Procedure

1. Insert the IBM Cognos PowerPlay Server CD that is appropriate for your operating system. On UNIX, you must mount the CD using Rock Ridge file extensions.

2. If the Welcome page does not appear, do one of the following:
   • On Windows, in the win32 directory on the CD, double-click the issetup.exe file.
   • On UNIX, in the directory that is appropriate for your operating system, type ./issetup

3. Select the language to use for the installation.
   The language that you select determines the language of the installation wizard.

4. Follow the directions in the installation wizard.

5. On the Component Selection page, clear all components except IBM Cognos Series 7 Migration Components.

6. In the Multiple Installation Locations page, specify the IBM Cognos Series 7 location to install the components.
   You must install IBM Cognos Series 7 migration components in the same directory as IBM Cognos Series 7 version 4 (7.4).
   If you are installing the IBM Cognos Series 7 migration components on a Microsoft Windows computer, the installation location must be a physical drive and not a mapped drive. Otherwise, you will not be able to start the migration service.
   If you are prompted for an IBM Cognos BI installation location, you can accept the default location or enter a new local location. This location is used to write install files. You do not have to enter the path to an IBM Cognos BI installation on a different computer and you do not require IBM Cognos BI components on the IBM Cognos Series 7 computer.

7. In the Migration Configuration Information page, for the Migration Service Port Number, type a port number that the IBM Cognos Series 7 migration service will use. The default is 21567.

8. In the Finish page, click Finish.

Results

Like other IBM Cognos products, the installation process creates log files that include information such as details about transferred files and installation errors. The log files are located in the installation_location\instlog directory.
Configuring the migration service in a distributed IBM Cognos Series 7 environment

If you installed IBM Cognos Series 7 migration components on both a PowerPlay Enterprise Server computer and a separate Upfront computer, you must set up and configure a shared network location. The migration service writes temporary files to this location during migration processing.

The following limitations apply for migration from Upfront when PowerPlay Enterprise Server and Upfront are on separate computers.

PowerPlay Enterprise Server and Upfront must access PowerCubes using the same path, such as \machine_name\cubes. If the cubes are located on the same computer as PowerPlay Enterprise Server, PowerPlay Enterprise Server will access the cubes using a local path and Upfront will access the cubes using a path that includes the PowerPlay Enterprise computer name. Migration from Upfront will not work in this situation.

Procedure

1. Create a folder in a shared network location that is accessible from both the PowerPlay Enterprise Server computer and the Upfront computer.
   Ensure that the services for PowerPlay Enterprise Server, Upfront, and IBM Cognos Series 7 migration run under named accounts that have write access to the folder.

2. Complete the following steps on each computer that includes IBM Cognos Series 7 migration components.
   - From the installation_location/mig7service, open the migs7service_configuration.xml file in an XML or text editor.
   - Edit the series7-shared-location description line to specify the network location and activate the line (remove comment tags). For example,
     `<series7-shared-location description="Path to shared folder">\bott93\shareT\s7migration</series7-shared-location>`
   - Save and close the file.

3. Restart the IBM Series 7 migration service.

Results

The configuration to support migration from separate PowerPlay Enterprise Server and Upfront computers is complete.

Start the IBM Cognos Series 7 Migration Service

Before you can migrate content from IBM Cognos Series 7 PowerPlay to IBM Cognos PowerPlay, you must start the migration service for IBM Cognos Series 7. On Windows, the migration service for IBM Cognos Series 7 starts automatically when it is first installed.

Procedure

Start the migration service:

- On Windows, if the service is stopped, then restart the migration service using the IBM Cognos Migration Series 7 Service entry in the Services list under Administrative Tools.
On UNIX, go to the `c10_location/migs7` directory and start the service by typing

```
./configure.sh --start
```
Chapter 6. Installing and Configuring Server Components on Different Computers

Use the installation wizard to select the server components that you want to install and the location on your computer where you want to install them. Only the components that you choose to install are copied from the disk to your computer.

If you plan to install two or more components on the same computer, install them in the same installation location to avoid conflicts among ports and other default settings.

If you are installing IBM Cognos PowerPlay with IBM Cognos Business Intelligence Server, install and configure IBM Cognos Business Intelligence server first. Both IBM Cognos PowerPlay and IBM Cognos Business Intelligence server must be the same version.

The IBM Cognos PowerPlay installation includes components that support the migration of PowerPlay content from IBM Cognos Series 7 to IBM Cognos Business Intelligence.

The server components include the following:
- Content Manager
- Application Tier Components
- Gateway
- IBM Cognos Series 7 Migration components

To migrate content from IBM Cognos Series 7 PowerPlay to IBM Cognos PowerPlay, you must install the IBM Cognos Series 7 migration components on the computer where IBM Cognos Series 7 PowerPlay Enterprise Server is installed. To migrate PowerPlay content from Upfront, you must install the IBM Cognos Series 7 migration components on the computer where Upfront is installed.

You can install each component on a separate computer, or on the same computer. You must install the gateway on a computer that is also running a Web server.

**Stopping services sequence**

If you need to stop services in a distributed environment, the sequence is important. Stop the IBM Cognos service for Application Tier Components first, followed by the standby Content Manager, and then the active Content Manager.

It is important to also stop the following:
- applications that are related to the IBM Cognos service, such as Framework Manager, IBM Cognos Transformer, IBM Cognos Connection, IBM Cognos Administration, and Metric Designer
- any Software Development Kit applications that are running

**Upgrading your installation**

If you are upgrading from a previous release of IBM Cognos PowerPlay, you must use the upgrading steps.
If you are upgrading from a previous release of IBM Cognos products, see Chapter 4, “Upgrade IBM Cognos Business Intelligence,” on page 39.

If you are upgrading from an earlier version of IBM Cognos BI, all the distributed components must be the same version of IBM Cognos BI. If you install IBM Cognos BI on additional or alternate hosts, you must update location-specific properties in IBM Cognos Configuration.

If you will be using PowerCubes that are secured against an IBM Cognos Series 7 namespace, you must install IBM Cognos PowerPlay on a computer that supports IBM Cognos Series 7.

If you are upgrading IBM Cognos BI in an environment that includes earlier versions of other IBM Cognos BI products, such as IBM Cognos BI Controller Version 8.x IBM Cognos BI Planning Version 8.x, or IBM Cognos BI Analysis for Microsoft Excel Version 8.x, install the new version of IBM Cognos BI in a separate location from the other IBM Cognos BI product and configure the new version of IBM Cognos BI to operate independently of that product. After you upgrade the other product to a compatible version with IBM Cognos BI, you can then configure the two products to operate together.

**Windows installations**

For Microsoft Windows operating system installations, ensure that you have administrator privileges for the Windows computer you are installing on. Also ensure that your computer has a TEMP system variable that points to the directory where you want to store temporary files. During installation, files from the disk are temporarily copied to this directory.

**UNIX installations**

For UNIX operating system installations, you can install server components using a graphical user interface or by running a silent installation. To run graphical-mode installation, the console attached to your UNIX computer must support a Java-based graphical user interface.

Also, IBM Cognos BI respects the file mode creation mask (umask) of the account running the installation program. This affects only the installation directories. It does not affect the file permissions within the directories. However, run-time generated files, such as logs, respect the mask. Use umask 022 on the installation directory.

**Cognos Content Database as content store**

If you want to use Cognos Content Database as your content store, you must select it in the installation wizard. If you are installing components on several computers, you need to only install Cognos Content Database once.

**Printer requirements**

To ensure that reports print properly on Windows, Adobe Reader requires that you configure at least one printer on the operating system where Application Tier Components are installed. All reports, regardless of the print format that you choose, are sent as temporary PDF files to Adobe Reader for printing.
Installation sequence for server components

In a distributed installation, the sequence in which you configure components is important. Configure and start the services in at least one location where you installed Content Manager before you configure other server components.

You must configure the gateway component last so that cryptographic keys are shared and secure communication can take place among the three components. The server specified for the external dispatcher URI property on the gateway computer must be the last server component that you start.

We recommend that you install and configure all server components before you install Microsoft Windows operating system components.

The following diagram shows the sequence of the installation process for distributed components. After planning and preparing your environment, install and configure Content Manager components, then Application Tier Components and then gateways. After server components are installed, you install and configure Framework Manager.
Recommendation - Install and Configure the Basic Installation for Distributed Installations

When you do a distributed installation, there are many different installation and configuration options that you can do to customize IBM Cognos BI so that it fits into your corporate infrastructure.

Do a basic installation first, which involves installing one or more instances of each of the required server components (gateway, Application Tier Components and Content Manager) and installing Framework Manager. Perform only the required configuration tasks, such as configuring distributed components to communicate with each other, to get your distributed environment running before you customize your settings.
Later, you can add optional components and customize your configuration settings to better suit your business intelligence needs.

The sequence in which you configure computers is important. You must configure and then start the services on at least one computer where you installed Content Manager before you configure other server components or Framework Manager. For more information, see “Installation sequence for server components” on page 89.

The simplest and quickest way to get IBM Cognos BI running in your environment is ensuring that a basic installation works in your environment.

### Installing and Configuring Content Manager

You can install more than one Content Manager to ensure failover, and you can install Content Manager in a separate location than other components to enhance performance.

The Content Manager computers must know the location of the content store, the location of other Content Manager components, and the database that is used for notification.

In a distributed installation, at least one of the computers where you install Content Manager must be configured, running and accessible before you configure other computers in your IBM Cognos environment. This ensures that the certificate authority service, which is installed with Content Manager, is available to issue certificates to other computers.

Your installation may include more than one Content Manager, each on a different computer. One Content Manager computer is active and one or more Content Manager computers are on standby.

### Permissions

You can install using either root or non-root authority.

Also, IBM Cognos BI respects the file mode creation mask (umask) of the account running the installation program. This affects only the installation directories. It does not affect the file permissions within the directories. However, run-time generated files, such as logs, respect the mask. We recommend umask 022 on the installation directory.

### Rules for configuring

In an installation where you have more than one Content Manager components, or where Content Manager is located in a separate location, at least one of the one Content Manager must be configured, running and accessible before you configure other components in your environment. This ensures that the certificate authority service, which is installed with Content Manager, is available to issue certificates to other IBM Cognos computers.

For information about the sequence of the installation process for distributed components, see “Installation sequence for server components” on page 89.
**Rules for active Content Manager**

If you are installing multiple Content Manager components, the first Content Manager computer that you start becomes the default active Content Manager. You can designate another Content Manager computer as default active, using IBM Cognos Administration.

The standby Content Manager computers are for failover protection. If the active Content Manager computer is not available because of a software or hardware failure, a standby Content Manager computer becomes active and requests are directed to it.

When the active Content Manager fails, unsaved session data is lost. When another Content Manager becomes active, users may be prompted to log on.

For information about activating a Content Manager service, see the *Administration and Security Guide*. For information about active and standby Content Manager components, see "Active and Standby Content Manager Components."

In installations with multiple Content Managers, configure IBM Cognos BI to use compiled gateways instead of the default CGI gateway. For example, use Apache Module for Apache Server or for IBM HTTP Server, or use ISAPI for IIS. Otherwise, performance may be affected after failover.

**Upgrading**

If you are upgrading from ReportNet or an earlier version of IBM Cognos BI, you can use the existing configuration data. However, some features in IBM Cognos BI are new and may require configuration.

**PowerCubes**

If you plan to install IBM Cognos Transformer and you will be using PowerCubes that are secured against an IBM Cognos Series 7 namespace, you must install Content Manager on a computer that supports IBM Cognos Series 7.

**Active and Standby Content Manager Components**

You can install any number of installations of Content Manager, although only one is active at any time. The other installations each act as a standby Content Manager.

The standby Content Manager components are for failover protection. If the active Content Manager is not available because of a software or hardware failure, a standby Content Manager becomes active and requests are directed to it.

When the active Content Manager fails, unsaved session data is lost. When another Content Manager becomes active, users may be prompted to log on.

By default, the first Content Manager installed with IBM Cognos BI is the active one. An IBM Cognos BI server administrator can change the default Content Manager and the active Content Manager at any time. When IBM Cognos BI is started, the default Content Manager locks the content store from access by all other installations of Content Manager. These other Content Manager installations enter standby mode.
This failover mechanism works because dispatchers and the active Content Manager routinely communicate with each other. If a dispatcher can no longer reach Content Manager, the dispatcher signals a standby Content Manager, which becomes the active Content Manager. The other installations of Content Manager remain in standby mode for continuing failover support. The standby Content Managers retrieve cryptographic settings, such as the common symmetric key (used to encrypt and decrypt data), from the active Content Manager.

**Install the Content Manager components**

To install Content Manager, use the disk for your operating system. In the installation wizard, clear all components except Content Manager.

If you are installing IBM Cognos PowerPlay to work with IBM Cognos Business Intelligence, install the PowerPlay Content Manager component on the same computers that include the IBM Cognos Business Intelligence Content Manager components.

If you are installing multiple Content Managers, you must ensure that the system clocks on the Content Manager computers are synchronized for successful failover between Content Managers.

**Cognos Content Database**

If you want to use the Cognos Content Database as your content store, must select it in the installation wizard. If you are installing components on several computers, you need to only install Cognos Content Database once.

**Installing Content Manager on UNIX or Linux operating systems**

Use the following procedure to install Content Manager on a UNIX or Linux operating system.

**Before you begin**

Go to the [IBM Software Product Compatibility Reports (SPCR) page](https://www.ibm.com/support/docview.wss?uid=swg27037784). Verify that you have the required patches installed on your computer before you install the product.

**Procedure**

1. If you are installing to a directory with other IBM Cognos BI components, stop the IBM Cognos service.
2. Set the JAVA_HOME environment variable to point to the installation location of your Java Runtime Environment (JRE).
   
   An example of the installation location of a Java Runtime Environment is `/directory/java/java_version/jre`.

   IBM Cognos BI requires a JVM, such as the Java that is provided by IBM, to run on a Linux operating system.

   If you are installing in a location with other IBM Cognos BI components, use the existing JAVA_HOME environment variable.

3. On HP-UX, set the _M_ARENA_OPTS environment variable as follows:

   _M_ARENA_OPTS 1:4

   This increases the memory allocation for HP-UX to more closely match that of other UNIX platforms.
4. On AIX, if you are using a servlet gateway, set the AIXTHREAD_SCOPE environment variable as follows:
   AIXTHREAD_SCOPE=S
   This sets the contention scope for user threads to system-wide, which supports more efficient scheduling of user threads.

5. If installing from a download, go to the location where the installation files were downloaded and extracted.

6. If installing from a disk, mount the disk using Rock Ridge file extensions.
To mount the disk on HP-UX, do the following:
   • Add the pfs_mount directory in your path.
     For example,
     PATH=/usr/sbin/:$PATH
     export PATH
   • To start the required NFS daemons and run the daemons in the background, type bg pfs_mountd and then type bg pfsd
   • To mount the drive, type
     pfs_mount -t rrip <device><mount_dir> -o xlat=unix
     For example,
     pfs_mount /dev/dsk/c0t2d0 /cdrom -o xlat=unix
   You can now install or copy files as a non-root user using an IBM Cognos disk from this drive.
   • When the installation is complete, type pfs_umount /cdrom and kill the pfsd and pfs_mountd daemons to unmount the disk.

7. To start the installation wizard, go to the operating system directory and then type
   ./issetup

   Note: When you use the issetup command with XWindows, Japanese characters in messages and log files may be corrupted. When installing in Japanese on UNIX or Linux, first set environment variables LANG=C and LC_ALL=C (where C is the language code, for example ja_JP.PCK on Solaris), and then start the installation wizard.
   If you do not use XWindows, run an unattended installation (Chapter 12, “Using an unattended installation and configuration,” on page 265).
   If you do not use XWindows, run an unattended installation. For more information, see the Installation and Configuration Guide.
   If you are installing on Linux operating systems, and you receive error messages about missing openmotif libraries, you can use an unattended installation with the issetupnx command.

8. Follow the directions in the installation wizard and copy the required files to your computer.
   • When selecting the directory, consider the following:
     Install Content Manager in a directory that contains only ASCII characters in the path name. Some UNIX and Linux Web servers do not support non-ASCII characters in directory names.
     If you are installing IBM Cognos BI on a computer that has an earlier version of IBM Cognos BI and you want to keep the earlier version, you must install IBM Cognos BI in a different directory.
   • When selecting components, clear all components except Content Manager.
If you want to use the pre configured database, also select Cognos Content Database.

9. In the Finish page of the installation wizard, do the following:
   • If you want to see the log files, click View for the appropriate log file.
   • If you want to see late-breaking information about the product, select the check box for IBM Cognos Release Notes.
   • Do not configure IBM Cognos BI immediately because you must do other tasks first to ensure that your environment is properly set up. Ensure that the IBM Cognos Configuration check box is clear.
     You can later configure IBM Cognos BI using IBM Cognos Configuration by typing cogconfig.sh in the \c10\location\bin64 directory.
   • Click Finish.

10. Append the \c10\location\bin directory to the appropriate library path environment variable.
    • For Solaris and Linux, LD_LIBRARY_PATH
    • For AIX, LIBPATH
    • For HP-UX, SHLIB_PATH

Installing Content Manager on Windows operating systems
Use the following procedure to install Content Manager on a Microsoft Windows operating system.

For Windows Vista, Windows 7, or Windows 2008 computers, the default installation location uses the Program Files (x86) directory. If you install to this location, ensure that you run IBM Cognos Configuration as an Administrator. Alternatively, you can install the product outside of the Program Files (x86) directory. For example, you can change the installation directory to something like C:\IBM\cognos\c10.

Before you begin
Go to the IBM Software Product Compatibility Reports (SPCR) page (www.ibm.com/support/docview.wss?uid=swe27037784). Verify that you have the required patches installed on your computer before you install the product.

Procedure
1. If you are installing to a directory with other IBM Cognos BI components, stop the IBM Cognos service.
2. Do one of the following:
   • Insert the IBM Cognos product disk.
     If the installation wizard does not open automatically, go to the operating system directory, and double-click issetup.exe.
   • Go to the location where the installation files were downloaded and extracted and then double-click issetup.exe.
3. Select the language to use for the installation.
   The language that you select determines the language of the user interface. All supported languages are installed. You can change the user interface to any of the installed languages after installation.
4. Follow the directions in the installation wizard to copy the required files to your computer.
   • When selecting the directory, consider the following:
Install Content Manager in a directory that contains only ASCII characters in the path name. Some Microsoft Windows operating system Web servers do not support non-ASCII characters in directory names.

If you are installing IBM Cognos BI on a computer that has an earlier version of IBM Cognos BI and you want to keep the earlier version, you must install IBM Cognos BI in a different directory.

- When selecting components, clear all components except Content Manager.
  If you want to use the pre configured database, also select Cognos Content Database.

5. In the Finish page of the installation wizard, do the following:
   - If you want to see the log files, click View for the appropriate log file.
   - If you want to see late-breaking information about the product, select the check box for IBM Cognos Release Notes.
   - If you start IBM Cognos Configuration from the installation wizard, ensure that you follow the additional tasks in this section to ensure that your environment is properly set up before you start the services.

You can start IBM Cognos Configuration using the IBM Cognos Configuration shortcut from the Start menu.

- Click Finish.

### Installing fix packs

IBM provides interim maintenance packages that contain updates to one or more components in your IBM Cognos product. If a fix pack is available when you are installing or upgrading your product, you must install it after you install the IBM Cognos components.

Fix packs are cumulative. When you install the latest fix pack, it includes updates from all the previous fix packs. Fix packs are available for download from IBM Support (http://www.ibm.com/support/entry/portal/overview).

**Note:** Fix packs are not standalone installations. You must install them on computers that have IBM Cognos components installed. Install the fix packs that are appropriate for your product version. To check your version, open the component list file at \c10_location\cmplst.txt and check the line that starts with C8PPCLIENT_version= for the PowerPlay Client and C8PPES_version= for the PowerPlay server version.

### Installing Fix Packs on Windows operating systems

Fix packs are product updates that contain cumulative code fixes that were made since the last release of the product. IBM Cognos fix packs are installed in the same location as the existing product.

**Procedure**

1. Insert the fix pack disk for the Windows operating system or go to the location where you downloaded and extracted the files, and double-click the issetup.exe file.
2. Follow the directions in the installation wizard to install the fix pack files to the same location as the existing IBM Cognos components.
3. If required, update the new installation files with any changes from the backup copies of your customized files.

   To prevent errors, before copying the customized files, compare both versions of the files. This validation determines whether you can replace the file.
4. If you have a distributed environment, repeat these steps for all remaining IBM Cognos servers.

**Installing IBM Cognos fix packs on UNIX or Linux operating systems**

Fix packs are product updates that contain cumulative code fixes that were made since the last release of the product. IBM Cognos fix packs are installed in the same location as the existing product.

**Procedure**

1. Go to the location where the installation files are downloaded, or insert the disc if you have one.
2. To start the installation wizard, type the following command
   ```bash
   ./issetup
   ```
3. Follow the directions in the installation wizard to install the fix pack files to the same location as the existing IBM Cognos components.
4. If required, update the new installation files with any changes from the backup copies of your customized files.
   To prevent errors, before copying the customized files, compare both versions of the files. This validation determines whether you can replace the file.
5. If you have a distributed environment, repeat these steps for all remaining IBM Cognos servers.

**Set up database connectivity for the content store database**

If you are using a database other than Cognos Content Database or Microsoft SQL Server as the content store, you may have to install database client software, or Java Database Connectivity (JDBC) drivers, or both, on each computer where you install Content Manager. Doing this allows Content Manager to access the content store database.

**Set up database connectivity for an IBM DB2 content store**

This procedure describes how to set up database connectivity for a DB2 content store. You must perform this procedure on each computer where you install Content Manager.

You must use a type 4 Java Database Connectivity (JDBC) driver to connect to your content store if you are using IBM DB2.

The type 4 driver is considered an independent product. It does not require the DB2 client to be installed.

**Procedure**

Copy the following files from `DB2_installation\sql\lib\java` directory to the `c10_location\webapps\p2pd\WEB-INF\lib` directory:
- The universal driver file, `db2jcc.jar`
- The license file:
  - For DB2 on Linux, UNIX, or Windows operating systems, use `db2jcc_license_cu.jar`.
  - For DB2 on z/OS, use `db2jcc_license_cisuz.jar`.
  - If you are connecting to DB2 on z/OS, use the driver version from Linux, UNIX, or Windows version 9.1 fix pack 5 or version 9.5 fix pack 2.
Tip: To check the driver version, run the following command:
java -cp path\db2jcc.jar com.ibm.db2.jcc.DB2Jcc -version

Generating a script file to create a database for a DB2 content store:

You can generate a script file to automatically create the content store in IBM DB2 on all platforms. The script file is called a DDL file.

Procedure
1. Start IBM Cognos Configuration.
2. In the Explorer window, under Data Access > Content Manager, click Content Store.
   The default configuration is for an IBM DB2 database. Ensure that the Type is DB2 database.
3. In the Database server and port number field, enter the name of your computer and port number on which DB2 is running. For example, localhost:50000. Where, 50000 is the default port number that is used by IBM DB2. If you are using a different port number, ensure you use that value.
4. Click the Value field next to the User ID and password property and then click the edit icon. Type the appropriate values and click OK.
5. In the Properties window, for the Database name property, type the name for your content store database.
   **Important:** Do not use a name longer than eight characters and use only letters, numbers, underscores, and hyphens in the name.
6. Right-click Content Store, and click Generate DDL.
7. Click Details to record the location of the generated DDL file.
   The DDL file named createDB.sql is created. The script is created in the c10_location/configuration/schemas/content/db2 directory.

What to do next

Use this script to create a database in IBM DB2. For more information about using a DDL file, see your IBM DB2 documentation.

If you use the IBM DB2 command-line interface, you can run the script by entering the following command:
```
db2 -tvf createDB.sql
```

Creating tablespaces for a content store on DB2 for z/OS:

A database administrator must run scripts to create a set of tablespaces required for the content store database. Modify the scripts to replace the placeholder parameters with ones that are appropriate for your environment.

By default, the content store is used for notifications, human tasks, and annotations. You can create separate databases for each.

About this task

Ensure that you use the naming conventions for DB2 on z/OS. For example, all names of parameters must start with a letter and the length must not exceed eight characters. There are two exceptions to the character length limit:
• CMSCRIPT_CS_ID is no more than 2 characters.
• CMSCRIPT_TABLESPACE is no more than 6 characters.

The reason for the exception is that when the two parameters are concatenated the character length can be no more than 8.

For more information, see the IBM DB2 Information Center.

**Procedure**
1. Connect to the database as a user that has privileges to create and drop tablespaces and to allow execution of SQL statements.
2. Go to the directory that contains the scripts:
   ```
c10_location/configuration/schemas/content/db2z0S
   ```
3. Make a backup copy of the `tablespace_db2z0S.sql` script file and save the file to another location.
4. Open the original `tablespace_db2z0S.sql` script file.
   a. Add a connection statement to the beginning of the script.
      For example, `connect to databasename;`
   b. Use the following table to help you to replace the generic parameters with ones appropriate for your environment.
      Not all of the parameters listed are in the script, but some might be added in the future.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMSCRIPT_STOGROUP</td>
<td>Specifies the name of the storage group.</td>
</tr>
<tr>
<td>CMSCRIPT_DATABASE</td>
<td>Specifies the name of the content store database.</td>
</tr>
<tr>
<td>CMSCRIPT_CS_ID</td>
<td>Specifies the subsystem identification for the content store database.</td>
</tr>
<tr>
<td></td>
<td>The ID must not be longer than 2 characters.</td>
</tr>
</tbody>
</table>
| CMSCRIPT_TABLESPACE  | Specifies the name of the tablespace that contains all of the base tables in
                      | the content store.                                                       |
|                      | Auxiliary tables are not included.                                          |
|                      | The name cannot be longer than 6 characters.                               |
| CMSCRIPT_LARGE_BP    | Specifies the name of the large buffer pool allocated for especially large objects. |
|                      | This buffer pool is the 32 KB buffer pool that was created when the database administrator created the content store database on the z/OS system. |
Table 25. Parameter names and description for the content store tablespace script (continued)

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMSCRIPT_REGULAR_BP</td>
<td>Specifies the name of the regular size buffer pool allocated for regular and large objects. This bufferpool is the 16 KB buffer pool that was created when the database administrator created the content store database on the z/OS system.</td>
</tr>
<tr>
<td>CMSCRIPT_USERNAME</td>
<td>Specifies the user account that accesses the content store database.</td>
</tr>
</tbody>
</table>

5. Save and run the script.
   For example, if you set up your clp.properties file and your DB2 alias in your profile or tcshrc script file, type the following command to run the script:
   ```
   db2 -tvf tablespace_db2zOS.sql
   ```

6. Grant the IBM Cognos user rights to the tablespaces that were created when you ran the tablespace_db2zOS.sql file script:
   a. Make a copy of the rightsGrant_db2zOS.sql script file and store it in another location.
   b. In the remote access tool, open the original rightsGrant_db2zOS.sql script file and replace the placeholder parameters with values that are appropriate for your environment.
      Ensure that you use the same values that you used when you allocated resources to the buffer pools and user account.
   c. Add a connection statement to the beginning of the script.
      For example, `connect to databasename user username using password;`
   d. Save and then run the script.
      For example, `db2 -tvf rightsGrant_db2zOS.sql`

7. To create the notification tablespaces, go to the c10_location/configuration/schemas/delivery/zosdb2 directory.
   a. Make a backup copy of the NC_TABLESPACES.sql script file and save the file to another location.
   b. Open the original NC_TABLESPACES.sql script file and use the following table to help you to replace the placeholder parameters with ones appropriate for your environment.

Table 26. Tablespace parameter names and descriptions for the DB2 notification database on z/OS

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCCOG</td>
<td>Specifies the name of the notification database.</td>
</tr>
<tr>
<td>DSN8G810</td>
<td>Specifies the name of the storage group.</td>
</tr>
<tr>
<td>BP32K</td>
<td>Specifies the name of the buffer pool.</td>
</tr>
</tbody>
</table>

Not all of the parameters listed are in the script, but might be added in the future.

   c. Save and run the script.
For example,
```
db2 -tvf NC_TABLESPACES.sql
```
d. Open the NC_CREATE_DB2.sql script file and replace the NCCOG placeholder parameter with the name of the notification database.
e. Save the script.
The Job and Scheduling Monitor services will automatically run the script. However, you may choose to run it yourself.

8. To create the human tasks tablespaces, go to the `c10_location/configuration/schemas/hts/zosdb2` directory.
a. Make a backup copy of the HTS_tablespaces.sql script file and save the file to another location.
b. Open the original HTS_TABLESPACES.sql script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCCOG</td>
<td>Specifies the name of the database.</td>
</tr>
<tr>
<td>DSN8G810</td>
<td>Specifies the name of the storage group.</td>
</tr>
<tr>
<td>BP32K</td>
<td>Specifies name of the 32 k buffer pool.</td>
</tr>
</tbody>
</table>

See the script for a complete list of the parameters required.
c. Save and run the script.
d. Open the HTS_CREATE_Db2zos.sql script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCCOG</td>
<td>The name of the database.</td>
</tr>
</tbody>
</table>

See the script for a complete list of the parameters required.
e. Save and run the script.

9. To create the annotations tablespaces, go to the `c10_location/configuration/schemas/ans/zosdb2` directory.
a. Make a backup copy of the ANN_TABLESPACES.sql script file and save the file to another location.
b. Open the original ANN_TABLESPACES.sql script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCCOG</td>
<td>The name of the database.</td>
</tr>
<tr>
<td>DSN8G810</td>
<td>The name of the storage group.</td>
</tr>
<tr>
<td>BP32K</td>
<td>The name of the 32 k buffer pool.</td>
</tr>
</tbody>
</table>

See the script for a complete list of the parameters required.
c. Save and run the script.
d. Open the ANS2_CREATE_Db2zos.sql script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCCOG</td>
<td>The name of the database.</td>
</tr>
</tbody>
</table>

See the script for a complete list of the parameters required.

Set up database connectivity for an Oracle content store
This procedure describes how to set up database connectivity for an Oracle content store. You must perform this procedure on each computer where you install Content Manager.

Procedure
1. On the computer where the Oracle client is installed, go to the ORACLE_HOME/jdbc/lib directory.
2. Copy the correct library file for your version of the Oracle client to the c10_location/webapps/p2pd/WEB-INF/lib directory on the computer where Content Manager is installed and where notification is sent to an Oracle database.
   - If you are using Oracle 10g, you must have ojdbc14.jar.
   - If you are using Oracle 11g, you must have ojdbc5.jar.
   The files are available from an Oracle client or server install, and can also be downloaded from the Oracle technology Web site.

Set up database connectivity for an Informix content store
This procedure describes how to set up database connectivity for an Informix content store. You must perform this procedure on each computer where you install Content Manager.

Procedure
1. On the computer where Informix is installed, go to the Informix_location/sqllib/java directory.
2. Copy the following files to the c10_location/webapps/p2pd/WEB-INF/lib directory on every computer where Content Manager is installed.
   - the universal driver file, db2jcc.jar
   - the license file, db2jcc_license_cisuz.jar

Set up database connectivity for a Sybase content store
This procedure describes how to set up database connectivity for a Sybase content store. You must perform this procedure on each computer where you install Content Manager.

Procedure
1. On the computer where Sybase is installed, go to the Sybase_location/jConnect-6/classes directory.
2. Copy the jconn3.jar file to the c10_location/webapps/p2pd/WEB-INF/lib directory on every computer where Content Manager is installed and where notification is sent to a Sybase database.
Start IBM Cognos Configuration

Use IBM Cognos Configuration to configure IBM Cognos Business Intelligence components and to start and stop IBM Cognos services if you are using the default Tomcat servlet container.

Before you begin

Before starting IBM Cognos Configuration, ensure that the operating environment is properly set up. For example, ensure that all environment variables have been set.

On a Microsoft Windows operating system, you can start IBM Cognos Configuration in the last page of the installation wizard only if additional setup is not required. For example, if you use a database server other than Microsoft SQL or Cognos Content Database for the content store, copy the Java Database Connectivity (JDBC) drivers to the appropriate location before you start the configuration tool.

On UNIX or Linux operating systems, do not start IBM Cognos Configuration in the last page of the installation wizard. Additional setup is required before you can configure IBM Cognos BI. For example, you must update your Java environment.

Ensure that user or service account used to run IBM Cognos has been set up.

Procedure

1. On Microsoft Windows, click Start > IBM Cognos Configuration.
   
   If you are using a Windows Vista, Windows 7, or Windows 2008 computer, and have installed the product to the Program Files (x86) directory, start IBM Cognos Configuration as an Administrator.

2. On UNIX or Linux operating systems, go to the c10_location/bin64 directory and then type the following command:
   
   ./cogconfig.sh
   
   If IBM Cognos Configuration does not open, ensure that you set the DISPLAY environment variable.

   If you see a JAVA.Lang.unsatisfied link message, verify that you are using a supported version of Java.

   If you see a Java.lang.unsupportedClassVersionError message, ensure that you are using a 64-bit version of Java.

Set Database Connection Properties for the Content Store

You must specify the database server information to ensure that Content Manager can connect to the database you use for the content store. Content Manager uses the database logon to access the content store. After you set the database connection properties, you can test the connection between Content Manager and the content store.

If you installed Cognos Content Database, the database connection properties use the Cognos Content Database by default. You do not have to change the default connection properties. However, Cognos Content Database is for test or proof-of-concept systems only. When you move to a production environment, you must use an enterprise-level database for your content store.
If you are upgrading from ReportNet or an earlier version of IBM Cognos BI, configure IBM Cognos BI to point to a copy of the existing content store database. After you save the configuration and start the IBM Cognos service, the data in the content store is automatically upgraded and cannot be used by the earlier version. By using a copy of the original database with the new version, you can keep ReportNet or the earlier version running with the original data.

**Setting database connection properties for a DB2 content store**

You must specify the database server information to ensure that Content Manager can connect to the database you use for the content store.

**Procedure**

1. In the location where you installed Content Manager, start IBM Cognos Configuration.
2. In the Explorer window, under Data Access, Content Manager, click Content Store.
3. In the Properties window, for the Database name property, type the name of the database or the database alias.
4. Change the logon credentials to specify a valid user ID and password:
   - Click the Value box next to the User ID and password property and then click the edit button when it appears.
     - If you are connecting to a database on DB2 on z/OS, ensure that you specify the same user ID as the value you specified for CMSCRIPT_USERNAME when you created the tablespaces.
   - Type the appropriate values and click OK.
5. In the Database server and port number field, enter the name of your computer and port number on which DB2 is running. For example, localhost:50000. 50000 is the default port number used by DB2. If you are using a different port number, ensure you use that value.
6. If you are connecting to a database on DB2 on z/OS:
   a. In the Explorer window, click Local Configuration.
   b. In the Properties window, next to Advanced properties, click inside the Value box, and then click the edit icon.
   c. Click Add to add the parameters that you used to create the tablespaces. Add all of the parameters except CMSCRIPT_USERNAME.
7. From the File menu, click Save.

**Setting database connection properties for a Microsoft SQL Server, Oracle, Informix, or Sybase content store**

You must specify the database server information to ensure that Content Manager can connect to the database you use for the content store.

**Procedure**

1. Start IBM Cognos Configuration.
2. In the Explorer window, under Data Access, Content Manager, right-click Content Store and click Delete.
   - This step deletes the connection to the default resource. Content Manager can access only one content store.
3. Right-click Content Manager, and then click New resource, Database.
4. In the Name box, type a name for the resource.
5. In the Type box, select the type of database and click OK.
Tip: If you want to use an Oracle Net8 keyword-value pair to manage the database connection, select Oracle database (Advanced).

6. In the Properties window, provide the values for your database type:
   - If you use a Microsoft SQL Server database, type the appropriate values for the Database server with port number or instance name and Database name properties.
     For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the Database server with port number or instance name property.
     For the Database server with port number or instance name property, include the instance name if there are multiple instances of Microsoft SQL Server.
     To connect to a named instance, you must specify the instance name as a Java Database Connectivity (JDBC) URL property or a data source property. For example, you can type localhost\instance1. If no instance name property is specified, a connection to the default instance is created.
     The properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:
     jdbc:JSQLConnect://localhost\instance1/user=sa/
more properties as required
     To connect to a named instance, you must specify the instance name. For example, you can type localhost\instance1. If an instance name is not specified, a connection to the default instance is created.
   - If you use an Oracle database, type the appropriate values for the Database server and port number and SID properties.
   - If you use an advanced Oracle database, for the Database specifier property, type the Oracle Net8 keyword-value pair for the connection.
     Here is an example:
     (description=(address=(host=myhost)(protocol=tcp)(port=1521)
     (connect_data=(sid=(orcl))))))
     When you select the advanced Oracle database, IBM Cognos BI uses enterprise-oriented Oracle features to select a listener, switch to another listener if the first listener fails, automatically reconnect to the database if the connection fails, balance connection requests among listeners, and balance connection requests among dispatchers.
   - If you use an Informix database, type the appropriate values for the Database server and port number and Database name properties.
   - If you use a Sybase database, type the appropriate values for the Database server and port number and Database name properties.

7. To configure logon credentials, specify a user ID and password:
   - Click the Value box next to the User ID and password property and then click the edit icon when it appears.
   - Type the appropriate values and click OK.

8. If you host more than one content store database on an Informix instance, create the advanced property CMSCRIPT_CS_ID and specify the account under which the instance runs:
   - In the Explorer window, click Local Configuration.
   - In the Properties window, click the Value column for Advanced properties and then click the edit icon.
   - In the Value - Advanced properties dialog box, click Add.
In the Name column, type CMSCRIPT_CS_ID
In the Value column, type the user ID of the account under which the instance of the content store runs.
Use a different user account for each instance of Informix content store database.

9. From the File menu, click Save.
The logon credentials are immediately encrypted.

Results
Content Manager can now create the required tables in the content store when you start the IBM Cognos service for the first time. If the connection properties are not specified correctly, you cannot start the IBM Cognos services.

Configure Environment Properties for Content Manager Computers
The Content Manager computers must know the location of the content store, the other Content Manager computers, and the database that is used for notification.

After installing Content Manager on the computers you are using for failover protection, you must configure Content Manager on those computers. If you installed more than one Content Manager, you must list all Content Manager URIs on each Content Manager computer.

After you complete the required configuration tasks and start the IBM Cognos BI service, the certificate authority service is available to issue certificates to other computers. You can then perform the required configuration tasks on other computers, such as the Application Tier Components computer and gateway computers. Otherwise, you can continue to configure the Content Manager computers by changing the default property settings (see “Changing Default Configuration Settings” on page 182) so that they better suit your environment. For example, you can configure IBM Cognos BI components to use an authentication provider (see Chapter 8, “Configuring IBM Cognos Components to Use an Authentication Provider,” on page 141), enable and disable services (see “Enable and Disable Services” on page 193) on the Content Manager computers, or change global settings (see “Changing Global Settings” on page 223).

Note that if you change global settings on one Content Manager computer, you must make the same changes on the other Content Manager computers.

Configuring the active Content Manager
The Content Manager computers must know the location of the content store, the other Content Manager computers, and the database that is used for notification.

Procedure
1. On the Content Manager computer that you want to designate as the default active Content Manager, start IBM Cognos Configuration.

   Tip: Use the computer with the highest processor speed for the default active Content Manager.

2. In the Explorer window, click Environment.

3. In the Properties window, click the value for Content Manager URIs and then click the edit button.
4. Specify the URIs for the other Content Manager computers:
   - In the **Value - Content Manager URIs** dialog box, click **Add**.
   - In the blank row of the table, click and then type the full URI of the Content Manager computer.
     Do not delete the first value in the table. This value identifies the local Content Manager computer and is required.
     Replace the localhost portion of the URI with a host name or IP address. All URI properties must use the the same format: all host names or all IP addresses.
     - Repeat the previous two bulleted steps for each URI to be added.
     You must include all Content Manager URIs in the list.
   - Click **OK**.
5. In the **Explorer** window, under **Security**, click **Cryptography**.
6. In the **Properties** window, under **CSK settings**, set **Store symmetric key locally** to **True**.
7. From the **File** menu, click **Save**.

**Configuring standby Content Managers**

The Content Manager computers must know the location of the content store, the other Content Manager computers, and the database that is used for notification.

**Procedure**

1. Ensure that you already configured the Environment properties on at least one Content Manager computer and that IBM Cognos BI components are running on that computer.
2. On the standby Content Manager computer, start IBM Cognos Configuration.
3. In the **Explorer** window, click **Environment**.
4. In the **Properties** window, click the value for **Content Manager URIs**, and then click the edit button.
5. Specify the URIs for the other Content Manager computers:
   - In the **Value - Content Manager URIs** dialog box, click **Add**.
   - In the blank row of the table, click and then type the full URI of the Content Manager computer.
     Do not delete the first value in the table. This value identifies the local Content Manager computer and is required.
     Replace the localhost portion of the URI with a host name or IP address. All URI properties must use the the same format: all host names or all IP addresses.
     - Repeat the previous two bulleted steps for each URI to be added.
     You must include all Content Manager URIs in the list.
   - Click **OK**.
6. In the **Explorer** window, under **Security > Cryptography**, click **Cognos**, the default cryptographic provider.
7. Ensure that all cryptographic settings match what you configured on the default active Content Manager computer.
8. In the **Explorer** window, under **Data Access > Content Manager**, click **Content Store**.
9. Ensure that the values for all of the properties match what you configured on the default active Content Manager computer.
Specify a Connection to a Mail Server Account

If you want to send reports by email, you must configure a connection to a mail server account.

You must also change the host name portion of the Gateway URI from localhost to either the IP address of the computer or the computer name. Otherwise the URL in the email will contain localhost and remote users will not be able to open the report.

Procedure

1. In the location where Content Manager is installed, start IBM Cognos Configuration.
2. In the Explorer window, under Data Access, click Notification.
3. In the Properties window, for the SMTP mail server property, type the host name and port of your SMTP (outgoing) mail server.

   Tip: To be able to open reports that are sent as links, ensure that the Gateway URI on report servers and notification servers specifies an accessible Web server hosting IBM Cognos content. If you have mobile users accessing links remotely, consider using an external URI.
4. Click the Value box next to the Account and password property and then click the edit button when it appears.
5. Type the appropriate values in the Value - Account and password dialog box and then click OK.

   Tip: If logon credentials are not required for the SMTP server, remove the default information for the Account and password property. When you are prompted for confirmation to leave this property blank, click OK. Ensure that the default user name has been removed. Otherwise, the default account is used and notifications will not work properly.
6. In the Properties window, type the appropriate value for the default sender account.
7. Test the mail server connections. In the Explorer window right-click Notification and click Test.

IBM Cognos Business Intelligence tests the mail server connection.

Results

If you do not plan to send reports by email, or do not want to set up a mail server account immediately, you are not required. However, when you save the configuration and then you start the services in IBM Cognos Configuration, you will see a warning message when the mail server connection is tested. You can safely ignore the warning.

Enable Security

By default, IBM Cognos Business Intelligence allows anonymous access. If you want to use security in your IBM Cognos BI environment, you must disable anonymous access and configure IBM Cognos BI to use an authentication provider.
Procedure
1. In the IBM Cognos Configuration Explorer window, click Security -> Authentication -> Cognos.
2. Click the Value box for Allow Anonymous Access, and select False.
4. In the Name box, type a name for your authentication namespace.
5. In the Type list, click the appropriate namespace type and then click OK.
   The new authentication provider resource appears in the Explorer window, under the Authentication component.
6. In the Properties window, for the Namespace ID property, specify a unique identifier for the namespace.
7. From the File menu, click Save.

Configure an IBM Cognos Series 7 Namespace in IBM Cognos BI

If you want to migrate security information or secured content from IBM Cognos Series 7 to IBM Cognos Business Intelligence, you must configure a namespace in IBM Cognos BI that is identical to the IBM Cognos Series 7 namespace.

You can configure multiple namespaces for authentication in IBM Cognos BI. For more information, see Chapter 8, “Configuring IBM Cognos Components to Use an Authentication Provider,” on page 141.

Note: You cannot use an IBM Cognos Series 7 Local Authentication Export (LAE) file for authentication with IBM Cognos BI components.

All IBM Cognos Series 7 namespaces should use the same primary IBM Cognos Series 7 Ticket Server. Otherwise, you may receive errors or be prompted for authentication more than once.

If you change the configuration information stored in the directory server used for IBM Cognos Series 7, you must restart the IBM Cognos BI service before changes take effect in the IBM Cognos installation.

A user must be in at least one Access Manager user class to be able to log on to IBM Cognos BI components.

Procedure
1. Start IBM Cognos Configuration.
2. In the Explorer window, under Security, Authentication, click Cognos.
3. Click the Value box for Allow Anonymous Access, and select False.
5. In the Name box, type a name for the authentication namespace.
6. In the Type list, click IBM Cognos Series 7 and then click OK.
   The new authentication provider resource appears in the Explorer window, under the Authentication component.
7. In the Resource Properties window, specify the mandatory values.
Certain values must match the values you used when you configured the IBM Cognos Series 7 namespace in Configuration Manager. In Configuration Manager, the properties are located in Services, Access Manager - Runtime, Directory Server.

- For **Namespace ID**, specify a unique identifier for the namespace.
- For **Host and port**, type the same value that you used for the **Computer** property in Configuration Manager.
  The format must be identical. If you use an IP address in IBM Cognos Series 7, type the same IP address. If you use a network host name in IBM Cognos Series 7, type the same network host name.
- For **Base Distinguished Name**, type the same value that you used for the **Base Distinguished Name (DN)** property in Configuration Manager.
- For **Namespace name**, type the same value that you used for the **Default Namespace** property in Configuration Manager.
  This value is case sensitive and must match exactly.

8. Specify the values for all other required properties to ensure that IBM Cognos BI components can locate and use your existing authentication provider.

   If your IBM Cognos Series 7 namespace version is 16.0, ensure that the **Data encoding** property is set to UTF-8. In addition, the computers where Content Manager is installed must use the same locale as the data in the IBM Cognos Series 7 namespace.

9. If your namespace environment includes version 15.2 of the IBM Cognos Series 7 namespace, you must disable the **Series7NamespacesAreUnicode** setting.

   - In the Properties window, in the Advanced Properties value, click the edit icon.
   - In the Value - Advanced properties window, click Add.
   - In the Name box, type Series7NamespacesAreUnicode.
   - In the Value box, type False, and then click OK.

10. In the Properties window, under Cookie settings, ensure that the **Path, Domain, and Secure flag enabled** properties match the settings configured for IBM Cognos Series 7.

11. From the File menu, click Save.

**Start Content Manager**

After you have set the database connection properties for the content store, you can start the Content Manager computer.

**Before you begin**

Ensure that user or service account is set up. For information, see "Configure a User Account or Network Service Account for IBM Cognos Business Intelligence" on page 33.

**Procedure**

1. Start IBM Cognos Configuration.
   - If you are upgrading, a message appears indicating that configuration files were detected and upgraded to the new version.
2. Ensure that you save your configuration, otherwise you cannot start the IBM Cognos service.
3. From the Actions menu, click Test.
IBM Cognos Configuration checks the common symmetric keys (CSK) availability, tests the namespace configuration, and tests the connections to the content store and other resources.

Tip: If Test is not available for selection, in the Explorer window, click Local Configuration.

4. If the test fails, reconfigure the affected properties and then test again.
You can test some components individually by right-clicking the component in the Explorer panel and selecting Test.
Do not start the service until all tests pass.

5. From the Actions menu, click Start.
It may take a few minutes for the IBM Cognos service to start.
This action starts all installed services that are not running and registers the IBM Cognos service on Windows.

Test the Content Manager Installation
You can test the installation using a Web browser.

Procedure
1. Open a Web browser.
2. Test that Content Manager is running by typing the URI for the active Content Manager. For example, http://host_name:port/p2pd/servlet
   The default value for host_name:port is localhost:9300.
   Content Manager is available when the State value is Running.

Installing and Configuring Application Tier Components
You can install the Application Tier Components on different computers or on the same computer.

Application Tier Components include PowerPlay Server and PowerPlay Administration. Both are selected by default.

For distributed installations that include only PowerPlay, install both PowerPlay Server and PowerPlay Administration together on one or more computers. For distributed installations that include both PowerPlay and IBM Cognos Business Intelligence, you can install PowerPlay Application tier Components on the same computers as IBM Cognos BI Application Tier Components or on separate computers. If you install PowerPlay Application Tier Components on a separate computer from IBM Cognos BI Application Tier Components, do the following:
- Install just the PowerPlay Administration component on all computers that include IBM Cognos BI Application Tier Components.
- On the computer where you installed the PowerPlay Application Tier components (both PowerPlay Server and PowerPlay Administration), open Cognos Configuration and under IBM Cognos Services, disable the presentation service and report service. Optionally, to reduce demand on system resources, you can disable the query service.

The Application Tier Components computer must know the location of the Content Manager computers and the location of the notification database to use for job and schedule information. Ensure that the computer where you installed the active
Content Manager is configured and available before you configure Application Tier Components computers. If you installed more than one Content Manager, you must list all Content Manager URIs on each Application Tier Components computer.

Perform the following tasks to install and configure the Application Tier Components:

- Install the Application Tier Components
- Install fix packs if available
- Start IBM Cognos Configuration
- Configure environment properties for Application Tier computers
- Start the Application Tier components
- Test the Application Tier components

Install the Application Tier Components

You can install Application Tier Components on one or more computers, depending on your environment.

Application Tier Components include PowerPlay Server and PowerPlay Administration. Both are selected by default.

If you are upgrading from ReportNet or an earlier version of IBM Cognos BI, IBM Cognos BI uses the existing configuration data for the Application Tier Components computers. However, if you installed the Application Tier Components in a new location, you must configure the environment properties.

Ensure that the computer where you installed the active Content Manager is configured and available before you configure Application Tier Components computers.

Installing the Application Tier Components on UNIX or Linux operating systems

You can install Application Tier Components on one or more computers, depending on your environment.

Before you begin

Go to the IBM Software Product Compatibility Reports (SPCR) page (www.ibm.com/support/docview.wss?uid=swg27037784). Verify that you have the required patches installed on your computer before you install the product.

Procedure

1. If you are installing to a directory with other IBM Cognos BI components, stop the IBM Cognos service.
2. Set the JAVA_HOME environment variable to point to the installation location of your Java Runtime Environment (JRE).
   An example of the installation location of a Java Runtime Environment is /directory/java/java_version/jre.
   IBM Cognos BI requires a JVM, such as the Java that is provided by IBM, to run on a Linux operating system.
   If you are installing in a location with other IBM Cognos BI components, use the existing JAVA_HOME environment variable.
3. On HP-UX, set the _M_ARENA_OPTS environment variable as follows:
This increases the memory allocation for HP-UX to more closely match that of other UNIX platforms.

4. On AIX, if you are using a servlet gateway, set the AIXTHREAD_SCOPE environment variable as follows:
   AIXTHREAD_SCOPE=S
   This sets the contention scope for user threads to system-wide, which supports more efficient scheduling of user threads.

5. If installing from a download, go to the location where the installation files were downloaded and extracted.

6. If installing from a disk, mount the disk using Rock Ridge file extensions.

   To mount the disk on HP-UX, do the following:
   • Add the pfs_mount directory in your path.
     For example,
     PATH=/usr/sbin/:$PATH
     export PATH
   • To start the required NFS daemons and run the daemons in the background, type bg pfs_mountd and then type bg pfsd
   • To mount the drive, type
     pfs_mount -t rrip <device><mount_dir> -o xlat=unix
     For example,
     pfs_mount /dev/dsk/c0t2d0 /cdrom -o xlat=unix
     You can now install or copy files as a non-root user using an IBM Cognos disk from this drive.
   • When the installation is complete, type pfsUnmount /cdrom and kill the pfsd and pfs_mountd daemons to unmount the disk.

7. To start the installation wizard, go to the operating system directory and then type
   ./issetup

   **Note:** When you use the issetup command with XWindows, Japanese characters in messages and log files may be corrupted. When installing in Japanese on UNIX or Linux, first set environment variables LANG=C and LC_ALL=C (where C is the language code, for example ja_JP.PCK on Solaris), and then start the installation wizard.

   If you do not use XWindows, run an unattended installation (see "Use a response file from an installation on another computer" on page 266).

   If you do not use XWindows, run an unattended installation. For more information, see the *Installation and Configuration Guide*.

   If you are installing on Linux operating systems, and you receive error messages about missing openmotif libraries, you can use an unattended installation with the issetupnx command.

8. Follow the directions in the installation wizard and copy the required files to your computer.

   • When selecting the directory, consider the following:
     Install Application Tier Components in a directory that contains only ASCII characters in the path name. Some UNIX and Linux Web servers do not support non-ASCII characters in directory names.
9. In the **Finish** page of the installation wizard, do the following:
   - If you want to see the log files, click **View** for the appropriate log file.
   - If you want to see late-breaking information about the product, select the check box for IBM Cognos Release Notes.
   - Do not configure IBM Cognos BI immediately because you must do other tasks first to ensure that your environment is properly set up. Ensure that the IBM Cognos Configuration check box is clear.
     You can later configure IBM Cognos BI using IBM Cognos Configuration by typing `cogconfig.sh` in the `c10_location/bin64` directory.
   - Click **Finish**.

10. Append the `c10_location/bin` directory to the appropriate library path environment variable.
   - For Solaris and Linux, `LD_LIBRARY_PATH`
   - For AIX, `LIBPATH`
   - For HP-UX, `SHLIB_PATH`

### Installing the Application Tier Components on Windows operating system

You can install Application Tier Components on one or more computers, depending on your environment.

For Windows Vista, Windows 7, or Windows 2008 computers, the default installation location uses the Program Files (x86) directory. If you install to this location, ensure that you run IBM Cognos Configuration as an Administrator. Alternatively, you can install the product outside of the Program Files (x86) directory. For example, you can change the installation directory to something like `C:\IBM\cognos\c10`.

**Procedure**

1. If you are installing to a directory with other IBM Cognos BI components, stop the IBM Cognos service.

2. Do one of the following:
   - Insert the IBM Cognos product disk.
     If the installation wizard does not open automatically, go to the operating system directory, and double-click `issetup.exe`.
   - Go to the location where the installation files were downloaded and extracted and then double-click `issetup.exe`.

3. Select the language to use for the installation.
   The language that you select determines the language of the user interface. All supported languages are installed. You can change the user interface to any of the installed languages after installation.

4. Follow the directions in the installation wizard and copy the required files to your computer.
   - When selecting the directory, consider the following:
     Install Application Tier Components in a directory that contains only ASCII characters in the path name. Some Web servers do not support non-ASCII characters in directory names.
   - When selecting components, clear all components except **Application Tier Components**.
5. In the Finish page of the installation wizard, do the following:
   • If you want to see the log files, click View for the appropriate log file.
   • If you want to see late-breaking information about the product, select the check box for IBM Cognos Release Notes.
   • If you start IBM Cognos Configuration from the installation wizard, ensure that you follow the additional tasks in this section to ensure that your environment is properly set up before you start the services.
   You can start IBM Cognos Configuration using the IBM Cognos Configuration shortcut from the Start menu.
   • Click Finish.

Installing fix packs

IBM provides interim maintenance packages that contain updates to one or more components in your IBM Cognos product. If a fix pack is available when you are installing or upgrading your product, you must install it after you install the IBM Cognos components.

Fix packs are cumulative. When you install the latest fix pack, it includes updates from all the previous fix packs. Fix packs are available for download from IBM Support (http://www.ibm.com/support/entry/portal/overview).

Note: Fix packs are not standalone installations. You must install them on computers that have IBM Cognos components installed. Install the fix packs that are appropriate for your product version. To check your version, open the component list file at c10_location\cmplst.txt and check the line that starts with CBPPCLIENT_version= for the PowerPlay Client and CBPPES_version= for the PowerPlay server version.

Installing Fix Packs on Windows operating systems

Fix packs are product updates that contain cumulative code fixes that were made since the last release of the product. IBM Cognos fix packs are installed in the same location as the existing product.

Procedure

1. Insert the fix pack disk for the Windows operating system or go to the location where you downloaded and extracted the files, and double-click the issetup.exe file.
2. Follow the directions in the installation wizard to install the fix pack files to the same location as the existing IBM Cognos components.
3. If required, update the new installation files with any changes from the backup copies of your customized files.
   To prevent errors, before copying the customized files, compare both versions of the files. This validation determines whether you can replace the file.
4. If you have a distributed environment, repeat these steps for all remaining IBM Cognos servers.

Installing IBM Cognos fix packs on UNIX or Linux operating systems

Fix packs are product updates that contain cumulative code fixes that were made since the last release of the product. IBM Cognos fix packs are installed in the same location as the existing product.
Procedure
1. Go to the location where the installation files are downloaded, or insert the disc if you have one.
2. To start the installation wizard, type the following command
   ./issetup
3. Follow the directions in the installation wizard to install the fix pack files to the same location as the existing IBM Cognos components.
4. If required, update the new installation files with any changes from the backup copies of your customized files.
   To prevent errors, before copying the customized files, compare both versions of the files. This validation determines whether you can replace the file.
5. If you have a distributed environment, repeat these steps for all remaining IBM Cognos servers.

Start IBM Cognos Configuration
Use IBM Cognos Configuration to configure IBM Cognos Business Intelligence components and to start and stop IBM Cognos services if you are using the default Tomcat servlet container.

Before you begin
Before starting IBM Cognos Configuration, ensure that the operating environment is properly set up. For example, ensure that all environment variables have been set.

On a Microsoft Windows operating system, you can start IBM Cognos Configuration in the last page of the installation wizard only if additional setup is not required. For example, if you use a database server other than Microsoft SQL or Cognos Content Database for the content store, copy the Java Database Connectivity (JDBC) drivers to the appropriate location before you start the configuration tool.

On UNIX or Linux operating systems, do not start IBM Cognos Configuration in the last page of the installation wizard. Additional setup is required before you can configure IBM Cognos BI. For example, you must update your Java environment.

Ensure that user or service account used to run IBM Cognos has been set up.

Procedure
1. On Microsoft Windows, click Start > IBM Cognos Configuration.
   If you are using a Windows Vista, Windows 7, or Windows 2008 computer, and have installed the product to the Program Files (x86) directory, start IBM Cognos Configuration as an Administrator.
2. On UNIX or Linux operating systems, go to the c10_location/bin64 directory and then type the following command:
   ./cogconfig.sh
   If IBM Cognos Configuration does not open, ensure that you set the DISPLAY environment variable.
   If you see a JAV.A.Lang.unsatisfied link message, verify that you are using a supported version of Java.
   If you see a Java.lang.unsupportedClassVersionError message, ensure that you are using a 64-bit version of Java.
Configure Environment Properties for Application Tier Components Computers

If you install the Application Tier Components component on a different computer than Content Manager, you must configure the Application Tier Components computer so that it knows the location of Content Manager. The distributed components can then communicate with each other.

The Application Tier Components computer must know the location of the Content Manager computers and the notification database to use for job and schedule information. The Application Tier Components computer must use the same notification database that the Content Manager computers use. For more information, see “Change the notification database” on page 202.

If you installed more than one Content Manager, you must list all Content Manager URIs on each Application Tier Components computer.

Procedure
1. Start IBM Cognos Configuration.
2. In the Explorer window, click Environment.
3. In the Properties window, change the localhost portion of the Content Manager URIs property to the name of any Content Manager computer.
4. Specify the URIs for the remaining Content Manager computers:
   • In the Value - Content Manager URIs dialog box, click Add.
   • In the blank row of the table, click and then type the full URI of the Content Manager computer.
     Replace the localhost portion of the URI with a host name or IP address. All URI properties must use the same format: all host names or all IP addresses.
   • Repeat the previous two bulleted steps for each URI to be added.
     You must include all Content Manager URIs in the list.
   • Click OK.
5. Change the localhost portion of the Gateway URI property to the name of the computer on which you plan to install the gateway component.
   This will ensure that users in different locations can connect to reports and workspaces that are sent by email.
6. Change the localhost portion of the remaining URI properties to the name or IP address of your IBM Cognos BI server.
7. In the Explorer window, under Security > Cryptography, click Cognos, the default cryptographic provider.
8. Under the Certificate Authority settings property group, set the Password property to match what you configured on the default active Content Manager computer.
9. Ensure that all other cryptographic settings match what you set on the default active Content Manager computer.
10. From the File menu, click Save.

Start the Application Tier Components

After you have configured the environment properties, you can start the services on the Application Tier Components computer.
Before you begin

To use IBM Cognos BI for reporting, you must install and configure the server components, start the IBM Cognos service, and have a package that references an available data source. Note that if you are upgrading, you can continue to use the same data sources.

Ensure that user or service account is set up. For information, see "Configure a User Account or Network Service Account for IBM Cognos Business Intelligence" on page 33.

Procedure

1. Start IBM Cognos Configuration.
   If you are upgrading, a message appears indicating that configuration files were detected and upgraded to the new version.
2. Ensure that you save your configuration, otherwise you cannot start the IBM Cognos service.
3. From the Actions menu, click Test.
   IBM Cognos Configuration checks the common symmetric keys (CSK) availability, tests the namespace configuration, and tests the connections to the content store and other resources.

   Tip: If Test is not available for selection, in the Explorer window, click Local Configuration.
4. If the test fails, reconfigure the affected properties and then test again.
   You can test some components individually by right-clicking the component in the Explorer panel and selecting Test.
   Do not start the service until all tests pass.
5. From the Actions menu, click Start.
   It may take a few minutes for the IBM Cognos service to start.
   This action starts all installed services that are not running and registers the IBM Cognos service on Windows.

Test the Application Tier Components

You can test the installation using a Web browser.

Procedure

1. Open a Web browser.
2. Test the availability of the dispatcher by typing the External dispatcher URI value from IBM Cognos Configuration. For example, http://host_name:port/p2pd/servlet/dispatch
   The default value for host_name:port is localhost:9300.
   The dispatcher is available when IBM Cognos Connection appears but displaying no graphics or images.

Test IBM Cognos BI Migration Service

You can test the installation of the IBM Cognos Business Intelligence migration service by checking that the Migration Assistant icon appears in IBM Cognos Administration.
Procedure

1. In IBM Cognos Connection, from the toolbar, click Launch, IBM Cognos Administration.
2. Click the Configuration tab.
3. Click Content Administration.

   The Migration Assistant icon appears on the toolbar.

Results

Before you can use the Migration Assistant to migrate IBM Cognos Series 7 content from Upfront, PowerPlay Enterprise Server, and IBM Cognos Connection, you must install migration components with IBM Cognos Series 7. For more information about migration content, see the PowerPlay Migration and Administration Guide.

Installing and Configuring the Gateway

You can install the gateway on one or more computers, depending on your environment. If you have a Web farm, you may want to install an IBM Cognos Business Intelligence gateway on each Web server. Using multiple Web servers to manage incoming requests provides better service. If you install only the gateway component on the same computer as the Web server, your Web server manages the core Web services and does not process user requests. This separation of processing may be required if you have a network firewall between the Web server and your other server components.

Ensure that the computer where you installed the active Content Manager is configured and available before you configure gateway computers.

Perform the following steps to install and configure the gateway:

- Install the gateway components
- Install fix packs if available
- Start IBM Cognos Configuration
- Configure environment and security properties for the gateway
- Configure your Web server
- Test the gateway installation

Installing the gateway components on UNIX or Linux operating systems

You can install the gateway on one or more computers, depending on your environment. If you have a Web farm, you may want to install an IBM Cognos BI gateway on each Web server.

If you installing PowerPlay to work with IBM Cognos Business Intelligence, install the PowerPlay gateway components on the same computers that include the IBM Cognos Business Intelligence gateway components.

Before you begin

Go to the IBM Software Product Compatibility Reports (SPCR) page (www.ibm.com/support/docview.wss?uid=swg27037784). Verify that you have the required patches installed on your computer before you install the product.
**Procedure**

1. If you are installing to a directory with other IBM Cognos BI components, stop the IBM Cognos service.

2. Set the JAVA_HOME environment variable to point to the installation location of your Java Runtime Environment (JRE).
   - An example of the installation location of a Java Runtime Environment is /directory/java/java_version/jre.
   - IBM Cognos BI requires a JVM, such as the Java that is provided by IBM, to run on a Linux operating system.
   - If you are installing in a location with other IBM Cognos BI components, use the existing JAVA_HOME environment variable.

3. On HP-UX, set the _M_ARENA_OPTS environment variable as follows:
   
   _M_ARENA_OPTS 1:4
   
   This increases the memory allocation for HP-UX to more closely match that of other UNIX platforms.

4. On AIX, if you are using a servlet gateway, set the AIXTHREAD_SCOPE environment variable as follows:
   
   AIXTHREAD_SCOPE=S
   
   This sets the contention scope for user threads to system-wide, which supports more efficient scheduling of user threads.

5. If installing from a download, go to the location where the installation files were downloaded and extracted.

6. If installing from a disk, mount the disk using Rock Ridge file extensions.
   - To mount the disk on HP-UX, do the following:
     - Add the pfs_mount directory in your path.
       
       For example,
       
       ```
       PATH=/usr/sbin:/$PATH
       export PATH
       ```
     - To start the required NFS daemons and run the daemons in the background, type bg pfs_mounthood and then type bg pfsd
     - To mount the drive, type
       
       ```
       pfs_mount -t rrip <device><mount_dir> -o xlat=unix
       ```
       
       For example,
       
       ```
       pfs_mount /dev/dsk/c0t2d0 /cdrom -o xlat=unix
       ```
       
       You can now install or copy files as a non-root user using an IBM Cognos disk from this drive.
     - When the installation is complete, type pfs_umount /cdrom and kill the pfsd and pfs_mounthood daemons to unmount the disk.

7. To start the installation wizard, go to the operating system directory and then type
   
   ```
   ./issetup
   ```

**Note:** When you use the issetup command with XWindows, Japanese characters in messages and log files may be corrupted. When installing in Japanese on UNIX or Linux, first set environment variables LANG=C and LC_ALL=C (where C is the language code, for example ja_JP.PCK on Solaris), and then start the installation wizard.

If you do not use XWindows, run an unattended installation (see Chapter 12, "Using an unattended installation and configuration," on page 265).
If you do not use XWindows, run an unattended installation. For more information, see the Installation and Configuration Guide.

If you are installing on Linux operating systems, and you receive error messages about missing openmotif libraries, you can use an unattended installation with the isetupnx command.

8. Follow the directions in the installation wizard and copy the required files to your computer.
   • When selecting the directory, consider the following:
     Install Gateway components in a directory that contains only ASCII characters in the path name. Some UNIX and Linux Web servers do not support non-ASCII characters in directory names.
   • When selecting components, clear all components except Gateway.

9. In the finish page of the installation wizard, do the following:
   • If you want to see the log files, click View for the appropriate log file.
   • If you want to see late-breaking information about the product, select the check box for IBM Cognos Release Notes.
   • Do not configure IBM Cognos BI immediately because you must do other tasks first to ensure that your environment is properly set up. Ensure that the IBM Cognos Configuration check box is clear.
     You can later configure IBM Cognos BI using IBM Cognos Configuration by typing cogconfig.sh in the c10_location/bin64 directory.
   • Click Finish.

10. Append the c10_location/bin directory to the appropriate library path environment variable.
    • For Solaris and Linux, LD_LIBRARY_PATH
    • For AIX, LIBPATH
    • For HP-UX, SHLIB_PATH

What to do next

If you want users to see product documentation in a language other than English, you must install the Supplementary Language Documentation component in the location where you installed the Gateway components. For more information, see “Installing translated product documentation” on page 59.

Installing the gateway components on Windows operating systems

You can install the gateway on one or more computers, depending on your environment. If you have a Web farm, you may want to install an IBM Cognos BI gateway on each Web server.

Procedure

1. If you are installing to a directory with other IBM Cognos BI components, stop the IBM Cognos service.

2. Do one of the following:
   • Insert the IBM Cognos product disk.
     If the installation wizard does not open automatically, go to the operating system directory, and double-click isetup.exe.
   • Go to the location where the installation files were downloaded and extracted and then double-click isetup.exe.
3. Select the language to use for the installation.
   The language that you select determines the language of the user interface. All
   supported languages are installed. You can change the user interface to any of
   the installed languages after installation.

4. Follow the directions in the installation wizard to copy the required files to
   your computer.
   • When selecting the directory, consider the following:
     Install Gateway components in a directory that contains only ASCII
     characters in the path name. Some Microsoft Windows operating system Web
     servers do not support non-ASCII characters in directory names.
   • When selecting components, clear all components except Gateway.

5. In the Finish page of the installation wizard, do the following:
   • If you want to see the log files, click View for the appropriate log file.
   • If you want to see late-breaking information about the product, select the
     check box for IBM Cognos Release Notes.
   • If you want to start IBM Cognos Configuration now, select Start IBM
     Cognos Configuration.
     You can also start IBM Cognos Configuration using the IBM Cognos
     Configuration shortcut from the Start menu.
   • Click Finish.

What to do next

If you want users to see product documentation in a language other than English,
you must install the Supplementary Language Documentation component in the
location where you installed the Gateway components. For more information, see
“Installing translated product documentation” on page 59.

Installing fix packs

IBM provides interim maintenance packages that contain updates to one or more
components in your IBM Cognos product. If a fix pack is available when you are
installing or upgrading your product, you must install it after you install the IBM
Cognos components.

Fix packs are cumulative. When you install the latest fix pack, it includes updates
from all the previous fix packs. Fix packs are available for download from IBM

Note: Fix packs are not standalone installations. You must install them on
computers that have IBM Cognos components installed. Install the fix packs that
are appropriate for your product version. To check your version, open the
component list file at c10_location\cmplst.txt and check the line that starts with
C8PPCLIENT_version= for the PowerPlay Client and C8PPES_version= for the
PowerPlay server version.

Installing IBM Cognos fix packs on UNIX or Linux operating
systems

Fix packs are product updates that contain cumulative code fixes that were made
since the last release of the product. IBM Cognos fix packs are installed in the
same location as the existing product.
Procedure
1. Go to the location where the installation files are downloaded, or insert the disc if you have one.
2. To start the installation wizard, type the following command
   ./issetup
3. Follow the directions in the installation wizard to install the fix pack files to the same location as the existing IBM Cognos components.
4. If required, update the new installation files with any changes from the backup copies of your customized files.
   To prevent errors, before copying the customized files, compare both versions of the files. This validation determines whether you can replace the file.
5. If you have a distributed environment, repeat these steps for all remaining IBM Cognos servers.

Installing Fix Packs on Windows operating systems
Fix packs are product updates that contain cumulative code fixes that were made since the last release of the product. IBM Cognos fix packs are installed in the same location as the existing product.

Procedure
1. Insert the fix pack disk for the Windows operating system or go to the location where you downloaded and extracted the files, and double-click the issetup.exe file.
2. Follow the directions in the installation wizard to install the fix pack files to the same location as the existing IBM Cognos components.
3. If required, update the new installation files with any changes from the backup copies of your customized files.
   To prevent errors, before copying the customized files, compare both versions of the files. This validation determines whether you can replace the file.
4. If you have a distributed environment, repeat these steps for all remaining IBM Cognos servers.

Start IBM Cognos Configuration
Use IBM Cognos Configuration to configure IBM Cognos Business Intelligence components and to start and stop IBM Cognos services if you are using the default Tomcat servlet container.

Before you begin
Before starting IBM Cognos Configuration, ensure that the operating environment is properly set up. For example, ensure that all environment variables have been set.

On a Microsoft Windows operating system, you can start IBM Cognos Configuration in the last page of the installation wizard only if additional setup is not required. For example, if you use a database server other than Microsoft SQL or Cognos Content Database for the content store, copy the Java Database Connectivity (JDBC) drivers to the appropriate location before you start the configuration tool.

On UNIX or Linux operating systems, do not start IBM Cognos Configuration in the last page of the installation wizard. Additional setup is required before you can configure IBM Cognos BI. For example, you must update your Java environment.
Ensure that user or service account used to run IBM Cognos has been set up.

**Procedure**

1. On Microsoft Windows, click **Start > IBM Cognos Configuration**.
   - If you are using a Windows Vista, Windows 7, or Windows 2008 computer, and have installed the product to the **Program Files (x86)** directory, start IBM Cognos Configuration as an Administrator.

2. On UNIX or Linux operating systems, go to the **c10_location/bin64** directory and then type the following command:
   ```bash
   ./cogconfig.sh
   ```
   - If IBM Cognos Configuration does not open, ensure that you set the DISPLAY environment variable.
   - If you see a **JAVA.Lang.unsatisfied link** message, verify that you are using a supported version of Java.
   - If you see a **Java.lang.unsupportedClassVersionError** message, ensure that you are using a 64-bit version of Java.

**Configure Environment and Security Properties for Gateway Computers**

If you install the gateway component on a different computer than Content Manager or Application Tier Components, you must configure the gateway computer so that it knows the location of a dispatcher. A dispatcher is installed on every Content Manager and Application Tier Components computer. Configure the gateway to use the dispatcher on an Application Tier Components computer.

For failover protection, you can configure more than one dispatcher for a gateway computer. When multiple dispatchers are configured, requests are normally routed to the first dispatcher in the list. If this dispatcher becomes unavailable, the gateway determines the next functioning dispatcher on the list and routes requests there. The primary dispatcher status is monitored by the gateway, and requests are routed back to this component when it returns to service.

After you do the required configuration tasks, the gateway computer can work in your environment.

**Before you begin**

Ensure that the computers where you installed Content Manager are configured and the default active Content Manager computer is available before you configure gateway computers.

**Procedure**

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, under **Gateway Settings**, specify the values for **Dispatcher URIs for the gateway**:
   - Click in the value column.
   - Click the edit button.
   - Change the localhost portion of the URI to the name or IP address of an Application Tier Components computer.
   - This will ensure that users in different locations can connect to reports and workspaces that are sent by email.
Tip: If you want to send requests to the dispatcher from an Software Development Kit application or an IBM Cognos BI modeling tool that is outside of a network firewall, connect to a dedicated gateway that is configured to connect to the dispatcher using the internal dispatcher URI for your environment (for example, http://localhost:9300/p2pd/servlet/dispatch). For security reasons, the default setting for the Dispatcher URI for gateway property prevents the dispatcher from accepting requests for an Software Development Kit application or modeling tool that is outside the firewall. Ensure that you configure appropriate security for this dedicated gateway, such as SSL (see “Configuring the SSL protocol for IBM Cognos components” on page 210). Do not change your main gateway to use the internal dispatcher URI. Doing so will reduce the security of the IBM Cognos BI portal and studios.

- If you want to add another URI, click Add and change the localhost portion of the new URI to the name or IP address of another Application Tier Components computer.

Tip: If you want to use the dispatcher on a standby Content Manager computer, ensure that you add it after you add the Application Tier Components computers. If you add the dispatcher from the active Content Manager computer, ensure that it is last in the list.

- After you specify all the URIs, click OK.

4. In the Explorer window, under Security > Cryptography, click Cognos, the default cryptographic provider.

5. Under the Certificate Authority settings property group, set the Password property to match what you configured on the default active Content Manager computer.

6. Ensure that all other cryptographic settings match what you set on the default active Content Manager computer.

7. Test that the symmetric key can be retrieved. In the Explorer window, right-click Cryptography and click Test.

IBM Cognos BI components check the common symmetric keys (CSK) availability.

8. From the File menu, click Save.

Configuring the web server

You must configure your Web server before users can connect to the IBM Cognos BI portal.

For IBM Cognos BI for reporting, you must also set the content expiry for the images directory in your Web server so that the Web browser does not check image status after the first access.

On UNIX and Linux operating systems, the account under which the Web server runs must have read access to the cogstartup.xml file in the cl0_location/configuration directory. By default the cogstartup.xml file has read permission for others. If you run your Web server under a specific group, you can change the cogstartup.xml file permissions to ensure that it belongs to the same group as the Web server. You can then remove the read permission for others.

Use compiled gateways for production systems

For production systems, you can improve performance by changing the gateway from the default CGI gateway.
The compiled gateways include:

- Microsoft Internet Server Application Programming Interface (ISAPI) for Microsoft Internet Information Services (IIS)
- Apache module for Apache Web Server or IBM HTTP Server
- Servlet Gateway Java application if you use an application server other than the default Apache Tomcat

**Use Apache modules on Apache Server or IBM HTTP Server:**

You can use Apache modules for Apache Server 2.2.x or Apache Server 2.0.x or for IBM HTTP Server 8, 7, or 6.1.

**Important:** You cannot use the Apache modules with the version of Apache Server 2.2 that is supplied with Red Hat Enterprise Linux version 5.3 and later.

**Procedure**

1. Append the `c10_location/cgi-bin` directory to the appropriate environment variable:
   - On Solaris or Linux, LD_LIBRARY_PATH
   - On HP-UX, SHLIB_PATH and LD_LIBRARY_PATH
   - On AIX, LIBPATH
2. Go to the `Webserver_installation/conf` directory.
3. Open the `httpd.conf` file in an editor.
4. Ensure that both the server name and web server port number values are specified for the `ServerName` property.
5. Add the following to the end of the load module list:
   ```
   LoadModule cognos_module "c10_location/cgi-bin/mod2_2_cognos.suffix"
   Where suffix is as listed in the following table.
   ```

**Table 31. Module suffix for your operating system**

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Suffix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>dll</td>
</tr>
<tr>
<td>Solaris, AIX, HP-UX IA, Linux</td>
<td>so</td>
</tr>
</tbody>
</table>

Apache modules are provided for different versions of Apache Server or IBM HTTP Server:

- Use the `mod2_2_cognos` module for Apache Server 2.2.x or IBM HTTP Server 8 and 7.
- Use the `mod2_cognos` module for Apache Server 2.0.x and IBM HTTP Server 6.1.

6. Add the following:
   ```
   ScriptAlias /ibmcognos/cgi-bin "c10_location/cgi-bin"
   <Directory "c10_location/cgi-bin">
     AllowOverride None
     Options None
     Order allow,deny
     Allow from all
   </Directory>
   Alias /ibmcognos "c10_location/webcontent"
   <Directory "c10_location/webcontent">
   ```
Options Indexes MultiViews
AllowOverride None
Order allow,deny
Allow from all
</Directory>
The <Directory> directive is optional.

**Note:** Ensure that you define the /ibmcognos/cgi-bin alias before the /ibmcognos alias.

**Important:** ibmcognos is the default value that is used in the Gateway URI and Controller URI for gateway values in IBM Cognos Configuration. If you do not use ibmcognos for the ScriptAlias and Alias values, ensure that you change the Gateway URI and Controller URI for gateway values to match the values you use. Also, ensure that you use the same value for the ibmcognos part of the ScriptAlias and Alias values as shown in the examples.

7. Add the following to the server status reports section:

```
<Location /ibmcognos/cgi-bin/module_alias>
SetHandler cognos-handler
Order allow,deny
Allow from all
</Location>
```

Where *module_alias* is a name that you can choose.

8. To enable the gateway diagnostic page, add the following to the server status reports section:

```
<Location /ibmcognos/cgi-bin/diag_module_alias>
SetHandler cognos-handler
Order allow,deny
Allow from all
</Location>
```

Where *diag_module_alias* is a name that you can choose.

9. Add the following to the user directory section:

```
<IfModule mod2_2_cognos.c>
CGIBinDir "c10_location/cgi-bin"
</IfModule>
```

Apache module files are provided for different versions of Apache Server or IBM HTTP Server:

- Use mod2_2_cognos.c for Apache Server 2.2.x or IBM HTTP Server 8 and 7.
- Use mod2_cognos.c for Apache Server 2.0.x and IBM HTTP Server 6.1.

10. Save and close the file.

11. On HP-UX, enable searching for SHLIB_PATH by running the following command in the Apache_installation/bin directory:

```
chatr +s enable +b enable httpd
```

12. Restart the web server.


14. In the **Explorer** panel, click **Local Configuration > Environment**.

15. In the **Gateway URI** box, change the cognos.cgi part of the URI to *module_alias*.

    For example, http://host_name:port/ibmcognos/cgi-bin/module_alias.

16. Save your changes.
Results

Users can access the server by entering the Apache module URI in their browser. For example,

http://servername:port/ibmcognos/cgi-bin/module_alias.

Use the ISAPI gateway on Microsoft Internet Information Services (IIS) version 7 or 8:

If you are using a Microsoft Internet Information Services (IIS) web server, configure IBM Cognos to use the ISAPI gateway rather than the default CGI gateway.

About this task

If you are using Microsoft IIS as your web server and you plan to run more than one IBM Cognos BI product, or several instances of the same product, on one computer, you must create a separate application pool for each product or instance and then associate the aliases for that product or instance to the application pool.

For more information about creating an application pool, see your web server documentation.

Important: If you are using the 32-bit version of the ISAPI gateway, you must enable 32-bit application for the application pool that is used for the IBM Cognos gateway. In the Internet Information Services (IIS) Manager, select the application pool that is used for IBM Cognos, and click Advanced Settings. Change the value for Enable 32-Bit Applications to True.

Procedure

1. In the Microsoft Windows Control Panel, click Programs > Programs and Features.
   If you are using Microsoft Windows 8 or 2012 Server, Programs and Features is available directly from the Control Panel.
2. Click Turn Windows features on or off.
3. If you are using Microsoft Windows 2008 Server, use the following steps:
   a. Click Server Manager > Roles > Web Server (IIS).
   b. Ensure that Common HTTP Features, or the features you require are enabled.
   c. If ISAPI extensions is set to Not installed, select ISAPI extensions and click Add Role Service.
4. If you are using Microsoft Windows 2012 Server, use the following steps:
   a. In the Add Roles and Features Wizard, click Role-based or feature-based installation, and click Next.
   b. Select your server, and click Next.
   c. Select Web Server (IIS), if it is not already installed, ensure that Common HTTP Features is selected, and click Next until you get to the Role Services section of the wizard.
   d. Expand Application Development.
   e. Select ISAPI extensions if it is not already selected, and click Next.
   f. Click Install.
5. If you are using Microsoft Windows 7 or 8, use the following steps:
   a. Select **Internet Information Services** if it is not already selected.
   b. Expand **Internet Information Services > World Wide Web Services**.
   c. Ensure that **Common HTTP Features**, or the features you require are enabled.
   d. Expand **Application Development Features**.
   e. If **ISAPI extensions** is not selected, select **ISAPI extensions**.
   f. Click **OK**.

6. In the **Internet Information Services (IIS) Manager** console, under **Connections**, select your server name.
   - If you are using Microsoft Windows 2012 Server, in **Server Manager**, select **IIS**, and then right-click your server name, and click **Internet Information Services (IIS) Manager**.
   - If you are using Microsoft Windows 2008 Server, in **Server Manager**, expand **Roles > Web Server (IIS)**, and then click **Internet Information Services (IIS) Manager**.
   - If you are using Microsoft Windows 8, from the **Control Panel**, click **Administrative Tools** to access the **Internet Information Services (IIS) Manager** console.
   - If you are using Microsoft Windows 7, from the **Control Panel**, click **System and Security > Administrative Tools** to access the **Internet Information Services (IIS) Manager** console.

7. Expand **Sites**, and under your website, add the virtual directories as shown in the table:

   **Table 32. Required virtual directories**

<table>
<thead>
<tr>
<th>Alias</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibmcognos</td>
<td>c10_location/webcontent</td>
</tr>
<tr>
<td>ibmcognos/cgi-bin</td>
<td>c10_location/cgi-bin</td>
</tr>
</tbody>
</table>

   **Important:** `ibmcognos` is the default value that is used in the **Gateway URI** and **Controller URI for gateway** values in IBM Cognos Configuration. If you do not use `ibmcognos` for the Alias values, ensure that you change the **Gateway URI** and **Controller URI for gateway** values to match the values you use.

8. Select the cgi-bin virtual directory that you created.
9. Double-click **Handler Mappings**.
10. Under **Actions**, click **Add Module Mapping**.
    a. In **Request Path**, type `cognosisapi.dll`.
    b. In **Module**, select **IsapiModule**.
    c. In **Executable**, enter the path to the `cognosisapi.dll` file.
       For example, enter:
       ```
       C:\Program Files\ibm\cognos\c10\cgi-bin\cognosisapi.dll
       ```
    d. In **Name**, enter a name for the entry, such as **CognosISAPI**.
    e. Click **OK**.
    f. Click **Yes** in the dialog box to allow the ISAPI extension.

11. Start IBM Cognos Configuration.
12. In the **Explorer** panel, click **Local Configuration > Environment**.
13. In the **Gateway URI** box, change the **cognos.cgi** part of the URI to **cognosisapi.dll**.

**Results**

Users can access the ISAPI gateway by entering `http://servername/ibmcognos/isapi` in their web browsers.

**Configure the servlet gateway for an application server:**

If you deploy IBM Cognos to an application server other than Tomcat, you can use the servlet gateway to serve the portal pages rather than using a web server.

**Before you begin**

Ensure the following tasks are complete:

- The application server is installed and running on each computer where the servlet gateway is to be installed.
- IBM Cognos BI gateway components are installed on the same system as the application server.
- The IBM Cognos BI Application Tier Components and Content Manager are installed and running in the environment.
- The application server user account has full access permission for the IBM Cognos installation.

**About this task**

Instead of routing requests directly to the dispatcher, you deploy the servlet gateway to a different JVM instance than the JVM instances that run the IBM Cognos BI Application Tier Components and Content Manager servlets. Doing this type of deployment separates the load for serving static content from the main applications.

**Procedure**

1. **Create a separate JVM instance**, if necessary.  
   If you plan to run IBM Cognos BI and the IBM Cognos Servlet Gateway on the same application server, the servlet gateway must be deployed to a separate JVM instance.

2. **Check that IBM Cognos components are properly set up**

3. **Set environment variables**

4. **Configure IBM Cognos Servlet Gateway to run on the application server**

5. **Change the application server startup script**, if necessary.

6. **Configure application server properties and deploy IBM Cognos Servlet Gateway**

7. **Enable SSL**, if required.

**Results**

You can now access IBM Cognos components using the servlet gateway by entering the gateway URI. For example, `http[s]:host_name:port/ServletGateway`.

The IBM Cognos Servlet Gateway URI is case-sensitive.
Use CGI gateways

You can use the CGI gateway on IBM HTTP Server, Apache Web Server, or Microsoft Internet Information Services (IIS) Server.

Use the CGI gateway on Apache Server or IBM HTTP Server:

The default gateway configured in IBM Cognos Configuration is the CGI gateway. To use the CGI gateway, you must configure aliases for Apache Server or IBM HTTP Server.

Procedure
1. Go to the Webserver_installation/conf directory.
2. Open the httpd.conf file in an editor.
3. Ensure that both the server name and web server port number values are specified for the ServerName property.
4. Add the following:
   ```
   ScriptAlias /ibmcognos/cgi-bin "c10_location/cgi-bin"
   <Directory "c10_location/cgi-bin">
     AllowOverride None
     Options None
     Order allow,deny
     Allow from all
   </Directory>
   Alias /ibmcognos "c10_location/webcontent"
   <Directory "c10_location/webcontent">
     Options Indexes MultiViews
     AllowOverride None
     Order allow,deny
     Allow from all
   </Directory>
   ```
   The <Directory> directive is optional.

   Note: Ensure that you define the /ibmcognos/cgi-bin alias before the /ibmcognos alias.

   Important: ibmcognos is the default value that is used in the Gateway URI and Controller URI for gateway values in IBM Cognos Configuration. If you do not use ibmcognos for the ScriptAlias and Alias values, ensure that you change the Gateway URI and Controller URI for gateway values to match the values you use. Also, ensure that you use the same value for the ibmcognos part of the ScriptAlias and Alias values as shown in the examples.

5. Save and close the file.
6. Restart the web server.

Results

Users can access the portal at http://servername:port/ibmcognos.

Use the CGI gateway on Microsoft Internet Information Services (IIS) version 7 or 8:

If you are using Microsoft Internet Information Services (IIS) version 7 or later, use the following task to configure the CGI gateway.
The CGI gateway is provided for both 32-bit and 64-bit web servers.

About this task

If you are using Microsoft IIS as your web server and you plan to run more than one IBM Cognos BI product, or several instances of the same product, on one computer, you must create a separate application pool for each product or instance and then associate the aliases for that product or instance to the application pool.

For more information about creating an application pool, see your web server documentation.

Procedure

1. In the Microsoft Windows Control Panel, click Programs > Programs and Features.
   If you are using Microsoft Windows 8 or 2012 Server, Programs and Features is available directly from the Control Panel.
2. Click Turn Windows features on or off.
3. If you are using Microsoft Windows 2008 Server, use the following steps:
   a. Click Server Manager > Roles > Web Server (IIS).
   b. Ensure that Common HTTP Features, or the features you require are enabled.
   c. If CGI is set to Not installed, select CGI and click Add Role Service.
4. If you are using Microsoft Windows 2012 Server, use the following steps:
   a. In the Add Roles and Features Wizard, click Role-based or feature-based installation, and click Next.
   b. Select your server, and click Next.
   c. Select Web Server (IIS), if it is not already installed, ensure that Common HTTP Features is selected, and click Next until you get to the Role Services section of the wizard.
   d. Expand Application Development.
   e. Select CGI if it is not already selected, and click Next.
   f. Click Install.
5. If you are using Microsoft Windows 7 or 8, use the following steps:
   a. Select Internet Information Services if it is not already selected.
   b. Expand Internet Information Services > World Wide Web Services.
   c. Ensure that Common HTTP Features, or the features you require are enabled.
   d. Expand Application Development Features.
   e. If CGI is not selected, select CGI.
   f. Click OK.
6. In the Internet Information Services (IIS) Manager console, under Connections, select your server name.
   - If you are using Microsoft Windows 2012 Server, in Server Manager, select IIS, and then right-click your server name, and click Internet Information Services (IIS) Manager.
   - If you are using Microsoft Windows 2008 Server, in Server Manager, expand Roles > Web Server (IIS), and then click Internet Information Services (IIS) Manager.
If you are using Microsoft Windows 8, from the Control Panel, click Administrative Tools to access the Internet Information Services (IIS) Manager console.

If you are using Microsoft Windows 7, from the Control Panel, click System and Security > Administrative Tools to access the Internet Information Services (IIS) Manager console.

7. Double-click ISAPI and CGI Restrictions.
8. Under Actions, click Add.
9. Enter the path to the cognos.cgi file. The file is in the c10_location\cgi-bin directory.
   
   You must enter the full path, including the file name. If the path includes spaces, ensure you use quotation marks around the path. For example, enter: “C:\Program Files\ibm\cognos\c10\cgi-bin\cognos.cgi”
10. Enter a Description, such as CognosCGI.
11. Select Allow extension path to execute, and click OK.
12. Under Connections, expand Sites, and under your website, add the virtual directories as shown in the table:

   Table 33. Required virtual directories

<table>
<thead>
<tr>
<th>Alias</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibmcognos</td>
<td>c10_location/webcontent</td>
</tr>
<tr>
<td>ibmcognos/cgi-bin</td>
<td>c10_location/cgi-bin</td>
</tr>
</tbody>
</table>

13. Select the cgi-bin virtual directory that you created.
   a. In Request Path, type cognos.cgi.
   b. In Module, select CgiModule.
   c. Leave Executable (optional) blank.
   d. In Name, enter a name for the entry, such as CognosCGI.
   e. Click OK.

Results

Users can access the CGI gateway by entering http://servername/ibmcognos in their web browsers.

Use the CGI gateway on older versions of Microsoft IIS:

For versions of Microsoft Internet Information Services (IIS) earlier than version 7, use these steps to configure the CGI gateway.

Procedure

Create the virtual directories shown in the following table:

Table 34. Required virtual directories

<table>
<thead>
<tr>
<th>Alias</th>
<th>Location</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibmcognos</td>
<td>c10_location/webcontent</td>
<td>Read</td>
</tr>
<tr>
<td>ibmcognos/cgi-bin</td>
<td>c10_location/cgi-bin</td>
<td>Execute</td>
</tr>
</tbody>
</table>
**Important:** `ibmcognos` is the default value that is used in the Gateway URI and Controller URI for gateway values in IBM Cognos Configuration. If you do not use `ibmcognos` for the ScriptAlias and Alias values, ensure that you change the Gateway URI and Controller URI for gateway values to match the values you use.

**Configuring WebDAV to view and browse images**

To view and browse images in the Report Studio, configure Web Distributed Authoring and Versioning (WebDAV) on your web server. Report authors can browse for images to include in reports in a way that is similar to browsing a file system.

**Configuring WebDAV on Microsoft IIS web servers:**

On Microsoft Internet Information Services (IIS) web servers, you must first enable the WebDAV feature, and then configure your web server to access the image location.

**Procedure**

1. In the Microsoft Windows Control Panel, click Programs > Programs and Features.
   
   If you are using Microsoft Windows 8 or 2012 Server, Programs and Features is available directly from the Control Panel.

2. Click Turn Windows features on or off.

3. If you are using Microsoft Windows 2008 Server, use the following steps:
   
   a. Click Server Manager > Roles > Web Server (IIS).
   
   b. In the Role Services section, select Add Role Services.
   
   c. Under Web Server > Common HTTP Features, select WebDAV Publishing.
   
   d. Click Next, and then click Install.

4. If you are using Microsoft Windows 2012 Server, use the following steps:
   
   a. In the Add Roles and Features Wizard, click Role-based or feature-based installation, and click Next.
   
   b. Select your server, and click Next.
   
   
   d. Click Next > Next, and then click Install.

5. If you are using Microsoft Windows 7 or 8, use the following steps:
   
   a. Expand Internet Information Services > World Wide Web Services > Common HTTP Features.
   
   b. Select WebDAV Publishing, and click OK.

6. In the Internet Information Services (IIS) Manager console, under Connections, select your server name.
   
   - If you are using Microsoft Windows 2012 Server, in Server Manager, select IIS, and then right-click your server name, and click Internet Information Services (IIS) Manager.
   
   - If you are using Microsoft Windows 2008 Server, in Server Manager, expand Roles > Web Server (IIS), and then click Internet Information Services (IIS) Manager.
• If you are using Microsoft Windows 8, from the Control Panel, click Administrative Tools to access the Internet Information Services (IIS) Manager console.

• If you are using Microsoft Windows 7, from the Control Panel, click System and Security > Administrative Tools to access the Internet Information Services (IIS) Manager console.

7. Under Connections, expand your web server, Sites, and select your website. For example, select Default Web Site.


9. Click Enable WebDAV.

10. Click WebDAV Settings.

11. If you have anonymous access enabled, select True for Allow Anonymous Property Queries, and click Apply.

12. Select the directory or virtual directory to which you want to allow WebDAV access.


14. Click Add Authoring Rule, and add the appropriate rules for your environment. For example, if you installed the samples and you want to use the default path, under the ibmcognos virtual directory, expand samples, and select images, and add an authoring rule for the image files.

15. Right-click the directory or virtual directory you added authoring rules to, and click Edit Permissions.

16. Click Security, and add the appropriate permissions. For example, if you allow anonymous access to your web server, add permissions for the anonymous access user. You can find that user by select the website, double-clicking Authentication, and viewing the properties for the displayed users.

Results

With WebDAV enabled, Report Studio users can add images to their reports. When users click Browse in the image browser, the default location for browsing is http://servername/ibmcognos/samples/images. If you created another location, users can enter that location.

Test the Gateway

You can test the installation using a Web browser.

Procedure

1. Ensure that your Web server is running.

2. Open a Web browser.

3. In your address box, type the Gateway URI from IBM Cognos Configuration. For example,

   http://host_name:port/ibmcognos

   The Welcome page of the IBM Cognos BI portal appears.

Installing and Configuring Migration on IBM Cognos Series 7

Before you can use the Migration Assistant in IBM Cognos PowerPlay to migrate IBM Cognos Series 7 content from PowerPlay Enterprise Server, Upfront, or IBM Cognos Connection, you must install migration components on IBM Cognos Series
7 computers. The IBM Cognos Series 7 migration components are available on Microsoft Windows and UNIX, on the IBM Cognos PowerPlay Server CD.

Use the following checklist to guide you through the tasks to install and configure IBM Cognos Migration

- • Install IBM Cognos Series 7 migration components.
- • Configure the IBM Cognos Series 7 migration components, if required.
- • Start the IBM Cognos Series 7 migration service.

For information about migrating content from IBM Cognos Series 7 to IBM Cognos BI, including configuration recommendations for the migration process, see the IBM Cognos PowerPlay Migration and Administration Guide.

Install IBM Cognos Series 7 Migration Components

Ensure that your IBM Cognos Series 7 installations are working correctly before installing the IBM Cognos Series 7 migration components. This includes ensuring that the IBM Cognos Series 7 PowerPlay Enterprise Server service and the Upfront services, including the IBM Cognos Upfront Administration Service, IBM Cognos Upfront Data Store and the IBM Cognos Upfront Dispatcher services, are running.

You install IBM Cognos Series 7 migration components on the IBM Cognos Series 7 computers.

- To migrate content from a PowerPlay Enterprise Server you must install IBM Cognos Series 7 migration components on the PowerPlay Enterprise Server computer. If Upfront is located on the same computer you can also migrate content from Upfront. Installing migration components on the PowerPlay Enterprise Server computer also supports the migration of PowerPlay content that was published to Cognos Connection.
- To migrate content from Upfront you must install IBM Cognos Series 7 migration components on the Upfront computer. When Upfront and PowerPlay Enterprise Server are installed on separate computers, you must install IBM Cognos Series 7 migration components on the both the PowerPlay Enterprise Server computer and the Upfront computer. Also, you must set up and configure a shared network location to support migration processing.

Procedure

1. Insert the IBM Cognos PowerPlay Server CD that is appropriate for your operating system. On UNIX, you must mount the CD using Rock Ridge file extensions.
2. If the Welcome page does not appear, do one of the following:
   - On Windows, in the win32 directory on the CD, double-click the issetup.exe file.
   - On UNIX, in the directory that is appropriate for your operating system, type .isetup
3. Select the language to use for the installation.
   The language that you select determines the language of the installation wizard.
4. Follow the directions in the installation wizard.
5. On the Component Selection page, clear all components except IBM Cognos Series 7 Migration Components.
6. In the Multiple Installation Locations page, specify the IBM Cognos Series 7 location to install the components.
You must install IBM Cognos Series 7 migration components in the same directory as IBM Cognos Series 7 version 4 (7.4).

If you are installing the IBM Cognos Series 7 migration components on a Microsoft Windows computer, the installation location must be a physical drive and not a mapped drive. Otherwise, you will not be able to start the migration service.

If you are prompted for an IBM Cognos BI installation location, you can accept the default location or enter a new local location. This location is used to write install files. You do not have to enter the path to an IBM Cognos BI installation on a different computer and you do not require IBM Cognos BI components on the IBM Cognos Series 7 computer.

7. In the Migration Configuration Information page, for the Migration Service Port Number, type a port number that the IBM Cognos Series 7 migration service will use. The default is 21567.

8. In the Finish page, click Finish.

Results

Like other IBM Cognos products, the installation process creates log files that include information such as details about transferred files and installation errors. The log files are located in the installation_location\instlog directory.

Configuring the migration service in a distributed IBM Cognos Series 7 environment

If you installed IBM Cognos Series 7 migration components on both a PowerPlay Enterprise Server computer and a separate Upfront computer, you must set up and configure a shared network location. The migration service writes temporary files to this location during migration processing.

The following limitations apply for migration from Upfront when PowerPlay Enterprise Server and Upfront are on separate computers.

PowerPlay Enterprise Server and Upfront must access PowerCubes using the same path, such as \machine_name\cubes. If the cubes are located on the same computer as PowerPlay Enterprise Server, PowerPlay Enterprise Server will access the cubes using a local path and Upfront will access the cubes using a path that includes the PowerPlay Enterprise computer name. Migration from Upfront will not work in this situation.

Procedure

1. Create a folder in a shared network location that is accessible from both the PowerPlay Enterprise Server computer and the Upfront computer.

   Ensure that the services for PowerPlay Enterprise Server, Upfront, and IBM Cognos Series 7 migration run under named accounts that have write access to the folder.

2. Complete the following steps on each computer that includes IBM Cognos Series 7 migration components.
   - From the installation_location\mig7service, open the migs7service_configuration.xml file in an XML or text editor.
   - Edit the series7-shared-location description line to specify the network location and activate the line (remove comment tags). For example,
     <series7-shared-location description="Path to shared folder">\bott93\shareT\s7migration</series7-shared-location>
• Save and close the file.
3. Restart the IBM Series 7 migration service.

Results

The configuration to support migration from separate PowerPlay Enterprise Server and Upfront computers is complete.

**Start the IBM Cognos Series 7 Migration Service**

Before you can migrate content from IBM Cognos Series 7 PowerPlay to IBM Cognos PowerPlay, you must start the migration service for IBM Cognos Series 7. On Windows, the migration service for IBM Cognos Series 7 starts automatically when it is first installed.

**Procedure**

Start the migration service:

• On Windows, if the service is stopped, then restart the migration service using the **IBM Cognos Migration Series 7 Service** entry in the **Services** list under **Administrative Tools**.

• On UNIX, go to the `c10_location/migs7` directory and start the service by typing
  
  `.configure.sh --start`
Chapter 7. Installing the Cognos PowerPlay samples

To use the samples, install them from the IBM Cognos Business Intelligence Samples disc or from the location where you downloaded and extracted the files.

About this task

The samples include data sources, models, cubes, reports, and other types of content, to support all IBM Cognos Business Intelligence components.

Procedure

1. Insert the IBM Cognos samples disc or go to the location where the installation files were downloaded and extracted.
2. Double-click the isssetup.exe file.
   The Welcome page of the installation wizard appears.
3. Select the language to use for the installation.
4. Follow the directions in the installation wizard.
   Install the samples in a different directory than other IBM Cognos PowerPlay components.

What to do next

To set up the samples, you must create a data source connection and import the samples. After setting up the samples, you can use them to learn how to use the Cognos PowerPlay software.

Creating a data source connection to the PowerCube samples

IBM Cognos Business Intelligence PowerPlay uses data source connections to connect to the PowerCube samples and run sample reports or use sample packages. You must create a data source connection to IBM Cognos PowerCube to use the samples.

Procedure

1. Open IBM Cognos Administration by connecting to the IBM Cognos BI portal and clicking Administer IBM Cognos Content on the Welcome page.
2. Click the Configuration tab, and click Data Source Connections.
3. Click the new data source icon .
4. In the Name box, type great_outdoors_sales_en and then click Next. The name must be all lowercase and include the underscore characters.
5. In the connection page, select IBM Cognos Power Cube.
6. In the location box, type the path and file name for the great_outdoors_sales_en.mdc. For example, if you are creating a connection to samples installed to the default location on the local computer, type C:\Program Files\ibm\cognos\c10\webcontent\samples\datasources\cubes\PowerCubes\EN\great_outdoors_sales_en.mdc.
7. To confirm that you entered all parameters correctly, click Test the Connection.
8. On the Finish page, do not select Create a Package.
Importing the Cognos PowerPlay samples

To use the sample package and other content, you must import them from the sample deployment archive.

Before you begin

Before you import the content, ensure that you have created a data source connection to IBM Cognos PowerCube.

Procedure

1. Copy the IBM_Cognos_PowerPlay.zip file from the c10_location/webcontent/samples/content directory to the c10_location/deployment directory.
2. Connect to the IBM Cognos BI portal and on the Welcome page click **Administer IBM Cognos Content**.
3. On the Configuration tab, click **Content Administration**.
4. On the toolbar, click the **New Import** button.
5. In the Deployment Archive box select **IBM_Cognos_PowerPlay**.
6. Click **Next**.
7. In the Public Folders Content box, select the **Samples** folder.

Results

**IBM_Cognos_PowerPlay** appears in **Content Administration** and a **Samples** folder appears in **Public Folders** in IBM Cognos Connection.

Testing a sample report

To test that your samples were imported successfully, open a sample report in Cognos Viewer. Cognos Viewer is the default viewer when opening a report in IBM Cognos Connection.

Procedure

1. In IBM Cognos Administration, from the toolbar, click **Launch, IBM Cognos Connection**.
2. In the Public Folders list, open **Samples, PowerPlay**.
3. Click **great_outdoors_sales_en**.
4. Click any report in the list. The report opens in IBM Cognos Viewer.
Chapter 8. Configuring IBM Cognos Components to Use an Authentication Provider

IBM Cognos components run with two levels of logon: anonymous and authenticated. By default, anonymous access is enabled.

You can use both types of logon with your installation. If you choose to use authenticated logon only, you can disable anonymous access.

For authenticated logon, you must configure IBM Cognos components with an appropriate namespace for the type of authentication provider in your environment. You can configure multiple namespaces for authentication and then choose, at run time, which namespace you want to use. For more information, see the Administration and Security Guide.

IBM Cognos components support the following types of servers as authentication sources:
- IBM Cognos Series 7 namespace
- Active Directory Server
- Custom Authentication Provider
- LDAP
- CA SiteMinder
- RACF

If you use more than one Content Manager, you must configure identical authentication providers in each Content Manager location. This means that the type of authentication provider you select and the way you configure it must be identical in all locations for all platforms. The configuration must contain information that is accessible by all Content Managers.

When IBM Cognos is installed in a single Linux-based computer, or when Content Manager is installed on a Linux-based computer, IBM Cognos can be configured to use only LDAP V3-compliant directory servers and custom providers as authentication sources.

Some authentication providers require libraries external to the IBM Cognos environment to be available. If these libraries are not available on Linux, the authentication provider cannot be initialized.

If you want to configure one of the following as your authentication source, you must install Content Manager on a Microsoft Windows computer:
- IBM Cognos Series 7 namespace
- Active Directory Server

If you enable security, you must configure security settings immediately after you complete the installation and configuration process. For more information, see the Administration and Security Guide.

Important: Do not disable security after you enable it. If you delete a namespace, the user preferences, My Folders, and My Pages entries are permanently lost.
Existing permission settings will refer to users, groups, or roles that no longer exist. While this does not affect how the permissions work, a user administering the permission settings may see "unknown" entries. Because these entries refer to users, groups, and roles which no longer exist, you can safely delete them.

After you configure an authentication provider for IBM Cognos components, you can enable single signon between your authentication provider environment and IBM Cognos components. This means that a user logs on once and can then switch to another application without being asked to log on again.

Users can select namespaces when they log in to the IBM Cognos portal. You can hide Custom Java namespaces and CA SiteMinder namespaces from users. For more information, see "Hide the Namespace from Users During Login" on page 157.

To use an authentication provider and to require users to authenticate, do the following:

- Disable anonymous access if required.
- Configure IBM Cognos components to use an authentication provider.

### Disable Anonymous Access

If you want to use authenticated logon only, you can use IBM Cognos Configuration to disable anonymous access.

By default, IBM Cognos components do not require user authentication. Users can log on anonymously.

**Procedure**

1. In each location where Content Manager is installed, start IBM Cognos Configuration.
2. In the Explorer window, under Security > Authentication, click Cognos.
   The IBM Cognos resource represents the Cognos namespace. The Cognos namespace stores information about IBM Cognos groups, such as the Anonymous User, contacts, and distribution lists, and refers to objects in other security namespaces. For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.
3. In the Properties window, click the box next to the Allow anonymous access property and then select False.
4. From the File menu, click Save.

**Results**

Now, you must configure a namespace so that users are required to provide logon credentials when they access IBM Cognos resources.

### Restrict User Access to the Cognos Namespace

You can restrict access to users belonging to any group or role defined in the Cognos built-in namespace.

By default, all users belong to several built-in groups or roles. To restrict access, you must do the following:

- Enable the property to restrict access, using IBM Cognos Configuration.
• Remove the Everyone group from the built-in roles and groups, using IBM Cognos Administration.
• Ensure that authorized users belong to at least one role or group, using IBM Cognos Administration.

Procedure
1. In each Content Manager location, start IBM Cognos Configuration.
2. In the Explorer window, under Security, click Authentication.
3. In the Properties window, change the value of Restrict access to members of the built-in namespace to True.
4. From the File menu, click Save.

Results
You must now use the portal to remove the Everyone group from the built-in roles and groups, and then ensure that authorized users belong to at least one built-in role or group.

For information about adding or removing members of a group or role, see the IBM Cognos Business Intelligence Administration and Security Guide.

Configuring IBM Cognos Components to Use Active Directory Server

If you install Content Manager on a Microsoft Windows operating system computer, you can configure Active Directory as your authentication source using an Active Directory namespace.

If you install Content Manager on a UNIX-based computer, you must instead use an LDAP namespace to configure Active Directory as your authentication source. If you install Content Manager on a mix of Windows and UNIX computers, you must use an LDAP namespace to configure Active Directory for all Content Managers. When you use an LDAP namespace to authenticate against Active Directory Server, you are limited to LDAP features only. You do not have access to Active Directory features such as advanced properties for domains and single signon using Kerberos delegation.

If you install Content Manager on a Linux-based computer, the same restrictions apply as for UNIX. You must use an LDAP namespace to configure Active Directory as your authentication source.

If you want to use Microsoft SQL Server or Microsoft Analysis Server as a data source and use single signon for authentication, you must use Active Directory as your authentication source.

You cannot connect to the Active Directory Global Catalog, which is a caching server for Active Directory Server. If the connection uses port 3268, you must change it. By default, Active Directory Server uses port 389.

Procedure
1. Configure IBM Cognos components to use an Active Directory Server namespace
2. Enable secure communication to the Active Directory Server if required
3. Enable single signon between Active Directory and IBM Cognos components
Configure an Active Directory Namespace

You can use Active Directory Server as your authentication provider.

You also have the option of making custom user properties from the Active Directory Server available to IBM Cognos components.

Before you begin

For IBM Cognos to work properly with Active Directory Server, ensure that the Authenticated users group has Read privileges for the Active Directory folder where users are stored.

If you are configuring an Active Directory namespace to support single signon with a Microsoft SQL Server or Microsoft Analysis Server data source, ensure the following configuration:

- The IBM Cognos gateway is installed on an IIS Web server that is configured for Integrated Authentication on Microsoft Windows operating system.
- The gateway is assigned to the local intranet Web site in your Web browser.
- Content Manager is installed on a Windows 2000 or Windows 2003 server.
- Content Manager, Application Tier Components, IIS Web server, and the data source server (Microsoft SQL Server or Microsoft Analysis Server) belong to the Active Directory domain.
- The data source connection for Microsoft SQL Server or Microsoft Analysis Server is configured for **External Namespace** and that namespace must be the Active Directory namespace.

For more information about data sources, see the *IBM Cognos Business Intelligence Administration and Security Guide*.

Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the Explorer window, under Security, right-click **Authentication**, and then click **New resource** > **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the Type list, click the appropriate namespace and then click OK. The new authentication provider resource appears in the Explorer window, under the Authentication component.

5. In the Properties window, for the Namespace ID property, specify a unique identifier for the namespace.

6. Specify the values for all other required properties to ensure that IBM Cognos components can locate and use your existing authentication provider.

7. Specify the values for the Host and port property.
   To support Active Directory Server failover, you can specify the domain name instead of a specific domain controller. For example, use mydomain.com:389 instead of dc1.mydomain.com:389.

8. If you want to search for details when authentication fails, specify the user ID and password for the Binding credentials property.
   Use the credentials of an Active Directory Server user who has search and read privileges for that server.

9. From the File menu, click Save.

10. Test the connection to a new namespace. In the Explorer window, under Authentication, right-click the new authentication resource and click Test.

Results

IBM Cognos loads, initializes, and configures the provider libraries for the namespace.

Make Custom User Properties for Active Directory Available to IBM Cognos Components

You can use arbitrary user attributes from your Active Directory Server in IBM Cognos components. To configure this, you must add these attributes as custom properties for the Active Directory namespace.

The custom properties are available as session parameters through Framework Manager. For more information about session parameters, see the Framework Manager User Guide.

You can also use the custom properties inside command blocks to configure Oracle sessions and connections. You can use the command blocks can be used with Oracle light-weight connections and virtual private databases. For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.

Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.

2. In the Explorer window, under Security > Authentication, click the Active Directory namespace.

3. In the Properties window, click in the Value column for Custom properties and click the edit icon.

4. In the Value - Custom properties window, click Add.

5. Click the Name column and type the name you want IBM Cognos components to use for the session parameter.
6. Click the **Value** column and type the name of the account parameter in your Active Directory Server.

7. Repeat steps 4 to 6 for each custom parameter.

8. Click **OK**.

9. From the **File** menu, click **Save**.

**Enabling Secure Communication to the Active Directory Server**

If you are using an SSL connection to the Active Directory Server, you must copy the certificate from the Active Directory Server to the Content Manager location.

**Procedure**

1. In every Content Manager location, use your Web browser to connect to the Active Directory Server and copy the CA root certificate to the Content Manager location.

2. Add the CA root certificate to the certificate store of the account that you are using for the current IBM Cognos session:
   - If you are running the IBM Cognos session under a user account, use the same Web browser as in step 1 to import the CA root certificate to the certificate store for your user account.
     For information, see the documentation for your Web browser.
   - If you are running the IBM Cognos session under the local account, use Microsoft Management Console (MMC) to import the CA root certificate to the certificate store for the local computer.
     For information, see the documentation for MMC.

3. In IBM Cognos Configuration, restart the service:
   - In the **Explorer** window, click **IBM Cognos services, IBM Cognos**.
   - From the **Actions** menu, click **Restart**.

**Include or Exclude Domains Using Advanced Properties**

When you configure an authentication namespace for IBM Cognos, users from only one domain can log in. By using the Advanced properties for Active Directory Server, users from related (parent-child) domains and unrelated domain trees within the same forest can also log in.

If you set a parameter named chaseReferrals to true, users in the original authenticated domain and all child domains of the domain tree can log in to IBM Cognos. Users from a parent domain of the original authenticated domain or in a different domain tree cannot log in.

If you set a parameter named MultiDomainTrees to true, users in all domain trees in the forest can log in to IBM Cognos.

**Procedure**

1. In every location where you installed Content Manager, open IBM Cognos Configuration.

2. In the **Explorer** window, under **Security > Authentication**, click the Active Directory namespace.

3. In the **Properties** window, specify the **Host and port** property:
   - For users in one domain, specify the host and port of a domain controller for the single domain.
For users in one domain tree, specify the host and port of the top-level controller for the domain tree.

For users in all domain trees in the forest, specify the host and port of any domain controller in the forest.

4. Click in the Value column for Advanced properties and click the edit icon.
5. In the Value - Advanced properties window, click Add.
6. Specify two new properties, chaseReferrals and MultiDomainTrees, with the values from the following table:

Table 35. Advanced properties settings

<table>
<thead>
<tr>
<th>Authentication for</th>
<th>chaseReferrals</th>
<th>MultiDomainTrees</th>
</tr>
</thead>
<tbody>
<tr>
<td>One domain</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>One domain tree</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>All domain trees in the forest</td>
<td>True</td>
<td>True</td>
</tr>
</tbody>
</table>

7. Click OK.
8. From the File menu, click Save.

Related information:
“Configuring IBM Cognos Components to Use Active Directory Server” on page 143

If you install Content Manager on a Microsoft Windows operating system computer, you can configure Active Directory as your authentication source using an Active Directory namespace.

**Authenticating Domain Trees**

Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the Explorer window, under Security > Authentication, click the Active Directory namespace.
3. In the Properties window, specify the Host and port property:
   - For users in one domain, specify the host and port of a domain controller for the single domain.
   - For users in one domain tree, specify the host and port of the top-level controller for the domain tree.
   - For users in all domain trees in the forest, specify the host and port of any domain controller in the forest.
4. Click in the Value column for Advanced properties and click the edit icon.
5. In the Value - Advanced properties window, click Add.
6. Specify two new properties, chaseReferrals and MultiDomainTrees, with the values from the following table:

Table 36. Properties for setting authenticating domain trees

<table>
<thead>
<tr>
<th>Authentication for</th>
<th>chaseReferrals</th>
<th>MultiDomainTrees</th>
</tr>
</thead>
<tbody>
<tr>
<td>One domain</td>
<td>False</td>
<td>False</td>
</tr>
</tbody>
</table>

Chapter 8. Configuring IBM Cognos Components to Use an Authentication Provider  147
7. Click OK.
8. From the File menu, click Save.

**Enable single signon between Active Directory Server and IBM Cognos components**

By default, the Active Directory provider uses Kerberos authentication. It integrates with the IIS web server for single signon if Windows authentication (formerly named NT Challenge Response) is enabled on the IIS web server.

If Windows authentication is enabled, you are not prompted to reenter authentication information when you access IBM Cognos content that is secured by the Active Directory namespace.

If you use Kerberos authentication, you can choose to use Service for User (S4U). S4U allows users to access IBM Cognos BI from computers not on the Active Directory domain. To enable S4U, you must use enable constrained delegation.

For example, you have users whose computers do not belong to the domain, but they do have the domain account. When they open their web browsers, they are promoted for their domain account. However, they get the Kerberos ticket with Identity privilege only, which prevents them from getting authenticated to IBM Cognos BI. To resolve this issue, you can use S4U.

If you do not want Kerberos authentication, you can configure the provider to access the environment variable `REMOTE_USER` to achieve single signon.

**Important:** Ensure that you use only the variable `REMOTE_USER`. Using another variable can cause a security vulnerability.

To enable single signon to use Kerberos authentication, you must ensure that you complete the following tasks:
1. Set up Windows authentication on your IIS web server.
2. Install Content Manager on a computer that is part of the Active Directory domain, for the active and standby Content Managers.
3. Set up the computers, or the user account under which Content Manager runs, to be trusted.
If you install Content Manager on a Microsoft Windows operating system computer, you can configure Active Directory as your authentication source using an Active Directory namespace.

**Enabling single signon to use Kerberos authentication**

If your IIS web server is configured for Windows authentication, you do not have to add any additional settings. Kerberos authentication is used as the default.

**Enabling single signon to use Kerberos authentication with constrained delegation**

To be able to use constrained delegation, you must define the service principal names (SPN) for the users that are configured to run the IBM Cognos components and your Microsoft Internet Information Services (IIS) web server's application pool in your Active Directory domain.

If you use Kerberos with constrained delegation, you must add an `sAMAccountName` user for Content Manager when you configure your gateway. All active and stand by Content Managers must be configured to run under the same account.

If you are configuring single signon to your database servers, you must configure the `sAMAccountName` for the user who runs the Application Tier Components when you add the Active Directory namespace. All Application Tier Components must be configured to run under the same account.

The SPNs are the users that you enter in the `sAMAccountName` fields in IBM Cognos Configuration.

For example, assume that you have one user who runs the Content Manager component, another who runs the Application Tier Components, and another who runs your web server's application pool. The Content Manager user is `CognosCMUser`. The Application Tier Components user is `CognosATCUser`. The application pool user is `IISUser`. Each user is in the `MyDomain` domain.

1. You must set up IIS so that your `MyDomain\IISUser` is the application pool identity.
2. Run the `setspn` command for the computer where IIS is running.
   
   For example:
   ```
   setspn -A http/IISServerName MyDomain\IISUser
   setspn -A http/IISServerName.MyDomain.com MyDomain\IISUser
   ```
3. Run the `setspn` command for your IBM Cognos users.
   
   For example:
   ```
   setspn -A ibmcognosba/CognosCMUser MyDomain\CognosCMUser
   setspn -A ibmcognosba/CognosATCUser MyDomain\CognosATCUser
   ```
   
   In these commands, you must use `ibmcognosba` as shown in the examples. The user names and domains must match your environment.

   **Note:** In this example, the `sAMAccountName` users you must enter are `CognosCMUser` and `CognosATCUser`.
4. If you are configuring single signon to your Microsoft SQL Server or Microsoft SQL Server Analysis Services database server, you must set up the SPN for the database server. For more information, see your database server documentation.
5. Finally, you must configure the constrained delegation in the Active Directory Users and Computers administration tool. On the Delegation tab for all users (IISUser, CognosCMUser, and CognosATCUser), you must select Trust this user for delegation to specified services only and Use Kerberos only to use Kerberos with constrained delegation. Select Trust this user for delegation to specified services only and Use any authentication protocol if you are using the S4U Kerberos extension.

And then you must add the required SPNs. For example, add ibmcognosba as a service type. And add DomainController1 and DomainController2 as service type ldap.

If you are configuring single signon for the datasource, add the MSOLAPSvc3 or MSQLSVC service.

Procedure

1. On the computer where you installed Content Manager, open IBM Cognos Configuration.

2. In the Explorer window, under Security > Authentication, and select the Active Directory namespace.

3. Click in the Value column for Advanced properties and then click the edit icon.

4. In the Value - Advanced properties dialog box, click Add.

5. In the Name column, type singleSignonOption.

6. In the Value column, enter one of the following values:
   - Enter KerberosS4UAuthentication if you want to use Kerberos authentication first. If Kerberos fails, Service For User (S4U) authentication is attempted. If S4U fails, the user is prompted for credentials.
   - Enter S4UAuthentication if you want to use S4U authentication first. If S4U fails, the user is prompted for credentials.

7. In the Value - Advanced properties dialog box, click Add.

8. In the Name column, type trustedCredentialType.

9. In the Value column, enter one of the following values:
   - Enter CredentialForTC if you want to save the user's credentials as a trusted credential. For example, if you want to use the credentials to run scheduled jobs.
   - Enter $4UForTC if you want to save only the authenticated user name as a trusted credential. The user name is saved in UPN format, and scheduled jobs can be run with the UPN without requiring the user's password.

10. Click OK.

11. Click in the Value column for Application Tier Components sAMAccountName, and enter the sAMAccountName of the user who runs the Application Tier Components.

   **Important:** This value is required only if you are configuring single signon to your Microsoft SQL Server or Microsoft SQL Server Analysis Services database server. If you are not configuring single signon to the database server, do not change this value.

12. Click File > Save.

13. Restart the IBM Cognos service.

14. On the computer where you installed the Gateway components, open IBM Cognos Configuration.

15. In the Explorer window, click Environment.
16. Click in the Value column for Content Manager sAMAccountName, and enter the sAMAccountName of the user who runs Content Manager.

17. Click File > Save.

**Enabling single signon between Active Directory Server and IBM Cognos Components to use REMOTE_USER**

If you do not want Kerberos authentication, you can configure the provider to access the environment variable REMOTE_USER to achieve single signon.

You must set the advanced property singleSignOnOption to the value IdentityMapping. You must also specify bind credentials for the Active Directory namespace.

Microsoft IIS sets REMOTE_USER by default when you enable Windows authentication. If Kerberos authentication is not used, single signon to Microsoft OLAP (MSAS) data sources is not possible.

When you define the REMOTE_USER, you can also choose to save the REMOTE_USER as a trusted credential. Saving as a trusted credential means that scheduled jobs authenticate the REMOTE_USER with the Binding Credential privileges.

**Important:** Ensure that you use only the variable REMOTE_USER. Using another variable can cause a security vulnerability.

**Procedure**

1. On the computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the Explorer window, under Security > Authentication, and select the Active Directory namespace.
3. Click in the Value column for Advanced properties and then click the edit icon.
4. In the Value - Advanced properties dialog box, click Add.
5. In the Name column, type singleSignOnOption
6. In the Value column, type IdentityMapping.
7. If you want to save the REMOTE_USER as a trusted credential, in the Value - Advanced properties dialog box, click Add.
8. In the Name column, type trustedCredentialType.
9. In the Value column, type IdentityMappingForTC.
10. Click OK.
11. Click in the Value column for Binding credentials, and then click the edit icon.
12. In the Value - Binding credentials dialog box, specify a user ID and password and then click OK.

---

**Configuring IBM Cognos to Use IBM Cognos Series 7 Namespace**

You can configure IBM Cognos components to use an IBM Cognos Series 7 namespace as the authentication provider. Users will be authenticated based on the authentication and signon configuration of the IBM Cognos Series 7 namespace.

An IBM Cognos Series 7 namespace is required if you want to use IBM Cognos Series 7 PowerCubes and Transformer models in IBM Cognos Business Intelligence. You must configure the namespace before you load the Transformer models.
Note: You cannot use an IBM Cognos Series 7 Local Authentication Export (LAE) file for authentication with IBM Cognos components.

You can configure IBM Cognos components to use multiple IBM Cognos Series 7 authentication providers. All IBM Cognos Series 7 namespaces must use the same primary IBM Cognos Series 7 Ticket Server. Otherwise, you may receive errors or be prompted for authentication more than once. To maintain performance, also ensure that the ticket server is running.

If you change the configuration information stored in the directory server used for IBM Cognos Series 7, you must restart the IBM Cognos service before the changes take effect in the IBM Cognos installation.

A user must be in at least one Access Manager user class to log on to IBM Cognos components.

Procedure
1. Configure a Series 7 namespace
2. Enable secure communication to the directory server used by the IBM Cognos Series 7 namespace if required
3. Enable single signon between IBM Cognos Series 7 and IBM Cognos

Configure an IBM Cognos Series 7 Namespace
You can configure IBM Cognos to use one or more IBM Cognos Series 7 namespaces for authentication.

Procedure
1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the Explorer window, under Security, right-click Authentication, and then click New resource > Namespace.
3. In the Name box, type a name for your authentication namespace.
4. In the Type list, click the appropriate namespace and then click OK.
   The new authentication provider resource appears in the Explorer window, under the Authentication component.
5. In the Properties window, for the Namespace ID property, specify a unique identifier for the namespace.
6. Specify the values for all other required properties to ensure that IBM Cognos components can locate and use your existing authentication provider.
   If your IBM Cognos Series 7 namespace version is 16.0, ensure that the Data encoding property is set to UTF-8. In addition, the locations where Content Manager is installed must use the same locale as the data in the IBM Cognos Series 7 namespace.
   The host value can be a server name or an IP address. If you are publishing from PowerPlay Enterprise Server to IBM Cognos BI, you must use the same value format used in IBM Cognos Series 7 Configuration Manager for the location of the directory server. For example, if the server name is used in IBM Cognos Series 7 Configuration Manager, you must also use the server name in IBM Cognos Configuration for IBM Cognos BI.
7. If your namespace environment includes version 15.2 of the IBM Cognos Series 7 namespace, you must disable the Series7NamespacesAreUnicode setting.
In the Properties window, in the Advanced Properties value, click the edit icon.

In the Value - Advanced properties window, click Add.

In the Name box, type Series7NamespacesAreUnicode.

In the Value box, type False, and then click OK.

8. In the Properties window, under Cookie settings, ensure that the Path, Domain, and Secure flag enabled properties match the settings configured for IBM Cognos Series 7.

9. From the File menu, click Save.

10. Test the connection to a new namespace. In the Explorer window, under Authentication, right-click the new authentication resource and click Test.

### Enabling Secure Communication to the Directory Server Used by the IBM Cognos Series 7 Namespace

If you are using an SSL connection to the Directory Server used by the IBM Cognos Series 7 namespace, you must copy the certificate from the Directory Server to each Content Manager location.

For more information, see the IBM Cognos Access Manager Administrator Guide and the documentation for your Directory Server.

### Enabling Single Signon Between IBM Cognos Series 7 and IBM Cognos

If your IBM Cognos Series 7 namespace has been configured for integration with your external authentication mechanisms for single signon, the IBM Cognos Series 7 provider will automatically use this configuration.

By configuring single signon, you are not prompted to reenter authentication information when accessing IBM Cognos content that is secured by the IBM Cognos Series 7 namespace.

**Procedure**

1. Ensure that you configured IBM Cognos components to use an IBM Cognos Series 7 namespace as an authentication provider.
2. For IBM Cognos Series 7, start Configuration Manager.
3. Click Open the current configuration.
5. In the Properties window, ensure that the Path, Domain, and Secure Flag Enabled properties match the settings configured for IBM Cognos BI.
6. Save and close Configuration Manager.
7. If the IBM Cognos Series 7 namespace uses the Trusted Signon plug-in for single signon, you must now define the SaferAPIGetTrustedSignonWithEnv function.

**Results**

You can now add IBM Cognos Upfront Series 7 NewsBoxes to your IBM Cognos Connection portal pages.
IBM Cognos Series 7 Namespaces and the IBM Cognos Series 7 Trusted Signon Plug-in

If the IBM Cognos Series 7 namespace uses the Trusted Signon plug-in for single signon, you must define the SaferAPIGetTrustedSignonWithEnv function in your plug-in. Then you must recompile and redeploy the library for single signon to be achieved between IBM Cognos components and your authentication mechanism.

The SaferAPIGetTrustedSignonWithEnv function is an updated version of the SaferAPIGetTrustedSignon function. This update is required because IBM Cognos logon is not performed at the Web server as is the case for IBM Cognos Series 7 applications. Therefore, it is not possible for the plug-in to perform a getenv() API call to retrieve Web server environment variables. The plug-in can request that specific environment variables be removed from the Web server using the SaferAPIGetTrustedSignonWithEnv function.

If you are running both IBM Cognos Series 7 and IBM Cognos products using the same plug-in, both the SaferAPIGetTrustedSignonWithEnv and SaferAPIGetTrustedSignon functions are required. For information about the SaferAPIGetTrustedSignon function, see the IBM Cognos Series 7 documentation.

**SaferAPIGetTrustedSignonWithEnv Function**

For users to be successfully authenticated by Access Manager, OS signons must exist and be enabled in the current namespace.

The memory for the returned trustedSignonName and trustedDomainName is allocated internally in this API. If the function returns SAFER_SUCCESS, Access Manager calls SaferAPIFreeTrustedSignon to free the memory allocated.

The memory for the returned reqEnvVarList is allocated internally in this API. If the function returns SAFER_INFO_REQUIRED, Access Manager calls SaferAPIFreeBuffer() to free the memory allocated.

You must implement both the SaferAPIGetTrustedSignon and SaferAPIFreeBuffer functions to successfully register the library when SaferAPIGetTrustedSignonWithEnv is implemented. The function SaferAPIGetError is required only if you want specific error messages returned from your plug-in.

**Syntax**

```c
SaferAPIGetTrustedSignonWithEnv(
    EnvVar envVar[],        /*[IN]*/
    char **reqEnvVarList,   /*[OUT]*/
    void **trustedSignonName, /*[OUT]*/
    unsigned long *trustedSignonNameLength, /*[OUT]*/
    void **trustedDomainName, /*[OUT]*/
    unsigned long *trustedDomainNameLength, /*[OUT]*/
    SAFER_USER_TYPE *userType, /*[OUT]*/
    void **implementerData); /*[IN/OUT]*/
```
### Parameters for the SaferAPIGetTrustedSignonWithEnv Function

**Table 37. Parameters and description for the SaferAPIGetTrustedSignonWithEnv Function**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[in] envVar</strong></td>
<td>An array of environment variable names and values that were retrieved from the Web server. The end of the array is represented by an entry with a null envVarName and a null envVarValue. Note that the first time this API is called, the envVar array contains only the end of array marker.</td>
</tr>
<tr>
<td><strong>[in] reqEnvVarList</strong></td>
<td>A string that contains a comma-separated list of environment variable names that are requested by the Safer implementation. The end of the list must be null-terminated.</td>
</tr>
<tr>
<td><strong>[out] trustedSignonName</strong></td>
<td>A sequence of bytes that identifies the currently authenticated user. This value does not need to be null-terminated. This value is mandatory.</td>
</tr>
<tr>
<td><strong>[out] trustedSignonNameLength</strong></td>
<td>An integer value that indicates the length of the trustedSignonName. This length should exclude the null terminator, if there is one. This value is mandatory.</td>
</tr>
<tr>
<td><strong>[out] trustedDomainName</strong></td>
<td>A sequence of bytes that identifies the domain of the currently authenticated user. You do not need to null-terminate this value. If there is no trustedDomainName, the return is null. This value is optional.</td>
</tr>
<tr>
<td><strong>[out] trustedDomainNameLength</strong></td>
<td>An integer value that indicates the length of the trustedDomainName. This length should exclude the null terminator, if there is one. This value is mandatory and must be set to zero if there is no trustedDomainName.</td>
</tr>
<tr>
<td><strong>[out] userType</strong></td>
<td>A value that indicates the type of user that Access Manager will authenticate. This value is mandatory. The following return values are required for Access Manager to successfully authenticate users:</td>
</tr>
<tr>
<td><strong>SAFER_NORMAL_USER</strong></td>
<td>A named user. OS signons must exist and be enabled in the current namespace.</td>
</tr>
<tr>
<td><strong>SAFER_GUEST_USER</strong></td>
<td>A guest user. A guest user account must exist and be enabled in the current namespace.</td>
</tr>
<tr>
<td><strong>SAFER_ANONYMOUS_USER</strong></td>
<td>An anonymous user. An anonymous user account must exist and be enabled in the current namespace.</td>
</tr>
<tr>
<td><strong>[in/out] implementerData</strong></td>
<td>A pointer used to preserve implementation-specific data between invocations. An invocation occurs every time Access Manager calls the trusted signon plug-in. This value is valid only if the trusted signon plug-in was invoked and you set a value for it.</td>
</tr>
</tbody>
</table>
Configuring IBM Cognos to Use a Custom Authentication Provider

If you implemented a custom Java authentication provider with your existing security infrastructure, you can configure IBM Cognos components to use it.

You can use a custom authentication provider to access and authenticate users to an alternate authentication source. You can also use it as a single signon mechanism to integrate IBM Cognos components with your security infrastructure. You can hide the namespace from users during logon.

For more information, see the Custom Authentication Provider Developer Guide.

Configure a Custom Authentication Namespace

You can configure IBM Cognos components to use a custom authentication namespace. Any additional configuration for authentication source access, single signon, or custom attributes are dependent on the custom authentication provider implementation.

Ensure that the versions of Java runtime environment (JRE) and Java Software Development Kit that you use are compatible with each other. If you use supported versions of the JRE and Java Software Development Kit that are not compatible with each other, then the custom Java authentication provider that you configure will not appear in the list of namespaces in IBM Cognos Configuration.

Procedure

1. In every location where Content Manager is installed, open IBM Cognos Configuration.
2. In the Explorer window, under Security, right-click Authentication, and click New resource > Namespace.
3. In the Name box, type a name for your authentication namespace.
4. In the Type list, select Custom Java Provider and then click OK.
   The new authentication provider resource appears in the Explorer window, under the Authentication component.
5. In the Properties window, for the NamespaceID property, specify a unique identifier for the namespace.
   Tip: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that IBM Cognos can locate and use your existing authentication provider.
7. From the File menu, click Save.
8. Test the connection to a new namespace. In the Explorer window, under Authentication, right-click the new authentication resource and click Test.

Results

IBM Cognos loads, initializes, and configures the provider libraries for the namespace.
**Hide the Namespace from Users During Login**

You can hide namespaces from users during login. You can have trusted signon namespaces without showing them on the namespace selection list that is presented when users log in.

For example, you may want to integrate single signon across systems but maintain the ability for customers to authenticate directly to IBM Cognos without being prompted to choose a namespace.

**Procedure**

1. In each location where you configured a custom Java authentication provider, open IBM Cognos Configuration.
2. In the Explorer window, under Security > Authentication, click the custom Java authentication provider.
3. In the Properties window, click the box next to Selectable for authentication and select False.
4. From the File menu, click Save.

**Results**

The namespace is not shown on the selection list that is presented at login.

---

**Configuring IBM Cognos Components to Use LDAP**

You can configure IBM Cognos components to use an LDAP namespace as the authentication provider. You can use an LDAP namespace for users that are stored in an LDAP user directory, Active Directory Server, IBM Directory Server, Novell Directory Server, or Oracle Directory Server.

You can also use LDAP authentication with DB2 and Essbase OLAP data sources by specifying the LDAP namespace when you set up the data source connection. For more information, see the *IBM Cognos Business Intelligence Administration and Security Guide*.

You also have the option of making custom user properties from the LDAP namespace available to IBM Cognos components.

If you want to bind users to the LDAP server, see "LDAP Mapping."

**Procedure**

1. "Configure an LDAP Namespace” on page 158
2. Make custom user properties available to IBM Cognos components if required
3. Enable secure communication to the LDAP server if required
4. Enable single signon between LDAP and IBM Cognos components if required

**LDAP Mapping**

To bind a user to the LDAP server, the LDAP authentication provider must construct the distinguished name (DN). If the Use external identity property is set to True, it uses the External identity mapping property to try to resolve the user’s DN. If it cannot find the environment variable or the DN in the LDAP server, it attempts to use the User lookup property to construct the DN.
If users are stored hierarchically within the directory server, you can configure the User lookup and External identity mapping properties to use search filters. When the LDAP authentication provider performs these searches, it uses the filters you specify for the User lookup and External identity mapping properties. It also binds to the directory server using the value you specify for the Bind user DN and password property or using anonymous if no value is specified.

When an LDAP namespace has been configured to use the External identity mapping property for authentication, the LDAP provider binds to the directory server using the Bind user DN and password or using anonymous if no value is specified. All users who log on to IBM Cognos using external identity mapping see the same users, groups, and folders as the Bind user.

If you do not use external identity mapping, you can specify whether to use bind credentials to search the LDAP directory server by configuring the Use bind credentials for search property. When the property is enabled, searches are performed using the bind user credentials or using anonymous if no value is specified. When the property is disabled, which is the default setting, searches are performed using the credentials of the logged-on user. The benefit of using bind credentials is that instead of changing administrative rights for multiple users, you can change the administrative rights for the bind user only.

Note that if you use a DN syntax, such as uid=$[userID], ou=mycompany.com, for the properties User lookup, External identity mapping, or Bind user DN and password, you must escape all special characters that are used in the DN. If you use a search syntax, such as (uid=$[userID]), for the properties User lookup or External identity mapping, you must not escape special characters that are used in the DN.

**Configure an LDAP Namespace**

You can configure IBM Cognos components to use an LDAP namespace when the users are stored in an LDAP user directory. The LDAP user directory may be accessed from within another server environment, such as Active Directory Server or CA SiteMinder.

If you are configuring an LDAP namespace for a directory server other than LDAP, see the appropriate section:

- For Active Directory Server, see Configure an LDAP Namespace for Active Directory Server
- For IBM Directory Server, see Configure an LDAP Namespace for IBM Directory Server
- For Novell Directory Server, see Configure an LDAP Namespace for Novell Directory Server
- For Oracle Directory Server, see Configure an LDAP Namespace for Oracle Directory Server

You can also use LDAP authentication with DB2 and Essbase OLAP data sources by specifying the LDAP namespace when you set up the data source connection. For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.

**Procedure**

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the Explorer window, under Security, right-click Authentication, and then click New resource > Namespace.

3. In the Name box, type a name for your authentication namespace.

4. In the Type list, click the appropriate namespace and then click OK.
   The new authentication provider resource appears in the Explorer window, under the Authentication component.

5. In the Properties window, for the Namespace ID property, specify a unique identifier for the namespace.

6. Specify the values for all other required properties to ensure that IBM Cognos components can locate and use your existing authentication provider.

7. If you want the LDAP authentication provider to bind to the directory server using a specific Bind user DN and password when performing searches, then specify these values.
   If no values are specified, the LDAP authentication provider binds as anonymous.
   If external identity mapping is enabled, Bind user DN and password are used for all LDAP access. If external identity mapping is not enabled, Bind user DN and password are used only when a search filter is specified for the User lookup property. In that case, when the user DN is established, subsequent requests to the LDAP server are executed under the authentication context of the end user.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following:
   • Ensure that Use external identity is set to False.
   • Set Use bind credentials for search to True.
   • Specify the user ID and password for Bind user DN and password.
   If you do not specify a user ID and password, and anonymous access is enabled, the search is done using anonymous.

9. Check the mapping settings for required objects and attributes.
   Depending on the LDAP configuration, you may have to change some default values to ensure successful communication between IBM Cognos components and the LDAP server.
   LDAP attributes that are mapped to the Name property in Folder mappings, Group mappings, and Account mappings must be accessible to all authenticated users. In addition, the Name property must not be blank.

10. From the File menu, click Save.

11. Test the connection to a new namespace. In the Explorer window, under Authentication, right-click the new authentication resource and click Test.

**Results**

IBM Cognos loads, initializes, and configures the provider libraries for the namespace.

**Configure an LDAP namespace for Active Directory Server**

If you configure a new LDAP namespace for use with an Active Directory Server, you must modify the necessary settings and change the values for all properties of the Active Directory objects.
Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the Explorer window, under Security, right-click Authentication, and then click New resource > Namespace.
3. In the Name box, type a name for your authentication namespace.
4. In the Type list, click the appropriate namespace and then click OK.
   The new authentication provider resource appears in the Explorer window, under the Authentication component.
5. In the Properties window, for the NamespaceID property, specify a unique identifier for the namespace.
   Tip: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that IBM Cognos components can locate and use your existing authentication provider.
   The following settings are examples:
   • For User lookup, enter (sAMAccountName=${userID})
   • If you use single signon, for Use external identity, set the value to True.
   • If you use single signon, for External identity mapping, enter (sAMAccountName=${environment("REMOTE_USER")})
     If you want to remove the domain name from the REMOTE_USER variable, enter (sAMAccountName=${replace(${environment("REMOTE_USER")}, "domain\", ",")}).
     Important: Ensure that you use only the variable REMOTE_USER. Using another variable can cause a security vulnerability.
   • For Bind user DN and password, enter user@domain.
   • For Unique identifier, enter objectGUID
7. If you want the LDAP authentication provider to bind to the directory server using a specific Bind user DN and password when performing searches, then specify these values.
   If no values are specified, the LDAP authentication provider binds as anonymous.
8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following steps:
   • Ensure that Use external identity is set to False.
   • Set Use bind credentials for search to True.
   • Specify the user ID and password for Bind user DN and password.
9. To configure the LDAP advanced mapping properties for use with the Active Directory Server objects, use the values that are specified in the following table.

<table>
<thead>
<tr>
<th>Mappings</th>
<th>LDAP property</th>
<th>LDAP value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Object class</td>
<td>organizationalUnit,organization,container</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>ou, o, cn</td>
</tr>
<tr>
<td>Group</td>
<td>Object class</td>
<td>group</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
</tbody>
</table>
Table 38. LDAP advanced mapping values for use with Active Directory Server objects (continued)

<table>
<thead>
<tr>
<th>Mappings</th>
<th>LDAP property</th>
<th>LDAP value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>member</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>cn</td>
<td></td>
</tr>
<tr>
<td>Account</td>
<td>Object class</td>
<td>user</td>
</tr>
<tr>
<td>Business phone</td>
<td>telephonenumber</td>
<td></td>
</tr>
<tr>
<td>Content locale</td>
<td>(leave blank)</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>description</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>mail</td>
<td></td>
</tr>
<tr>
<td>Fax/Phone</td>
<td>facsimiletelephonenumber</td>
<td></td>
</tr>
<tr>
<td>Given name</td>
<td>givenname</td>
<td></td>
</tr>
<tr>
<td>Home phone</td>
<td>homephone</td>
<td></td>
</tr>
<tr>
<td>Mobile phone</td>
<td>mobile</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>displayName</td>
<td></td>
</tr>
<tr>
<td>Pager phone</td>
<td>pager</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>unicodePwd</td>
<td></td>
</tr>
<tr>
<td>Postal address</td>
<td>postaladdress</td>
<td></td>
</tr>
<tr>
<td>Product locale</td>
<td>(leave blank)</td>
<td></td>
</tr>
<tr>
<td>Surname</td>
<td>sn</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>sAMAccountName</td>
<td></td>
</tr>
</tbody>
</table>

These mapping properties represent changes that are based on a default Active Directory Server installation. If you have modified the schema, you may have to make additional mapping changes.

LDAP attributes that are mapped to the **Name** property in **Folder mappings**, **Group mappings**, and **Account mappings** must be accessible to all authenticated users. In addition, the **Name** property must not be blank.

10. From the **File** menu, click **Save**.
11. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

Results

IBM Cognos loads, initializes, and configures the provider libraries for the namespace.

**Related information:**

“Configuring IBM Cognos Components to Use Active Directory Server” on page 143

If you install Content Manager on a Microsoft Windows operating system computer, you can configure Active Directory as your authentication source using an Active Directory namespace.

**Configure an LDAP Namespace for IBM Directory Server**

If you configure a new LDAP namespace for use with an IBM Directory Server, you must modify the necessary settings and change the values for all properties of the IBM Directory objects.
**Procedure**

1. In each location where you installed Content Manager, open IBM Cognos Configuration.
2. In the *Explorer* window, under *Security*, right-click *Authentication*, and then click **New resource > Namespace**.
3. In the *Name* box, type a name for your authentication namespace.
4. In the *Type* list, click *LDAP*, and then click **OK**.
   The new authentication namespace resource appears in the *Explorer* window, under the *Authentication* component.
5. In the *Properties* window, for the *NamespaceID* property, specify a unique identifier for the namespace.
   
   **Tip:** Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that IBM Cognos can locate and use your existing authentication namespace.
   
   - For *User lookup*, specify *(cn=${userID})*
   - For *Bind user DN and password*, specify *cn=root*
7. If you want the LDAP authentication provider to bind to the directory server using a specific *Bind user DN and password* when performing searches, then specify these values.
   If no values are specified, the LDAP authentication namespace binds as anonymous.
8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following:
   
   - Ensure that *Use external identity* is set to *False*.
   - Set *Use bind credentials for search* to *True*.
   - Specify the user ID and password for *Bind user DN and password*.
9. To configure the LDAP advanced mapping properties for use with IBM Directory Server objects, use the values specified in the following table.

*Table 39. LDAP advanced mapping values for use with IBM Directory Server objects*

<table>
<thead>
<tr>
<th>Mappings</th>
<th>LDAP property</th>
<th>LDAP value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Object class</td>
<td>organizationalunit,organization,container</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>ou,o,cn</td>
</tr>
<tr>
<td>Group</td>
<td>Object class</td>
<td>groupofnames</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Member</td>
<td>member</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>cn</td>
</tr>
<tr>
<td>Account</td>
<td>Object class</td>
<td>inetorgperson</td>
</tr>
<tr>
<td></td>
<td>Business phone</td>
<td>telephonenumber</td>
</tr>
</tbody>
</table>
Table 39. LDAP advanced mapping values for use with IBM Directory Server objects (continued)

<table>
<thead>
<tr>
<th>Mappings</th>
<th>LDAP property</th>
<th>LDAP value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Content locale</td>
<td>(leave blank)</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Email</td>
<td>mail</td>
</tr>
<tr>
<td></td>
<td>Fax/Phone</td>
<td>facsimiletelephonenumber</td>
</tr>
<tr>
<td></td>
<td>Given name</td>
<td>givenname</td>
</tr>
<tr>
<td></td>
<td>Home phone</td>
<td>homephone</td>
</tr>
<tr>
<td></td>
<td>Mobile phone</td>
<td>mobile</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>cn</td>
</tr>
<tr>
<td></td>
<td>Pager phone</td>
<td>pager</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>userPassword</td>
</tr>
<tr>
<td></td>
<td>Postal address</td>
<td>postaladdress</td>
</tr>
<tr>
<td></td>
<td>Product locale</td>
<td>(leave blank)</td>
</tr>
<tr>
<td></td>
<td>Surname</td>
<td>sn</td>
</tr>
<tr>
<td></td>
<td>Username</td>
<td>uid</td>
</tr>
</tbody>
</table>

These mapping properties represent changes based on a default IBM Directory Server installation. If you have modified the schema, you may have to make additional mapping changes.

LDAP attributes that are mapped to the Name property in Folder mappings, Group mappings, and Account mappings must be accessible to all authenticated users. In addition, the Name property must not be blank.

10. From the File menu, click Save.

**Configure an LDAP Namespace for Novell Directory Server**

If you configure a new LDAP namespace for use with a Novell Directory Server, you must modify the necessary settings and change the values for all properties of the Novell Directory objects.

**Procedure**

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the Explorer window, under Security, right-click Authentication, and then click New resource > Namespace.
3. In the Name box, type a name for your authentication namespace.
4. In the **Type** list, click **LDAP** and then click **OK**.
   The new authentication namespace resource appears in the **Explorer** window, under the **Authentication** component.

5. 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.

6. Specify the values for all other required properties to ensure that IBM Cognos can locate and use your existing authentication namespace.
   - For **User lookup**, specify (cn=${userID})
   - For **Bind user DN and password**, specify the base DN for an administration user, such as cn=Admin,0=COGNOS

7. If you want the LDAP authentication provider to bind to the directory server using a specific **Bind user DN and password** when performing searches, then specify these values.
   If no values are specified, the LDAP authentication namespace binds as anonymous.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following:
   - Ensure that **Use external identity** is set to **False**.
   - Set **Use bind credentials for search** to **True**.
   - Specify the user ID and password for **Bind user DN and password**.

9. To configure the LDAP advanced mapping properties for use with Novell Directory Server objects, use the values specified in the following table.

   **Table 40. LDAP advanced mapping values for use with Novell Directory Server objects**

<table>
<thead>
<tr>
<th>Mappings</th>
<th>LDAP property</th>
<th>LDAP value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Object class</td>
<td>organizationalUnit,organization,container</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>ou,o,cn</td>
</tr>
<tr>
<td>Group</td>
<td>Object class</td>
<td>groupOfNames</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Member</td>
<td>member</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>cn</td>
</tr>
<tr>
<td>Account</td>
<td>Object class</td>
<td>inetOrgPerson</td>
</tr>
<tr>
<td></td>
<td>Business phone</td>
<td>telephonenumber</td>
</tr>
<tr>
<td></td>
<td>Content locale</td>
<td>Language</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Email</td>
<td>mail</td>
</tr>
</tbody>
</table>
Table 40. LDAP advanced mapping values for use with Novell Directory Server objects (continued)

<table>
<thead>
<tr>
<th>Mappings</th>
<th>LDAP property</th>
<th>LDAP value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fax/Phone</td>
<td>facsimiletelephonenumber</td>
<td></td>
</tr>
<tr>
<td>Given name</td>
<td>givenname</td>
<td></td>
</tr>
<tr>
<td>Home phone</td>
<td>homephone</td>
<td></td>
</tr>
<tr>
<td>Mobile phone</td>
<td>mobile</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>cn</td>
<td></td>
</tr>
<tr>
<td>Pager phone</td>
<td>pager</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>(leave blank)</td>
<td></td>
</tr>
<tr>
<td>Postal address</td>
<td>postaladdress</td>
<td></td>
</tr>
<tr>
<td>Product locale</td>
<td>Language</td>
<td></td>
</tr>
<tr>
<td>Surname</td>
<td>sn</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>uid</td>
<td></td>
</tr>
</tbody>
</table>

These mapping properties represent changes based on a default Novell Directory Server installation. If you have modified the schema, you may have to make additional mapping changes.

LDAP attributes that are mapped to the Name property in Folder mappings, Group mappings, and Account mappings must be accessible to all authenticated users. In addition, the Name property must not be blank.

For users to successfully log in to IBM Cognos Connection, they must have permission to read the ou and o attributes.

10. From the File menu, click Save.

**Configure an LDAP Namespace for Oracle Directory Server**

If you configure a new LDAP namespace for use with Oracle Directory Server, you must modify the necessary settings and change the values for all properties of the Oracle Directory Server objects.

**Procedure**

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the Explorer window, under Security, right-click Authentication, and then click New resource > Namespace.
3. In the Name box, type a name for your authentication namespace.
4. In the Type list, click LDAP and then click OK.

The new authentication namespace resource appears in the Explorer window, under the Authentication component.
5. 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.

6. Specify the values for all other required properties to ensure that IBM Cognos can locate and use your existing authentication namespace.

   The following settings are examples:
   - For **User lookup**, enter \( \text{uid} = \{\text{userID}\} \)
   - If you use single signon, for **Use external identity**, set the value to *True*.
   - If you use single signon, for **External identity mapping**, specify any attribute, such as the NT user domain ID or the user ID:
     \[
     \text{ntuserdomainid} = \$\text{environment}('\text{REMOTE}\_\text{USER}')
     \]
     \[
     \text{uid} = \$\text{environment}('\text{REMOTE}\_\text{USER}')
     \]

   **Important:** Ensure that you use only the variable `REMOTE_USER`. Using another variable can cause a security vulnerability.

   - For **Unique identifier**, type `nsuniqueid`

7. If you want the LDAP authentication provider to bind to the directory server using a specific **Bind user DN and password** when performing searches, then specify these values.

   If no values are specified, the LDAP authentication namespace binds as anonymous.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following:
   - Ensure that **Use external identity** is set to *False*.
   - Set **Use bind credentials for search** to *True*.
   - Specify the user ID and password for **Bind user DN and password**.

9. To configure the LDAP advanced mapping properties for use with Oracle Directory Server objects, use the values specified in the following table.

   **Table 41. LDAP advanced mapping values for use with Oracle Directory Server objects**

<table>
<thead>
<tr>
<th>Mappings</th>
<th>LDAP property</th>
<th>LDAP value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Object class</td>
<td>organizationalUnit,organization</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>ou,o</td>
</tr>
<tr>
<td>Group</td>
<td>Object class</td>
<td>groupofuniquenames</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Member</td>
<td>uniquemember</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>cn</td>
</tr>
<tr>
<td>Account</td>
<td>Object class</td>
<td>inetorgperson</td>
</tr>
<tr>
<td></td>
<td>Business phone</td>
<td>telephonenumber</td>
</tr>
<tr>
<td></td>
<td>Content locale</td>
<td>preferredlanguage</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Email</td>
<td>mail</td>
</tr>
<tr>
<td></td>
<td>Fax/Phone</td>
<td>facsimiletelephonenumber</td>
</tr>
<tr>
<td></td>
<td>Given name</td>
<td>givenname</td>
</tr>
<tr>
<td></td>
<td>Home phone</td>
<td>homephone</td>
</tr>
</tbody>
</table>
Table 41. LDAP advanced mapping values for use with Oracle Directory Server objects (continued)

<table>
<thead>
<tr>
<th>Mappings</th>
<th>LDAP property</th>
<th>LDAP value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile phone</td>
<td>mobile</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>cn</td>
<td></td>
</tr>
<tr>
<td>Pager phone</td>
<td>pager</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>userPassword</td>
<td></td>
</tr>
<tr>
<td>Postal address</td>
<td>postaladdress</td>
<td></td>
</tr>
<tr>
<td>Product locale</td>
<td>preferredlanguage</td>
<td></td>
</tr>
<tr>
<td>Surname</td>
<td>sn</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>uid</td>
<td></td>
</tr>
</tbody>
</table>

These mapping properties represent changes based on a default Oracle Directory Server installation. If you have modified the schema, you may have to make additional mapping changes.

LDAP attributes that are mapped to the Name property in Folder mappings, Group mappings, and Account mappings must be accessible to all authenticated users. In addition, the Name property must not be blank.

10. From the File menu, click Save.

Make Custom User Properties for LDAP Available to IBM Cognos Components

You can use arbitrary user attributes from your LDAP authentication provider in IBM Cognos components. To configure this, you must add these attributes as custom properties for the LDAP namespace. The custom properties are available as session parameters through Framework Manager.

You can also use the custom properties inside command blocks to configure Oracle sessions and connections. You can use the command blocks with Oracle lightweight connections and virtual private databases. For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.

For more information about session parameters, see the Framework Manager User Guide.

Procedure

1. In each location where you installed Content Manager, open Cognos Configuration.
2. In the Explorer window, under Security > Authentication, click the LDAP namespace.
3. In the Properties window, click in the Value column for Custom properties, and click the edit icon.
4. In the Value - Custom properties window, click Add.
5. Click the Name column, and type the name you want IBM Cognos components to use for the session parameter.
6. Click the Value column, and type the name of the account parameter in your LDAP authentication provider.
7. Repeat the preceding two steps for each custom parameter.
8. Click OK.
9. From the **File** menu, click **Save**.

**Enable Secure Communication to the LDAP Server**

Secure LDAP protocol (LDAPS) encrypts the communication between the Access Manager component of Content Manager and the directory server. LDAPS prevents sensitive information in the directory server and the LDAP credentials from being sent as clear text.

To enable LDAPS, install a server certificate that is signed by a certificate authority in the directory server. Next, create a certificate database to contain the certificates. Finally, configure the directory server and the IBM Cognos LDAP namespace to use LDAPS.

The server certificate must be a copy of either
- the trusted root certificate and all other certificates that make up the chain of trust for the directory server certificate.
- The trusted root certificate is the certificate of the root certificate authority that signed the directory server certificate.
- the directory server certificate only

The certificates must be Base64 encoded in ASCII (PEM) format. All certificates except the trusted root certificate must not be self-signed.

**Before you begin**

IBM Cognos works with both the cert8.db and cert7.db versions of the client certificate database. You must use the certutil tool from Netscape OpenSource toolkit NSS_3_11_4_RTM to create the certificate database. IBM Cognos does not accept other versions of cert8.db files, including those from the certutil tool that is provided with Microsoft Active Directory. The appropriate certutil tool is available from the FTP Web site at Mozilla.

You must also use version 4.6.7 of the NSPR library, which is available from the FTP Web site at Mozilla.

**Procedure**

1. Create a directory for the certificate database.
2. Create the certificate database by typing
   ```
   certutil -N -d certificate_directory
   ```
   where `certificate_directory` is the directory that you created in step 1.
   This command creates a cert8.db file and a key3.db file in the new directory.
3. Add the certificate authority (CA) certificate or the directory server certificate to the certificate database by typing the appropriate command for the type of certificate:
   - For a CA certificate, type
     ```
     certutil -A -n certificate_name -d certificate_directory -i CA.cert -t C,C,C
     ```
   - For a directory server certificate, type
     ```
     certutil -A -n certificate_name -d certificate_directory -i server_certificate.cert -t P
     ```
   where `certificate_name` is an alias that you assign, such as the CA name or host name; and `server_certificate` is the prefix of the directory server certificate file.
4. Copy the certificate database directory to the c10_location/configuration directory on every location where Content Manager is installed.

5. Configure the directory server to use LDAPS and restart the directory server.
   For more information, see the documentation for the directory server.

6. In each Content Manager location where you configured the LDAP namespace to use the directory server, start IBM Cognos Configuration.

7. In the Explorer window, under Security > Authentication, click the LDAP namespace.

8. In the Properties window, for the Host and port property, change the port to the secure LDAPS port.
   For the SSL certificate database property, specify the path to the cert7.db file.

9. In the Explorer window, right-click the LDAP namespace and click Test.
   If the test fails, revise the properties, ensuring that the correct certificate is used.

10. From the File menu, click Save.

11. From the Actions menu, click Restart.

12. Repeat steps 6 to 11 on every other location where Content Manager is installed.

**Enabling Single Signon Between LDAP and IBM Cognos Components**

You achieve single signon to IBM Cognos components by configuring the External Identity mapping property.

The External Identity mapping can refer to a CGI environment variable or an HTTP header variable. In the case of an application server gateway or dispatcher entry pointing to IBM Cognos components, the External Identity mapping can refer to the userPrincipalName session variable. The resolved value of the External Identity mapping property at runtime must be a valid user DN.

When an LDAP namespace is configured to use the External Identity mapping property for authentication, the LDAP provider binds to the directory server using the Bind user DN and password or using anonymous if no value is specified. All users who log on to IBM Cognos using external identity mapping see the same users, groups, and folders as the Bind user.

If you want IBM Cognos components to work with applications that use Java or application server security, you can configure the External identity mapping property to obtain the user ID from the Java user principal. Include the token ${environment("USER_PRINCIPAL")} in the value for the property. For more information, see the online help for IBM Cognos Configuration.

You can apply limited expression editing to the External Identity mapping property using the replace operation.

**Replace operation**

The replace operation returns a copy of the string with all occurrences of the old substring replaced by the new substring.

The following rules apply:

- The character \ escapes the characters in the function parameters. Characters such as \ and " need escaping.
• Nested function calls are not supported.
• Special characters are not supported.

Syntax

${\text{replace}}(\text{str}, \text{old}, \text{new})$

Parameters for the Replace Operation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>str</td>
<td>The string to search.</td>
</tr>
<tr>
<td>old</td>
<td>The substring to be replaced by the new substring.</td>
</tr>
<tr>
<td>new</td>
<td>The substring that replaces the old substring.</td>
</tr>
</tbody>
</table>

Examples

${\text{replace}}({\text{environment}}(\"REMOTE\_USER\")},"\text{NAMERICA\"}",})

${\text{replace}}({\text{environment}}(\"REMOTE\_USER\")},"\text{NAMERICA\"","\")}$

Configure IBM Cognos components to use CA SiteMinder

You can configure IBM Cognos components to use a CA SiteMinder namespace as an authentication source.

**Note:** The authentication provider uses the CA SiteMinder Software Development Kit to implement a custom agent. The custom agent deployment requires that you set the Agent Properties in the CA SiteMinder Policy server administration console to support 4.x agents.

**CA SiteMinder configured for more than one user directory**

If your CA SiteMinder environment is configured for more than one user directory, you must use the SiteMinder namespace type in IBM Cognos Configuration.

After you configure the SiteMinder namespace in IBM Cognos Configuration, you must also add a corresponding LDAP or Active Directory Server namespace to IBM Cognos Configuration for each user directory that is defined in CA SiteMinder.

When you configure a corresponding LDAP namespace, ensure that the **External identity mapping** property is enabled and that you include the **REMOTE_USER** token in property value. This does not mean that you must configure CA SiteMinder to set **REMOTE_USER**.

When you configure a corresponding Active Directory namespace, ensure that the singleSignOnOption property is set to **IdentityMapping**.

The SiteMinder namespace passes user information internally to the corresponding LDAP namespace using the **REMOTE_USER** environment variable when it receives successful user identification from the CA SiteMinder environment.
For more information, see “Enabling single signon between Active Directory Server and IBM Cognos Components to use REMOTE_USER” on page 151.

**Important:** Ensure that you use only the variable **REMOTE_USER**. Using another variable can cause a security vulnerability.

### CA SiteMinder configured with only one user directory

If your CA SiteMinder environment is configured with only one user directory, you do not have to use the **SiteMinder** namespace type in IBM Cognos Configuration.

In this case, you can use the user directory as your authentication source by configuring the appropriate namespace, or you can configure the **SiteMinder** with one user directory. For example, if the CA SiteMinder user directory is LDAP, you can configure IBM Cognos components with an LDAP namespace or with one **SiteMinder** namespace, referring to one user directory that is an LDAP namespace.

If the CA SiteMinder user directory is Active Directory, you can use an Active Directory namespace or an LDAP namespace that is configured for use with Active Directory.

If you want to use the user directory as your authentication source directly instead of configuring a **SiteMinder** namespace, you can configure the appropriate LDAP or Active Directory namespace. In this case, verify the Agent Configuration Object properties in CA SiteMinder Policy Server. Ensure that **SetRemoteUser** is activated.

When you configure the Active Directory namespace, ensure that the **singleSignOnOption** property is set to **IdentityMapping**.

When you configure a corresponding LDAP namespace, ensure that the **External identity mapping** property is enabled and that you include the **REMOTE_USER** token in property value.

For more information, see “Enabling single signon between Active Directory Server and IBM Cognos Components to use REMOTE_USER” on page 151.

**Important:** Ensure that you use only the variable **REMOTE_USER**. Using another variable can cause a security vulnerability.

### Configuring the SiteMinder namespace

If you configured CA SiteMinder for more than one user directory, you must use the **SiteMinder** namespace type in IBM Cognos Configuration. After you add the **SiteMinder** namespace, you must also add a corresponding LDAP namespace for each user directory in your CA SiteMinder environment.

You can also use the **SiteMinder** namespace type if users are stored in an LDAP server or an Active Directory server.

You can hide namespaces from users during login. You can have trusted signon namespaces without showing them on the namespace selection list that is presented when users login. For example, you want to integrate single sign-on across systems but maintain the ability for customers to authenticate directly to IBM Cognos without being prompted to choose a namespace.
Before you begin

To use the SiteMinder namespace, you must obtain the required CA SiteMinder library files, which are shown in the following table, and add the files to the appropriate library path for your operating system.

Table 43. CA SiteMinder library files

<table>
<thead>
<tr>
<th>Operating system</th>
<th>CA SiteMinder library file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris and AIX</td>
<td>libsmagentapi.so</td>
</tr>
<tr>
<td>Microsoft Windows 64-bit</td>
<td>smagentapi.dll</td>
</tr>
<tr>
<td>Microsoft Windows 32-bit</td>
<td>smagentapi.dll</td>
</tr>
<tr>
<td></td>
<td>smerrlog.dll</td>
</tr>
</tbody>
</table>

Procedure

1. On the computer where you installed Content Manager, append the directory that contains the CA SiteMinder library file to the appropriate library path environment variable.
   - For Solaris operating systems, `LD_LIBRARY_PATH`
   - For AIX operating systems, `LIBPATH`
   - For Microsoft Windows operating systems, `PATH`
2. Open IBM Cognos Configuration.
3. In the Explorer window, under Security, right-click Authentication, and click New resource > Namespace.
4. In the Name box, type a name for your authentication namespace.
5. In the Type list, select the SiteMinder and then click OK.
6. Select the namespace that you added.
7. In the Namespace ID property, specify a unique identifier for the namespace.
   
   **Note:** Do not use a colon (:) in the identifier.
8. Specify values for the other required properties.

   **Note:** If you do not want the namespace name to appear to users when they are logging in, set the Selectable for authentication property to False.
9. In the Explorer window, under Security > Authentication, right-click the namespace that you added, and click New resource > SiteMinder Policy Server.
10. In the Name box, type a name for the policy server and click OK.
11. In the Properties window, specify the Host property and any other property values you want to change.
12. In the Explorer window, right-click the new SiteMinder policy server that you added and click New resource > User directory.
13. In the Name box, type a name for the user directory and click OK.

   **Important:** The name of the user directory must match the policy server name.
15. Configure a user directory for each user directory in the SiteMinder policy server.
16. Click File > Save.
17. Test the connection to a new namespace. In the Explorer window, under Authentication, right-click the new authentication resource and click Test.
18. Configure a corresponding LDAP or Active Directory namespace for each user directory.
   Ensure that you use the same value for the Namespace ID property that you use for the Namespace ID property for the SiteMinder namespace.

**Configuring IBM Cognos to Use a RACF Provider for Authentication**

If you use a Resource Access Control Facility (RACF) provider for authentication in your enterprise environment, you can also use it for authentication in IBM Cognos products.

**Procedure**
1. Configure IBM Cognos components to use a RACF namespace
2. Configure secure communication
3. Enable single signon between the RACF provider and IBM Cognos components

**Configuring a RACF Namespace**

You can configure a Resource Access Control Facility (RACF) namespace using IBM Cognos Configuration.

**Before you begin**

Before you configure the RACF namespace, you must do the following:

- You must be running Tivoli Directory Server.
- Tivoli Directory Server must be configured for LDAP, to access the SDBM (RACF) database.

For more information, see the topic about configuring Tivoli Access Manager for LDAP in the IBM Information Center.

**Procedure**
1. In the location where you installed Content Manager, open IBM Cognos Configuration.
2. To create the namespace, do the following:
   - In the Explorer window, under Security, right-click Authentication, and click New resource > Namespace.
   - In the Name box, type a name for your authentication namespace.
   - In the Type list, click RACF and then click OK.
   The new authentication provider resource appears in the Explorer window, under the Authentication component.
3. In the Properties window, for the Namespace ID property, specify a unique identifier for the namespace.
   Do not use colons (;) in the Namespace ID property.
4. For the Host and port property, type the value that corresponds to the Tivoli Directory Server.
5. For the Base Distinguished Name property, type the value that matches the suffix that is configured for SDBM in the Tivoli Directory Server.
6. If you are using an SSL connection to the RACF provider, set the **Enable SSL** property to **true**.

7. To map to RACF account properties such as email and phone number, for the **Base segment DATA** and the **TSO segment USERDATA** properties under **Account mappings**, click in the value column and select the value from the drop-down list.

8. From the **File** menu, click **Save**.

9. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

**Enabling single signon between RACF and IBM Cognos**

Enable single signon between the Resource Access Control Facility (RACF) provider and IBM Cognos components to simplify the authentication process for users, avoid the need for multiple signons, and simplify user identity management across the network.

You achieve single signon by configuring identity mapping in IBM Cognos Configuration, configuring IBM WebSphere Application Server to set the REMOTE_USER, and then configuring WebSphere to authenticate against RACF.

**Important:** Ensure that you use only the variable REMOTE_USER. Using another variable can cause a security vulnerability.

When a RACF namespace is configured to use identity mapping for authentication, the RACF namespace binds to the RACF provider using the binding credentials or anonymously if no binding credentials are specified. All users who log on to IBM Cognos using identity mapping see the same users, groups, and folders as the binding user.

**Procedure**

1. In every location where you installed Content Manager, open IBM Cognos Configuration.

2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click the RACF namespace.

3. In the **Resource properties** window, change **Enable identity mapping** to **True**.

4. Click the value column for **Binding credentials** and then click the edit icon.

5. In the **Value - Binding credentials** dialog box, specify the **User ID** and **Password**.

6. In IBM Cognos Configuration, restart the service:
   - In the **Explorer** window, expand **IBM Cognos services**, and select the service.
   - From the **Actions** menu, click **Restart**.

7. Using the WebSphere documentation, configure WebSphere to set REMOTE_USER.

8. Using the WebSphere documentation, configure WebSphere to authenticate using the RACF provider.

**Configure IBM Cognos to use SAP**

To use an SAP server as your authentication provider, you must use a supported version of SAP BW.
The authorization rights required by the SAP user depend on who uses IBM Cognos components: users or administrators.

**SAP Authorization Settings for IBM Cognos Users**

The authorization objects in the following table are required for any IBM Cognos user.

*Table 44. SAP authorization settings for IBM Cognos users*

<table>
<thead>
<tr>
<th>Authorization object</th>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_RFC</td>
<td>Activity</td>
<td>RFC1 RS_UNIFICATION, SDTX, SH3A, SU_USER, SYST, SUSO</td>
</tr>
<tr>
<td></td>
<td>Name of RFC to be protected</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Type of RFC to be protected</td>
<td>FUGR</td>
</tr>
<tr>
<td>S_USER_GRP</td>
<td>Activity</td>
<td>03</td>
</tr>
<tr>
<td>User Master Maintenance: User Groups</td>
<td>Name of user group</td>
<td>*</td>
</tr>
</tbody>
</table>

Some of the values shown, such as *, are default values that you may want to modify for your environment.

**SAP Authorization Settings for IBM Cognos Administrators**

If users perform administrative tasks and searches for users and roles, the values from the following table must be added to the S_RFC authorization object in addition to the values for IBM Cognos users.

*Table 45. SAP authorization settings for IBM Cognos administrators*

<table>
<thead>
<tr>
<th>Authorization object</th>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_RFC</td>
<td>Activity</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>RFC_NAME</td>
<td>PRGN_J2EE, SHSS, SOA3</td>
</tr>
<tr>
<td></td>
<td>Type of RFC object to be protected</td>
<td>FUGR</td>
</tr>
</tbody>
</table>

Some of the values shown, such as *, are default values that you might want to modify for your environment.

**Configure an SAP Namespace**

You can configure IBM Cognos components to use an SAP server as the authentication source.
Before you begin

If you installed your IBM Cognos product on a 64-bit server, you must also manually copy the SAP RFC library files to the IBM Cognos installation directory.

Procedure

1. If running on a 64-bit server, do the following:
   - Go to the SAP installation directory on the 64-bit server.
   - Copy all 64-bit SAP RFC library files to c10_64_location\bin64, where c10_64_location is the directory where you installed the IBM Cognos server.
   - Copy all 32-bit SAP RFC library files to c10_64_location\bin.
2. If running on a 32-bit server, copy all 32-bit SAP library files from the SAP installation directory to the c10_64_location\bin64 directory.
3. In the location where you installed Content Manager, open IBM Cognos Configuration.
4. In the Explorer window, under Security, right-click Authentication, and click New resource > Namespace.
5. In the Name box, type a name for your authentication namespace.
6. In the Type list, click SAP and then click OK.
   The new authentication provider 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.
   Important: Do not use colons (:) in the Namespace ID property.
8. Specify the values for all required properties to ensure that IBM Cognos components can locate and use your existing authentication provider.
   Depending on your environment, for the Host property, you may have to add the SAP router string to the SAP host name.
9. If the SAP system encodes the contents of cookies, enable the decode tickets feature:
   - In the Properties window, for Advanced properties, click the Value and then click the edit icon.
   - Click Add.
   - Enter the name URLDecodeTickets and enter the value true
   - Click OK.
   All SAP logon tickets will be decoded by the SAP namespace before establishing a connection.
10. From the File menu, click Save.
11. Test the connection to a new namespace. In the Explorer window, under Authentication, right-click the new authentication resource and click Test.

Enable Single Signon Between SAP and IBM Cognos

You can enable single signon between SAP Enterprise Portal and IBM Cognos components as well as when using the external namespace function of the SAP BW data source connections.

To do so, ensure that you set the following system parameters on the SAP BW server:
Delete an Authentication Provider

If they are no longer required, you can delete namespaces that you added, or unconfigure namespaces that IBM Cognos components detected.

You must not delete the Cognos namespace. It contains authentication data that pertains to all users and is required to save the configuration.

When you delete a namespace, you can no longer log on to the namespace. Security data for the namespace remains in Content Manager until you permanently delete it in the portal. For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.

Procedure

1. In each location where you installed Content Manager, open Cognos Configuration.
2. In the Explorer window, under Security > Authentication, right-click the namespace and click Delete.
3. Click Yes to confirm.
   The namespace disappears from the Explorer window and you can no longer log on to the namespace in that location.
4. From the File menu, click Save.
5. Repeat steps 1 to 4 for each location where you installed Content Manager.
   You must now log on to the portal and permanently delete the data for the namespace. For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.

Results

After you delete a namespace, it appears as Inactive in the portal.
Chapter 9. Configuration options

After you install and configure IBM Cognos components, you can change the configuration for your environment. Initially, default property settings are used to configure the components. However, you can change these default settings if existing conditions make the default choices inappropriate, or to better suit your environment.

For example, you can configure features for IBM Cognos Application Firewall or specify the amount of resources that IBM Cognos components use. Also, you can deliver IBM Cognos content using another portal by configuring Portal Services.

You can configure IBM Cognos components to use other resources, such as using an authentication provider and then enabling single signon for the database connection and the users.

If you use a load-balancing scheme in your environment, you can change settings to improve performance. For example, you can balance requests among dispatchers by changing their processing capacity or by setting the minimum and maximum number of processes and connections. For more information about tuning server performance, see the Administration and Security Guide.

For all Microsoft Windows operating system and most UNIX and Linux operating system installations, use IBM Cognos Configuration to configure your settings. However, if the console attached to the UNIX or Linux computer on which you are installing IBM Cognos components does not support a Java-based graphical user interface you must manually edit the cogstartup.xml file in the c10_location/configuration directory, and then run IBM Cognos Configuration in silent mode.

Use these optional configuration tasks to customize your configuration so that IBM Cognos components easily integrate into your existing environment.

Start IBM Cognos Configuration

Use the configuration tool, IBM Cognos Configuration, to configure IBM Cognos, or to start and stop IBM Cognos services.

Before starting IBM Cognos Configuration, ensure that the operating environment is properly set up. For example, ensure that all variables have been set.

You should start IBM Cognos Configuration in the last page of the installation wizard on Microsoft Windows, UNIX, or Linux operating systems only if additional setup is not required. For example, if you use a database server other than Microsoft SQL for the content store, copy the JDBC drivers to the appropriate location before you start the configuration tool.

To start IBM Cognos Configuration on a Windows computer,

• From the Start menu, click Programs > IBM Cognos 10 > IBM Cognos Configuration.

To start IBM Cognos Configuration on a UNIX or Linux computer,
Changing the version of Java used by IBM Cognos BI components

IBM Cognos Business Intelligence components require a Java Runtime Environment (JRE) to operate.

You can change the Java version in situations where you want to use IBM Cognos BI components with an application server that requires a specific JRE version or you already use a JRE version with other applications.

Use the following steps to change the Java version:

1. Back up existing IBM Cognos data and encryption keys, if required.
2. Update the Java environment

Related concepts:

“Java requirements” on page 24

To support the cryptographic services in IBM Cognos Business Intelligence, you may be required to update your version of Java or set a JAVA_HOME environment variable. Depending on your security policy requirements, you may also have to install the unrestricted Java Cryptography Extension (JCE) policy file.

Back up existing IBM Cognos information

You must back up existing IBM Cognos information if IBM Cognos Business Intelligence components are running on an application server (including Tomcat) and you are changing to an application server that ships with its own JVM. You must also back up existing IBM Cognos information if you must change the JVM you are using.

Note: You must back up existing IBM Cognos information within the working environment prior to upgrade.

Before configuring IBM Cognos BI components to run on the new application server or JVM, you must back up:

- content store data by creating a deployment export.
- configuration information by exporting it. Any encrypted data is decrypted during the export.
- cryptographic keys by saving them to an alternate location. New cryptographic keys must be created using the same JVM that the application server uses. Because these keys can be created only if the previous keys are deleted, it is important to back up the previous keys.

To ensure the security and integrity of your IBM Cognos data, back up the content store, configuration information, and cryptographic keys to a directory that is protected from unauthorized or inappropriate access.

Tip: To check if any cryptographic keys exist, look in the c10_location/configuration directory. Cryptographic keys exist if this directory includes the following subdirectories: csk, encryptkeypair or signkeypair.

Procedure

1. If data exists in the content store, start the IBM Cognos service and export the entire content store using the Deployment tool.

- Go to the c10_location/bin directory and then type ./cogconfig.sh
For more information, see the topic about creating an export deployment specification in the *IBM Cognos Business Intelligence Administration and Security Guide*.

2. In IBM Cognos Configuration, from the **File** menu, click **Export As** and save the configuration information in a decrypted format. When naming the file, use a name such as decrypted.xml.

   Export the data to a directory that is protected from unauthorized or inappropriate access because passwords are stored in plain text. You are prompted to acknowledge that the export is an unsecure operation.

3. Stop the IBM Cognos service:
   - If you use Tomcat, stop the IBM Cognos service and close IBM Cognos Configuration.
   - If you use an application server other than Tomcat, shut down IBM Cognos BI in your environment.

4. Back up any existing cryptographic keys by saving the appropriate files and directories to an alternate location that is secure.

   The files are
   - `c10_location/configuration/cogstartup.xml`
   - `c10_location/configuration/caSerial`
   - `c10_location/configuration/cogconfig.prefs`
   - `c10_location/configuration/coglocale.xml`

   The directories are
   - `c10_location/configuration/csk`
   - `c10_location/configuration/encryptkeypair`
   - `c10_location/configuration/signkeypair`

5. Delete the `caSerial` and `cogconfig.prefs` files and the three directories: `csk`, `encryptkeypair`, and `signkeypair`.

6. Replace the `c10_location/configuration/cogstartup.xml` file with the file that contains the data exported from IBM Cognos Configuration (for example, `decrypted.xml`).

   In the `c10_location/configuration` directory, the file must use the name `cogstartup.xml`.

   The information in this file will be automatically re-encrypted using new cryptographic keys when you save the configuration in IBM Cognos Configuration.

### Change your Java version

You can change the Java version in situations where you want to use IBM Cognos BI components with an application server that requires a specific JRE version or you already use a JRE version with other applications. You change Java versions by setting the `JAVA_HOME` environment variable.

**JAVA_HOME**

Set a `JAVA_HOME` environment variable if:
- You are installing on a UNIX or Linux operating systems.
- You are installing on Microsoft Windows operating systems and you want to use your own Java or a Java bundled with other software. For example, if you are installing IBM Cognos BI on WebSphere Application Server.
Ensure that the JRE version is supported by IBM Cognos products.

On Microsoft Windows operating systems, if you do not have a JAVA_HOME variable, the JRE files that are provided with the installation are used.

To verify that your JRE is supported, go to the IBM Software Product Compatibility Reports (SPCR) page (www.ibm.com/support/docview.wss?uid=swg27037784). Click the link for your version of Cognos BI and locate the Java Run Time Libraries information.

**Unrestricted JCE Policy File**

JREs include a restricted policy file that limits you to certain cryptographic algorithms and cipher suites. If you require a wider range of cryptographic algorithms and cipher suites than are shown in IBM Cognos Configuration, you can download and install the unrestricted JCE policy file.

For Java that is provided by IBM, the unrestricted JCE policy file is available on the IBM website (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk).

**Changing Default Configuration Settings**

When you install IBM Cognos components, the installation uses default configuration settings. If you have any reason not to use these default values, such as a port is being used by another process, use IBM Cognos Configuration to change the value.

If you change the value of a property, you must save the configuration and then restart the IBM Cognos service to apply the new settings to your computer.

For distributed installations, ensure that you configured all computers where you installed Content Manager before you change default configuration settings on other IBM Cognos computers. For example, you can:

- change the default user and password for Cognos Content Database
- change a URI
- configure cryptographic settings
- configure IBM Cognos components to use IBM Cognos Application Firewall
- configure temporary file properties
- configure the gateway to use a namespace
- enable and disable services
- configure fonts
- change the default font for reports
- save report output to a file system
- change the notification database

After you change the default behavior of IBM Cognos components to better suit your IBM Cognos environment, you can configure Portal Services, configure an authentication provider, or test the installation.

For IBM Cognos BI, you can install and configure Framework Manager. For Metric Studio, you can install and configure Metric Designer.
Change Default User and Password for Cognos Content Database

If you install Cognos Content Database, the default database that is created is given a user ID and password. Change this user ID and password.

Administration tasks for Cognos Content Database are performed using a utility named ij. For information about this utility, see the Apache Derby documentation. The documentation is available in the c10_location/derby10.1.2.1/docs directory where you installed Cognos Content Database.

Changing the default user password

If you install Cognos Content Database, the default database that is created is given a user ID and password. Change this user ID and password.

Procedure

1. On the computer where you installed Cognos Content Database, go to the c10_location/derby10.1.2.1/bin directory.
2. Start the ij utility using the ij.bat or ij.ksh script file.
   The ij utility is a command line utility for creating and managing Cognos Content Database.
3. Connect to the default database by typing the following ij utility command:
   `connect 'jdbc:derby://localhost:1527/cm;user=cognos;password=cognos';`
   If you changed the port number from the default 1527, use the correct port number for your Cognos Content Database.
   The default database is named cm. The database name is case sensitive.
4. Change the default password for the cognos user by typing the following ij utility command:
   `CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.cognos', 'NewPassword');`
   The new password must be used for the next connection to the database.
5. Close the ij utility by typing the following command:
   `disconnect;`

Creating a new user and password

If you install Cognos Content Database, the default database that is created is given a user ID and password. Change this user ID and password.

Procedure

1. On the computer where you installed Cognos Content Database, go to the c10_location/derby10.1.2.1/bin directory.
2. Start the ij utility using the ij.bat or ij.ksh script file.
3. Connect to the default database by typing the following ij utility command:
   `connect 'jdbc:derby://localhost:1527/cm;user=cognos;password=cognos';`
   If you changed the port number from the default 1527, use the correct port number for your Cognos Content Database.
   The default database is named cm. The database name is case sensitive.
4. Create a new user by typing the following ij utility command:
   `CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.NewUser', 'NewUserPassword');`
5. Give the new user full access to the database by typing the following ij utility command:

```sql
CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY
  ('derby.database.fullAccessUsers','cognos, NewUser');
```

The property that you are changing, the list of users, is a comma-delimited field. In this step, you are including the new user in the list of users with full access. The default user, cognos, is still part of the list of users with full access. You can remove the cognos user.

6. Close the ij utility by typing the following command:

```sql
disconnect;
```

### Removing a user

If you have user accounts that you are no longer using for Cognos Content Database, you can remove them.

**Procedure**

1. On the computer where you installed Cognos Content Database, go to the `c10_location/derby10.1.2.1/bin` directory.
2. Start the ij utility using the ij.bat or ij.ksh script file.
3. Connect to the default database by typing the following ij utility command:

```sql
connect 'jdbc:derby://localhost:1527/cm;user=NewUser;
  password=NewUserPassword';
```

4. Choose the kind of user that you want to remove:
   - To remove a user from the list of users with full access, type the following ij utility command:
     ```sql
     CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY
       ('derby.database.fullAccessUsers', 'NewUser');
     ```
     You omit the user name from the list of users with full access. For example, the previous command, removes the default cognos user and keeps the new user that you just created.
   - To remove a user from the database, type the following ij utility command and omit the user password:
     ```sql
     CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.cognos', '');
     ```
     This command removes the password for the default cognos user, which also removes the user from the database.

5. Close the ij utility by typing the following command:

```sql
disconnect;
```

### Port and URI Settings

You can change certain elements in a URI depending on your environment. An IBM Cognos URI contains the following elements:

- For a Content Manager URI, Dispatcher URI for external applications, or dispatcher URI
  ```
  protocol://host_name_or_IP:port/context_root/alias_path
  ```
- For a Gateway URI or a Web content URI
  ```
  protocol://host_name_or_IP:port/virtual_directory/gateway_application
  ```
  or
  ```
  protocol://host_name_or_IP:port/context_root/alias_path
  ```

The elements are described in the following table:
Table 46. IBM Cognos URI elements and descriptions

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| protocol              | Specifies the protocol used to request and transmit information, either Hyper Text Transfer Protocol or Hyper Text Transfer Protocol (Secure).  
                         | **Example:** http or https                                                                                                                  |
| host name or IP       | Specifies the identity of the host on the network. You can use an IP address, a computer name, or a fully qualified domain name.  
                         | In a distributed installation, you must change the localhost element of a URI.  
                         | In a mixed environment of UNIX and Microsoft Windows operating system servers, ensure that host names can be resolved to IP addresses by all servers in the environment.  
                         | **Example:** localhost or 192.168.0.1 or [2001:0db8:0000:0000:0000:148:57ab]:80                                                                 |
| port                  | Specifies the port on which the host system listens for requests.  
                         | The default port for Tomcat is 9300. The default port for a Web server is 80.  
                         | **Example:** 9300 or 80                                                                                                                     |
| context root          | Used by Tomcat or an application server to determine the context of the application so that the request can be routed to the correct Web application for processing.  
                         | **Example:** p2pd                                                                                                                          |
| alias path            | Used by the application server to route a request to the correct component within a Web application.  
                         | The alias path must not be modified or IBM Cognos components will not function properly.  
                         | **Example:** servlet/dispatch                                                                                                                |
| virtual directory     | Used by the Web server to map a virtual directory or alias to a physical location.  
                         | For example, in the default Gateway URI of http://localhost:80/ibmcognos/cgi-bin/cognos.cgi, the virtual directory is ibmcognos/cgi-bin.  
                         | **Example:** ibmcognos/                                                                                                                     |
| gateway application   | Specifies the name of the Cognos gateway application that is used.  
                         | For example, if you are accessing IBM Cognos components using a Common Gateway Interface (CGI), then the default gateway application would be cognos.cgi.  
                         | **Example:** cognos.cgi                                                                                                                     |
Change a Port or URI Setting
Use the following procedure to change URI properties in IBM Cognos Configuration.

Procedure
1. Start IBM Cognos Configuration.
2. In the Explorer window, click the appropriate group or component:
   - To change an element for the dispatcher, click Environment.
   - To change an element for the local log server, under Environment, click Logging.
3. In the Properties window, click the Value box next to the URI property that you want to change.
4. Select the element and type the new information.

   Tips:
   - To change the port used by the local dispatcher, change the value of the internal dispatcher URI property. Because the change affects all the URIs that are based on the local dispatcher, you must change the URIs of all local components.
   - If you change the dispatcher port in the dispatcher URI, ensure that you specify the new port number when you configure remote computers that use the dispatcher, Content Manager, or Software Development Kit services on this system.
5. From the File menu, click Save.

Configuring Cryptographic Settings
IBM Cognos components require a cryptographic provider; otherwise they will not run. If you delete the default cryptographic provider, you must configure another provider to replace it.

You can configure the following cryptographic settings:
- general cryptographic settings
- settings for the default cryptographic provider
- settings for a cryptographic provider in an Entrust security infrastructure

Configure General Cryptographic Settings
In a distributed installation, IBM Cognos computers communicate with Content Manager to establish trust and obtain some cryptographic keys from Content Manager.

If you change the cryptographic keys in Content Manager, such as by changing application servers or reinstalling Content Manager, you must delete the cryptographic keys on the other IBM Cognos computers. You must then save the configuration on each computer so that they obtain the new cryptographic keys from Content Manager. In addition, all IBM Cognos components in a distributed installation must be configured with the same cryptographic provider settings.

Also, in a distributed environment, the symmetric key should only be stored on computers where Content Manager has been installed.

You can configure the following general cryptographic settings:
- common symmetric key store (CSK) properties
The CSK is used by IBM Cognos to encrypt and decrypt data.

- secure sockets layer (SSL) settings
  These include mutual authentication and confidentiality.
- advanced algorithm settings
  These include signing and digest algorithms.

**Procedure**

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, click **Cryptography**.
3. In the **Properties** window, change the default values by clicking the **Value** box and then selecting the appropriate value:
   - On computers that do not contain Content Manager, if you do not want to store the CSKs locally, under **CSK settings**, change **Store symmetric key locally** to **False**.
     - When **Store symmetric key locally** is **False**, the key is retrieved from Content Manager when required. The **Common symmetric key store location** property is ignored.
   - If you want the computers at both ends of a transmission to prove their identity, under **SSL Settings**, change **Use mutual authentication** to **True**.
     - Do not change the **Use confidentiality** setting.
   - If you want to change the digest algorithm, for the **Digest algorithm** property, select another value.
4. From the **File** menu, click **Save**.
5. Test the cryptographic provider on a gateway computer only. In the **Explorer** window, right-click **Cryptography** and click **Test**.
   - IBM Cognos components check the availability of the symmetric key.

**Results**

After you configure the cryptographic settings, passwords in your configuration and any data you create are encrypted.

**Configure Settings for the Default Cryptographic Provider**

You can configure some cryptographic settings for the cryptographic provider.

The configurable settings include the following:

- algorithms and ciphersuites
- identity name settings
- signing key store properties
  - The signing key pair includes the private key used to generate the digital signature and the public key used to verify authenticity.
- encryption key store properties
  - The encryption key pair includes the private key used to encrypt data and the public key used to decrypt data.
- certificate authority settings
  - These include properties for the provided certificate authority (CA) or a third-party CA.
Procedure

1. If you are using a JRE other than the one provided with IBM Cognos server, go to the \texttt{c10\_location/bin/jre/version/lib/ext}.
   If you are using 64-bit components, go to the \texttt{c10\_location/bin64/jre/version/lib/ext} directory.

2. Copy \texttt{bcprov-jdkversion.jar} to \texttt{JRE\_location/lib/ext}.

3. If you are using a JRE other than one IBM provides, you must also download and install the unrestricted Java Cryptograph Extension (JCE) policy file for your JRE to ensure that all available algorithms and cipher suites are shown in IBM Cognos Configuration.

4. Start IBM Cognos Configuration.

5. In the Explorer window, under Security, Cryptography, click Cognos.

6. In the Properties window, change the properties as needed.
   - To configure the confidentiality algorithm, under the appropriate property, Confidentiality algorithm or PDF Confidentiality algorithm, click in the Value column and then select the algorithm from the drop-down list.
     The value of a confidentiality algorithm determines how data is encrypted by IBM Cognos components. For example, database passwords entered in IBM Cognos Configuration are encrypted when you save the configuration. The algorithm selected when the data is encrypted must also be available for the data to be decrypted at a later date.
     The availability of confidentiality algorithms can change if there are changes to your environment. For example, if your Java Runtime Environment (JRE) has changed or if you have installed other cryptographic software on the computer. You must ensure that the Confidentiality algorithm that was selected when the data was encrypted is also available when you want to access the data.
     If you have made changes to a computer, such as upgraded the JRE or installed software that has upgraded the JRE, this may affect the availability of confidentiality algorithms. To ensure that the available algorithms and cipher suites are shown in IBM Cognos Configuration, download and install the unrestricted Java Cryptograph Extension (JCE) policy file. For Java that IBM provides, the unrestricted JCE policy file can be downloaded from Unrestricted JCE policy files (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk).
   - To adjust the cipher suites, under Supported ciphersuites, click in the Value column and then click the edit icon \( \mathbf{\text{\text{}}}_\text{\text{}}\).
     Remove the cipher suites that are not applicable and move the remaining cipher suites up or down in the list so that the cipher suites in the highest range are higher in the list.
     Do not mix cipher suites in the 40- to 56-bit range with cipher suites in the 128- to 168-bit range.
   - To change the location of the signing keys, under Signing key settings, change the Signing key store location property to the new location.
   - To change the location of the encryption keys, under Encryption key settings, change Encryption key store location to the new location.
   - To use another certificate authority, under Certificate Authority settings, change Use third party CA to True.
You must also ensure that you use the same values for the -k parameter as you used for the Signing key store location and Encryption key store location properties.

For more information, see "Configuring IBM Cognos components to use another certificate authority" on page 205.

7. From the File menu, click Save.

Results

If you use another Certificate Authority (CA) server, configure IBM Cognos components to use the CA. For more information, see "Configuring IBM Cognos components to use another certificate authority" on page 205.

Configure Cryptographic Provider Settings in an Entrust Security Infrastructure

To configure encryption in an Entrust security infrastructure, you replace the default cryptographic provider in IBM Cognos Configuration with a provider that you configure for Entrust and then you update security files in your IBM Cognos environment.

Before you begin

Ensure that the key store passwords match the one in your Entrust Profile (EPF).

To prevent gateway errors, ensure that the Internet Guest Account has read and write permission to the Entrust .epf file and read permission to the Entrust .ual file.

Procedure

1. If you are using a JRE other than the one provided with IBM Cognos server, go to the $c10_location/bin/jre/version/lib/ext.
   If you are using 64-bit components, go to the $c10_location/bin64/jre/version/lib64/ext directory.
2. Copy bcprov-jdkversion.jar to JRE_location/lib/ext.
3. Ensure that the following files from IBM Cognos and Entrust exist in the location where the JRE is installed:
   • From the Entrust Authority Security Toolkit that you download from Entrust, copy the .jar file, such as enttoolkit.jar, to JRE_location/lib/ext.
4. To ensure that all available algorithms and cipher suites are shown in IBM Cognos Configuration, download and install the unrestricted Java Cryptography Extension (JCE) policy file. For Java that IBM provides, the unrestricted JCE policy file can be downloaded from Unrestricted JCE policy files (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcensdk).
5. Start IBM Cognos Configuration.
6. In the Explorer window, under the Security group, click Cryptography.
7. In the Properties window, under Advanced algorithm settings, change the Digest algorithm to the appropriate message digest or secure hash algorithm for your security policy.
8. In the Explorer window, under the Security group and the Cryptography component, right-click the IBM Cognos resource, and click Delete.
9. Under the **Security** group, right-click **Cryptography**, and click **New resource > Provider**.

10. In the **Name** field, type a name for the encryption service you are creating.

11. In the **Type** field, click the arrow, and click **Entrust**, and then click **OK**.  
A branch with the name you assigned appears under **Cryptography**.

12. Click the branch you created.  
Resource properties appear in the properties window.

13. In the **Resource Properties** window, enter the appropriate values, as listed in the following table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INI file location</td>
<td>The location of the Entrust initialization file (.ini).</td>
</tr>
<tr>
<td>Identity file distinguished name (DN)</td>
<td>The distinguished name associated with the profile of the Entrust identity.</td>
</tr>
<tr>
<td>Identity file location</td>
<td>The location of the Entrust identity profile file (.epf).</td>
</tr>
<tr>
<td>Use Entrust Server Login</td>
<td>The parameter that controls whether users must enter a password to log on to the Entrust PKI.</td>
</tr>
<tr>
<td>Identity file password</td>
<td>The Entrust Profile password, which must match the one in your Entrust Profile (EPF).</td>
</tr>
<tr>
<td>Confidentiality algorithm</td>
<td>The level of encryption that is required to comply with your security policy.</td>
</tr>
<tr>
<td>PDF Confidentiality algorithm</td>
<td>The encryption algorithm to use when encrypting PDF data.</td>
</tr>
<tr>
<td>Supported ciphersuites</td>
<td>The cipher suites that are supported in your security environment. Remove the ones that are not applicable and rearrange the remaining cipher suites from highest to lowest. This ensures that the most secure cipher suite is used first.</td>
</tr>
<tr>
<td>Signing Key Store Location</td>
<td>The location of the key store that contains the signing key pairs.</td>
</tr>
<tr>
<td>Encryption Key Store Location</td>
<td>The location of the key store that contains encryption key pairs.</td>
</tr>
</tbody>
</table>

**Important:** Record your passwords in a secure location.

14. From the **File** menu, click **Save**.

15. Update to Entrust Java Toolkit 7.2 SP2 Patch 170072.

**IBM Cognos Application Firewall**

IBM Cognos Application Firewall analyzes and validates HTTP and XML requests before they are processed by IBM Cognos servers. IBM Cognos Application Firewall may modify these HTTP and XML requests.

IBM Cognos Application Firewall protects IBM Cognos Web products from malicious data. The most common forms of malicious data are buffer overflows and cross-site scripting (XSS) attacks, either through script injection in valid pages or redirection to another Web site.
You can track firewall activity by checking the log file, which contains rejected requests. By default, log messages are stored in the `c10_location/logs/cogserver.log` file.

All Cognos Application Firewall settings must be the same for all computers where IBM Cognos Application Tier Components are installed within a distributed environment. For example, if Cognos Application Firewall is disabled on some computers and enabled on others, unexpected behavior and product errors may result.

The following types of URLs are accepted by Cognos Application Firewall validation:

- fully qualified (absolute) URLs
  in the format `protocol://host:port/path`, where `protocol` is http or https and `host` is validated against the valid domain list

- URLs relative to the Web installation directory
  in the format `/Web_installation_root/.*` where `Web_installation_root` is the gateway Web directory, based on the ibmcognos alias that you configured on your Web server.
  For example, 
  `/ibmcognos/ps/portal/images/action_delete.gif`

- specific allowed URLs, including the following (all case insensitive)
  `about:blank`
  `JavaScript:window.close( )`
  `JavaScript:parent.close( )`
  `JavaScript:history.back( )`
  `parent.cancelErrorPage( )`
  `doCancel( )`

**Configure IBM Cognos Components to Use IBM Cognos Application Firewall**

Using IBM Cognos Configuration, you can change settings for other XSS tool support, and you can add host and domain names to the IBM Cognos list of valid names.

**Procedure**

1. In each location where IBM Cognos BI Application Tier Components are installed, start IBM Cognos Configuration.
2. In the Explorer window, under Security, click IBM Cognos Application Firewall.
3. In the Properties window, for the Enable CAF validation property, set the appropriate values.

   By default, IBM Cognos Application Firewall is enabled.

   **Important:** The IBM Cognos Application Firewall is an essential component of IBM Cognos security, helping to provide protection against penetration vulnerabilities. Disabling the IBM Cognos Application Firewall will remove this protection. Under normal circumstances, do not disable the IBM Cognos Application Firewall.

4. If you are using another XSS tool that checks for specific characters in GET request parameters, in the Properties window, for the Is third party XSS checking enabled property, change the value to True.
The default characters that are prohibited include >, <, and '.

5. Add host and domain names to the IBM Cognos list of valid names:
   - For the **Valid domains and hosts** property, click the value and then click the
     edit icon.
   - In the **Value - Valid domains or hosts** dialog box, click **Add**.

You must include the domains from all hyperlinks that are added in IBM Cognos Connection. For more information, see the topic about creating a URL in the *IBM Cognos Business Intelligence Administration and Security Guide*.

**Tip:** If you are using drill-through from IBM Cognos Series 7 to reports in IBM Cognos BI, add the hostnames of the IBM Cognos Series 7 gateway servers to the list.

   - In the blank row of the table, click and then type the host or domain name.
   - To allow a domain and all its sub-domains, use a wildcard character at the beginning of the domain name.
     For example, `*.mycompany.com`

   - Repeat the previous two bulleted steps for each name to be added.
   - Click **OK**.

IBM Cognos Application Firewall validates domain and host names to protect URLs that are created. By default, IBM Cognos Application Firewall considers domain names derived from the environment configuration properties to be safe domain names. Adding names to the list of valid names and hosts is useful when you need to redirect requests to non-IBM Cognos computers using the Back or Cancel functions or when using drill-through to different IBM Cognos product installations.

6. Save the configuration.
7. Restart the services.

### Encrypt Temporary File Properties

Temporary files are used in IBM Cognos BI to store recently viewed reports and to store data used by the services during processing. You can change the location of the temporary files and you can choose to encrypt their content.

By default, IBM Cognos components store temporary files in the `c10_location\temp` directory and the files are not encrypted.

For optimum security, deny all access to the temp directory, except for the service account used to start the IBM Cognos services. Read and write permissions are required for the service account.

**Procedure**

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, for the **Temporary files location** property, specify the new location.
4. If you require the content of temporary files to be encrypted, set the **Encrypt temporary files** property to **True**.
5. Ensure that the user account under which IBM Cognos BI components run have the appropriate privileges to the temporary files location. For example:
   - on Microsoft Windows operating systems, full control privileges
on UNIX or Linux operating systems, read-write privileges

**Configure the Gateway to Use a Namespace**

If IBM Cognos components use multiple namespaces, or if anonymous access is enabled and IBM Cognos components use one namespace, you can configure the gateway to connect to one namespace. Users logged onto the Web server where the gateway is located are not prompted to choose an authentication source. For example, if you have two Web servers, you can configure each Web server to use a different namespace.

**Procedure**

1. On the computer where the gateway is located, start IBM Cognos Configuration.
2. In the Explorer window, click Environment.
3. In the Properties window, in the Value box next to the Gateway namespace property, type the Namespace ID of the namespace that you want to use.
4. From the File menu, click Save.
5. Restart your Web server.

**Enable and Disable Services**

In a distributed installation, you can send certain types of requests to specific computers by enabling or disabling the installed services.

For example, to dedicate a computer to running and distributing reports, you can disable the presentation service on an Application Tier Components computer. To dedicate a computer in a distributed installation to processing Metric Studio application requests, disable the Data Integration Service on the computer.

**Note:** The default values for dispatcher service and presentation service are false on computers that only have Content Manager installed. On all other types of installations, the default values are true.

If you installed all components on several computers, you can disable appropriate services on each computer to get the distributed configuration you require. Requests are only sent to dispatchers where a given service is enabled.

Disabling a service prevents the service from loading into memory. When disabled, services do not start and therefore do not consume resources. The service does not run until you enable it.

If you disable the dispatcher service, the dispatcher-related services are disabled. Only dispatcher services that are enabled can process requests.

**Enabling and disabling services**

Use the following procedure to disable selected services on components in a distributed installation.

**Procedure**

1. Start IBM Cognos Configuration.
2. In the Explorer window, under Environment, click IBM Cognos services.
3. In the Properties window, click the Value next to the service that you want to disable or enable.
   By default, all services are enabled.
4. Click the appropriate state for the services:
   - To disable the service, click False.
   - To enable the service, click True.

5. From the File menu, click Save.

Configuring fonts

IBM Cognos components use fonts to render PDF reports on the IBM Cognos server. IBM Cognos components also use fonts to render charts used in PDF and HTML reports.

To show output correctly, fonts must be available where the report or chart is rendered. For charts and PDF reports, the fonts must be installed on the IBM Cognos server. If a requested font is not available, IBM Cognos components substitute a different font.

Because HTML reports are rendered on a browser, the required fonts must be installed on the computer of each IBM Cognos user who views the report. If a requested font is not available, the browser substitutes a different font.

Use the following checklist if you want to use a new font in your reports.

- **Add the font to the list of supported fonts**
- **Specify the file location of the new font**
- **Map the new font to the physical font name** if required.

Considerations to support Simplified Chinese

IBM Cognos BI products support the GB18030-2000 character set, which is used in the encoding of Simplified Chinese locales.

If you install on Microsoft Windows, support is provided for the GB18030-2000 character set in the SimSun-18030 font that is provided by Microsoft.

On operating systems other than Windows, you must install a font that supports GB18030-2000.

Add Fonts to the IBM Cognos Environment

You can add fonts to the list of supported fonts in your IBM Cognos environment if you want to generate reports that use fonts that are currently not available. You can also remove fonts. By default, IBM Cognos components use a set of global fonts, which are available on all IBM Cognos server computers.

**Procedure**

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the Actions menu, click Edit Global Configuration.
3. Click the Fonts tab.
4. Click Add.

   **Tip:** To remove a font from the list of supported fonts, click the box next to the font name and then click Remove.

5. In the Supported Font Name box, type the font name and then click OK.
6. From the File menu, click Save.
All global fonts, including new fonts that you add, must be installed on all IBM Cognos computers in your environment.

Results

If a global font is not installed on all IBM Cognos computers, you must map the global font to an installed, physical font.

Specify the Location of Available Fonts

You must specify the installation location of all fonts, including fonts that you add to the list of supported fonts.

By default, the list of fonts consists of fonts installed in the \c10_location\bin\fonts directory of the IBM Cognos computer. If IBM Cognos components are installed on a Microsoft Windows operating system computer, they also use the fonts installed in the Windows font directory.

You specify the font location on all computers where Application Tier Components are installed.

Procedure

1. On each Application Tier Components computer, start IBM Cognos Configuration.
2. In the Explorer window, click Environment.
3. In the Properties window, for the Physical fonts locations property, specify the location of the fonts.
   - If there are multiple font paths, separate each path by a semicolon (;).
   - If you are using an application server other than Tomcat, type the fully qualified path to the font location. For example: \c10_location\bin\fonts.
4. From the File menu, click Save.

Map Supported Fonts to Installed Fonts

You can substitute global fonts, which are not installed on the computer, for physical fonts.

You map fonts on each computer where the Application Tier Components are installed.

For example, you add a font to the list of supported fonts that is not installed on the IBM Cognos computer. You can specify which font to use as a substitute.

If you want to print reports faster by using the built-in PDF fonts, you can map a global font such as Arial to one of the built-in PDF fonts, such as Helvetica-PDF, using the following steps. You can also select one of the built-in PDF fonts for a text object in Report Studio or Query Studio. For more information, see the Query Studio User Guide or the Report Studio User Guide.

No mapping is required if you add a font to the supported font list that is installed on IBM Cognos computers. However, you must specify the location of the font.

Procedure

1. On each Application Tier Components computer, start IBM Cognos Configuration.
2. In the Explorer window, click Environment.
3. In the **Properties** window, click the **Value** box next to the **Physical fonts map** property, and then click the edit icon.

   The **Value - Physical fonts map** dialog box appears.

4. Click **Add**.

   **Tip:** To remove a font, select the check box next to the font and click **Remove**.

5. In the **Global Font Name** box, type the name of the font you added to the supported font list.

6. Click the **Physical Font Name** box.

7. If you know the physical font name, type it. Otherwise, click the edit icon.

   In the **Physical Font Name** dialog box, click **Search Now** and then click a font name from the results.

8. Repeat steps 4 to 7 for each global font that requires mapping.

9. Click **OK**.

10. From the **File** menu, click **Save**.

### Results

Now, if required, you must specify the installation location of the fonts.

### Change the default font for PDF reports

You can change the default font that IBM Cognos BI components use for PDF reports. You see this default font when you open a report.

You change the default font on the computer where Content Manager is installed. The font then becomes the default for all computers in your installation. You change the font used for PDF reports using IBM Cognos Configuration.

Ensure that the default font is installed on all computers in your IBM Cognos installation.

To ensure that GB18030 characters are displayed correctly in PDF reports, set the default font to SimSun-GB18030.

### Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **General** tab.
4. In the **Value** box, for **Default font**, type the font you want to use as the default for reports.
5. Click **OK**.
6. From the **File** menu, click **Save**.
7. On all Application Tier Components computers, ensure that the installation location of the default font is specified in the **Physical fonts locations** property (under **Environment** in the **Explorer** window) or that the font is in the Windows font directory.
Configure Embedded Fonts for PDF Reports

When a PDF report opens in Adobe Reader, all the fonts used in that report must be available. Fonts must be either embedded in the report or installed on the user’s computer. If a font is not available in either of these locations, Adobe Reader tries to substitute an appropriate font. This substitution may cause changes in the presentation of the report or some characters may not be displayed.

To ensure that PDF reports appear correctly in Adobe Reader, IBM Cognos BI embeds required fonts in reports by default. To minimize the file size, IBM Cognos BI embeds only the characters (also called glyphs) used in the report rather than all characters in the font set. IBM Cognos BI embeds fonts only if they are licensed for embedding. The license information is stored in the font itself and is read by IBM Cognos BI.

If you are confident that the fonts used in reports are available on users’ computers, you can limit or eliminate embedded fonts to reduce the size of PDF reports. When limiting fonts, you specify whether a font is always or never embedded, using an embedded fonts list in IBM Cognos Configuration.

Procedure

1. On the Content Manager computer, start IBM Cognos Configuration.
2. In the Explorer window, click Environment.
3. In the Properties window, under Font Settings, click the value for Fonts to embed (Batch report service) or Fonts to embed (Report service), and then click the edit icon.
4. If you are not using the default fonts directory or if you want to add a path to an additional directory, in the Fonts to Embed in PDF Reports dialog box, specify the new path in the font paths box.
   Tip: Click Search Now to get a list of the available fonts in the specified path or paths.
5. For a font that will always be available on users’ computers, scroll to the font name, and click the Never check box.
   IBM Cognos BI does not embed the font with any reports. Adobe Reader picks up the font from the user’s computer when the report is opened.
6. For a font that may not always be available on the users’ computers, scroll to the font name and click the Always check box.
   IBM Cognos BI embeds the font with all reports that use it. Adobe Reader uses the embedded font when the report is opened.
7. Click OK.

Saved Report Output

By default, report output files are saved in the content store. You have the option of saving a copy of the report output in another file location that is outside or inside IBM Cognos BI. If you use this option, a descriptor file with an _descr extension is also saved. Saved files are not managed by IBM Cognos BI.

Save Report Output Outside IBM Cognos BI

If you configure a file system location that is outside of IBM Cognos BI, you can then share the report output with external applications or people who don’t have IBM Cognos BI. This is how most report output files are saved.
To use this feature, you must first configure a root directory in IBM Cognos Configuration. An administrator must then set the file location in IBM Cognos Administration. For more information, see the topic about setting a file location for report output saved outside of IBM Cognos BI, in the IBM Cognos Business Intelligence Administration and Security Guide.

**Procedure**

1. Create a directory for your file system.
   - **Tip:** Ensure that the directory is accessible to users and separate from the installation directory. For example, in a distributed installation on Microsoft Windows, an archive folder such as `\servername\directory` could be used.

2. On the Content Manager computer, start IBM Cognos Configuration.
3. From the **Actions** menu, click **Edit Global Configuration**.
4. In the **Global Configuration** window, click the **General** tab.
5. For **Archive Location File System Root**, type a URI using the format
   ```text
   file://directory
   ```
   where `directory` is the directory that you created in step 1.
   The `file://` portion of the URI is required. Windows UNC names, such as `\servername\directory`, can be used. If so, the URI must be formatted as follows:
   ```text
   file://\servername\directory
   ```
   - **Tip:** Ensure that you do not use a mapped drive when running Cognos as a Microsoft Windows service.

6. To confirm that the correct location will be used, click **Test**.
7. Click **OK**.
8. From the **File** menu, click **Save**.

**Results**

The administrator must now configure the file location. For information, see the topic about setting a file location for report output saved outside of IBM Cognos BI, in the IBM Cognos Business Intelligence Administration and Security Guide.

**Save Report Output Inside IBM Cognos BI**

If you configure a file system location that is inside IBM Cognos BI, you can then use the report output again. This may also be useful for archive purposes, because files that are saved in the Content Store may be deleted regularly due to retention rules.

To use this feature, you must first enable the **Save report outputs to a file system** property in IBM Cognos Configuration. An administrator must then configure the file location using the `CM.OutPutLocation` parameter in IBM Cognos Administration. For more information, see the topic about setting a file location for report output saved inside IBM Cognos BI, in the IBM Cognos Business Intelligence Administration and Security Guide.

To protect the security of the report output when using this feature, the file system must have third-party encryption.
**Procedure**

1. Create a directory for your file system.

   **Tip:** Ensure that the directory is accessible to authorized users only.

2. On the Content Manager computer, start IBM Cognos Configuration.

3. In the **Explorer** window, click **Data Access > Content Manager**.

4. For the **Save report outputs to a file system** property, click **True**.

5. To test the connection to the report output directory, from the **Actions** menu, click **Test**.

6. From the **File** menu, click **Save**.

**Results**

The administrator must now configure the file location using the 
**CM.OutPutLocation** parameter. For information, see the topic about setting a file 
location for report output saved inside IBM Cognos BI, in the *IBM Cognos Business 
Intelligence Administration and Security Guide*.

**Changing the Location of Temporary Report Output**

When users run interactive reports, the report output is stored in Content Manager or in a temporary session cache in the local report file system. You can change the location of the temporary session cache to a remote computer such as a shared directory on a Microsoft Windows based system or a common mounted directory on a UNIX or Linux based system.

By default, the location of the temporary session cache on the report file system is 
`c10_location/temp/Session`. The Session directory is created by the report server when the first request from a user session is received.

To configure whether the temporary report output is stored in Content Manager or in the local report file system, see the topic about storing user session files on a local report file system in the *IBM Cognos Business Intelligence Administration and Security Guide*.

**Procedure**

1. On the computer where Application Tier Components are installed, start IBM Cognos Configuration.

2. In the **Explorer** window, click **Environment**.

3. In the **Properties** window, click the value for **Temporary files location**, and then click the edit icon.

4. In the **Select Folder** dialog box, use the **Save in** box to locate the computer and directory, and then click **Select**.

5. From the **File** menu, click **Save**.

   When a user runs an interactive report session, the temporary report output is now stored in the new location.
Use an external object store for report output

You can configure Content Manager to store report output to a local drive or network share by defining an external object store. Report output is available through IBM Cognos Connection and IBM Cognos SDK, but the report output is not stored in the content store database.

Using an external object store for report output reduces the size of the content store and provides performance improvements for Content Manager.

Before you begin

Ensure that you do the following before you create an external object store connection.

- Provide Content Manager computers with access to the file location of the external object store.
- Provide the user account that runs the IBM Cognos service with read and write access to the file location.
- Create the content store.

Procedure

1. Start IBM Cognos Configuration.
2. In the Explorer window, under Data Access > Content Manager, right-click the name of your Content Store, and then click New resource > External Object Store.
3. In the New Resource - External Object Store window, type a unique name for your file system repository, and click OK.
   
   You can have only one external object store.
4. Click the name for the repository.
5. In the External Object Store - Resource Properties window, click inside the value field, click edit, and when the URI values window opens, type the path to your file system location, where file-system-path is the full path to an existing file location.

   Table 48. Examples of URI values

<table>
<thead>
<tr>
<th>File system</th>
<th>URI value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>file:///c:/file-system-path</td>
</tr>
<tr>
<td></td>
<td>file://host/share/file-system-path</td>
</tr>
<tr>
<td>UNIX or Linux</td>
<td>file:///file-system-path</td>
</tr>
</tbody>
</table>

   Note: Relative paths, such as file:///../file-system-path and drive mappings are not supported.

   In a distributed installation, all Content Managers must have read and write access to the file system location. To improve performance when reading outputs, Application Tier Components, essentially the repository service, should have read access to the file system location. If they do not have read access, requests are routed to the active Content Manager.
6. Restart the IBM Cognos service.
Verify access to the external object store

Use IBM Cognos Configuration to verify that IBM Cognos components can connect to the external object store.

Procedure

1. Start IBM Cognos Configuration.
2. From Explorer > Data Access, right-click the name of your external object store connection.
3. Click Test.
   IBM Cognos Configuration verifies access to the external object store file location.
   You can also test this connection by right-clicking Local Configuration and selecting Test.

Customizing Server-side Printing for UNIX and Linux Platforms

The way in which the IBM Cognos Connection portal handles server printing can differ depending on your platform.

For this reason, you can customize the way in which the IBM Cognos Connection portal handles the printing of PDF format reports for UNIX and Linux platforms by configuring the rsprintpdf.sh file.

The rsprintpdf.sh file should not be configured for Microsoft Windows operating system print servers.

When a user selects Run with Options, changes the Format to PDF, selects Print the Report from the Delivery section, and then specifies additional formats through advanced options such as Landscape orientation, A4 paper size or a Time and Mode to run the report, problems might occur when printing to a UNIX or Linux print server. The output might not be generated, or it might appear cropped or incorrectly orientated.

Procedure

1. Open the rsprintpdf.sh file located in the c10_location/bin directory.
2. In a text editor, customize the section that is specific to your print server’s platform, for example AIX, HP-UX, or Linux.
3. Use the following information for customization. The information is passed to the rsprintpdf.sh script by the server process as command line options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p</td>
<td>printer</td>
<td>Specifies the print queue. If no print queue is specified, the default queue is used.</td>
</tr>
<tr>
<td>-o</td>
<td>orientation</td>
<td>Specifies the page orientation for a file, for example landscape or portrait. If no orientation is specified, portrait orientation is used.</td>
</tr>
</tbody>
</table>
Table 49. Customization options for the printing of PDF format reports (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-m</td>
<td>media</td>
<td>Specifies the media size of the output, for example letter or A4 paper size. If no media, or no height or width are specified, the default paper tray is used.</td>
</tr>
<tr>
<td>-h</td>
<td>height</td>
<td>For custom page sizes. Specifies the height of the page in points. It is valid only if specified with the -w option, and without the -m option.</td>
</tr>
<tr>
<td>-w</td>
<td>width</td>
<td>For custom page sizes. Specifies the width of the page in points. It is valid only if specified with the -h option, and without the -m option.</td>
</tr>
<tr>
<td>-L</td>
<td>log file</td>
<td>Specifies a path to a user-specified file for logging error messages. The default filename for the log file is rsprintpdf.errors.log.</td>
</tr>
</tbody>
</table>

4. **Tip**: Keep a copy of the rsprintpdf.sh file in case it should be overwritten by a future software upgrade.

---

**Change the notification database**

By default, the notification server uses the same database that Content Manager uses for the content store. You can use a separate database for notification in situations where you run large volumes of batch reports and email.

Using a separate database for notification involves the following tasks:

- **Creating a notification database.**
  - For DB2, Oracle, Microsoft SQL Server, or Sybase, use the same procedure that was used to create the content store database. Use the instructions in "Guidelines for creating the content store" on page 27.

  **Note**: If you are using DB2, you cannot generate a script to create the notification database in the same way as you can the content store.

- **Setting up the database connectivity.**
  - You can use the same procedure as to set the connectivity for the content store database, "Set up database connectivity for the content store database" on page 60.

- **Changing the connection properties for the notification database.**

  Use the instructions in "Change the Connection Properties for the Notification Database" on page 203.
Change the Connection Properties for the Notification Database

After you create a separate database for notification, you must configure IBM Cognos components to use the new database.

You must configure all Content Managers and Application Tier Components to use the same notification database.

Procedure

1. In the Explorer window, under Data Access, click Notification.
2. From the File menu, click Save.
3. Test the notification. In the Explorer window right-click Notification and click Test.
   This tests the database connection and the mail server connection.
   If you have been using the content store database for notification, the schedules will be replicated in the tables of the new notification database.

Create a New Content Store Using Cognos Content Database

Use the following steps to create another content store database using the Cognos Content Database. This might be required if you install more than one instance of your IBM Cognos product in the test location and you want to run the instances separately.

Before you begin

Only use Cognos Content Database for test or demonstration purposes. Cognos Content Database gets a test system running quickly. When moving to a production environment with your IBM Cognos product, set up the content store to use a supported database that can be secured and tuned for performance.

Before you create the new content store, do the following:

• Install the additional instance of your IBM Cognos wsproduct in a separate directory on the same computer.
  Ensure that you select Cognos Content Database on the Component Selection page of the installation wizard.
• Create a new user and password for the new content store database.

Procedure

1. In the location where you installed the new instance of Cognos Content Database, in the c10_location/derby10.1.2.1/bin directory, use the ij.bat or ij.ksh script to create a new database.
   Use the following syntax:
   `connect 'jdbc:derby://host:port/db_name;create=true;user=username;password=password';`
   Ensure that you use a different name, user, and password for the new content store.
   For example, to create a database named contentstore2 on the localhost computer on port number 1527 as a user named cognos2 with a password of cognos2, you would type
   `connect 'jdbc:derby://localhost:1527/contentstore2;create=true;user=cognos2;password=cognos2';`
The database name is case-sensitive.
The database files are located in the c10_location\contentstore directory.

2. When you are finished with the ij utility, disconnect by using the following command:
   disconnect;

Change the security standard compliance for IBM Cognos trust stores

By default, the IBM Cognos version 10.2.1 trust stores that are used for SSL communications include only certificates that are qualified for the NIST SP800-131a standard. You can change the certificates available to you by using the ThirdPartyCertificateTool.

You can add non-NIST SP800-131a standards and you can also remove the non-NIST SP800-131a standards you have added.

Restore non-NIST SP800-131a standard certificates to IBM Cognos trust stores

By default, the IBM Cognos version 10.2.1 trust stores includes only certificate authority (CA) certificates that are qualified for the NIST SP800-131a standard. If you use other certificates, such as SHA1 or 1024-bit CA certificates, you must add these certificates to the trust store individually. Or, you add these certificates from the trust store of the JRE you are using with the ThirdPartyCertificateTool restore command.

Note: The examples in this task use the default password, NoPassWordSet. If you change the Signing key store password, the Encryption key store password, and the Certificate Authority key store password in IBM Cognos Configuration, ensure you use the password that you set.

Before you begin

On UNIX or Linux operating systems, ensure that you set a JAVA_HOME environment variable before you use the ThirdPartyCertificateTool.

On Microsoft Windows installations, you can run the tool with -java:local to use the JRE that is provided with the installation. For example, ThirdPartyCertificateTool.bat -java:local -R -D ...

Procedure

1. Go to the c10_location\bin directory.
2. Restore the non-NIST SP800-131a standard certificates by typing the following command:
   On UNIX or Linux operating systems, type
   ThirdPartyCertificateTool.sh -R -D ../configuration -p NoPassWordSet
   On Windows operating systems, type
   ThirdPartyCertificateTool.bat -R -D ..\configuration -p NoPassWordSet
Remove non-NIST SP800-131a standard certificates from the IBM Cognos trust stores

If you have added non-NIST SP800-131a certificates to the IBM Cognos trust stores, such as SHA1 or 1024-bit CA certificates, you can remove those certificates with the ThirdPartyCertificateTool.

Note: The examples in this task use the default password, NoPassWordSet. If you change the Signing key store password, the Encryption key store password, and the Certificate Authority key store password in IBM Cognos Configuration, ensure you use the password that you set.

Before you begin

On UNIX or Linux operating systems, ensure that you set a JAVA_HOME environment variable before you use the ThirdPartyCertificateTool.

On Microsoft Windows installations, you can run the tool with -java:local to use the JRE that is provided with the installation. For example,

ThirdPartyCertificateTool.bat -java:local -N -D ...

Procedure

1. Go to the c10_location\bin directory.
2. Type the following command:
   On UNIX or Linux operating systems, type
   ThirdPartyCertificateTool.sh -N -D ../configuration -p NoPassWordSet
   On Windows operating systems, type
   ThirdPartyCertificateTool.bat -N -D ..\configuration -p NoPassWordSet

Configuring IBM Cognos components to use another certificate authority

By default, IBM Cognos BI components use their own certificate authority (CA) service to establish the root of trust in the IBM Cognos security infrastructure. However, you can configure IBM Cognos components to use a certificate from another certificate authority, such as iPlanet or Microsoft.

To use another CA certificate, you must use the following process:

1. “Create certificate signing request (CSR) files” on page 206
   Part of this task requires you to submit the CSRs to your certificate authority and generate the certificates. For more information about that process, see your CA documentation.
2. “Import the CA certificates into IBM Cognos components” on page 208
3. “Configure IBM Cognos BI Components to use certificates generated by your CA” on page 210

Some tasks use a command-line tool named ThirdPartyCertificateTool. The following tables list the options for this command-line tool.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>Creates a CSR</td>
</tr>
</tbody>
</table>
Table 50. Main operation mode (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i</td>
<td>Imports a certificate</td>
</tr>
</tbody>
</table>

Table 51. Operation modifiers

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td>Work with the signing identity</td>
</tr>
<tr>
<td>-e</td>
<td>Work with the encryption identity</td>
</tr>
<tr>
<td>-T</td>
<td>Work with the trust store (only with -i)</td>
</tr>
</tbody>
</table>

Table 52. Information flags

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>DN to use for certificate</td>
</tr>
<tr>
<td>-r</td>
<td>CSR or certificate file location (depends on mode)</td>
</tr>
<tr>
<td>-t</td>
<td>Certificate authority certificate file (only with -i)</td>
</tr>
<tr>
<td>-p</td>
<td>Key store password</td>
</tr>
<tr>
<td>-a</td>
<td>Key pair algorithm: either RSA or DSA. RSA is the default value.</td>
</tr>
<tr>
<td>-D</td>
<td>Directory location</td>
</tr>
</tbody>
</table>

The sample values from the following table are used:

Table 53. Sample values

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signing certificate distinguished name (DN)</td>
<td>A unique value, formatted as:</td>
</tr>
<tr>
<td></td>
<td>CN=SignCert,O=MyCompany,C=CA</td>
</tr>
<tr>
<td>Encryption certificate DN</td>
<td>A unique value, formatted as:</td>
</tr>
<tr>
<td></td>
<td>CN=EncryptCert,O=MyCompany,C=CA</td>
</tr>
<tr>
<td>Key store password</td>
<td>The default password: NoPassWordSet</td>
</tr>
</tbody>
</table>

This value must match the passwords in IBM Cognos Configuration under Security > Cryptography > Cognos. If you change the default values for Signing key store password, Encryption key store password, and Certificate Authority key store password, ensure you use the passwords that you set.

Create certificate signing request (CSR) files

To obtain a certificate from a certificate authority (CA), you must first generate certificate signing request (CSR) files for the signing keys and encryption keys from the IBM Cognos keystores. The CA uses these files to produce a signing certificate, an encryption certificate, and a CA certificate that you import into your keystores.
Note: The examples in this task use the default password, **NoPassWordSet**. If you change the **Signing key store password**, the **Encryption key store password**, and the **Certificate Authority key store password** in IBM Cognos Configuration, ensure you use the password that you set.

**Before you begin**

On UNIX or Linux operating systems, ensure that you set a JAVA_HOME environment variable before you use the **ThirdPartyCertificateTool**.

On Microsoft Windows installations, you can run the tool with **-java:local** to use the JRE that is provided with the installation. For example,

`ThirdPartyCertificateTool.bat -java:local -c -s -d ...`

**Procedure**

1. Back up your key data:
   a. Go to the `c10_location\configuration` directory.
   b. Back up the `cogstartup.xml` file to a secure location.
   c. Back up the contents of the following directories to a secure location:
      * `c10_location\configuration\signkeypair`
      * `c10_location\configuration\encryptkeypair`

2. Go to the `c10_location\bin` directory.

3. Create the certificate signing request for the signing keys by typing the following command:
   On UNIX or Linux operating systems, type
   ```bash
   ThirdPartyCertificateTool.sh -c -s -d "CN=SignCert,O=MyCompany,C=CA" -r signRequest.csr -D ../configuration/signkeypair -p NoPassWordSet
   ```
   On Microsoft Windows operating system, type
   ```bat
   ThirdPartyCertificateTool.bat -c -s -d "CN=SignCert,O=MyCompany,C=CA" -r signRequest.csr -D ..\configuration\signkeypair -p NoPassWordSet
   ```
   The distinguished name (DN) value in the command ("CN=SignCert,O=MyCompany,C=CA") uniquely identifies the IBM Cognos installation. The attributes that are used reflect a hierarchical structure in your organization.
   The password that you enter for this key must be used again when import the certificate and again in IBM Cognos Configuration.
   You can safely ignore any warnings about logging.
   The command creates the jSignKeystore file in the signkeypair directory, sets the specified password, creates a keypair, stores it in the keystore, and exports the signRequest.csr file to the c10_location\bin directory.

4. Create the certificate signing request for the encryption keys by typing the following command:
   On UNIX or Linux, type
   ```bash
   ```
   On Windows, type
   ```bat
   ThirdPartyCertificateTool.bat -c -e -d "CN=EncryptCert,O=MyCompany,C=CA" -r encryptRequest.csr -D ..\configuration\encryptkeypair -p NoPassWordSet
   ```
The distinguished name (DN) value in the command
("CN=SignCert, O=MyCompany, C=CA") uniquely identifies the IBM Cognos
installation. The attributes that are used reflect a hierarchical structure in your
organization.

The password that you enter for this key must be used again when import the
certificate and again in IBM Cognos Configuration.

You can safely ignore any warnings about logging.

The command creates the jEncKeystore file in the encryptkeypair directory,
sets the specified password, creates a keypair, stores it in the keystore, and
exports the encryptRequest.csr file to the c10_location\bin directory.

5. Copy the signRequest.csr and encryptRequest.csr files to a directory that is
accessible by your certificate authority.

6. Input the signRequest.csr and encryptRequest.csr files into the certificate
authority, and generate the certificates.

The certificate authority produces a signing key certificate, an encryption key
certificate, and a CA certificate.

Important: The certificates that are generated by your CA must be PEM
(Base-64 encoded ASCII) format.

Results

You can now import the generated certificates into your IBM Cognos components
in the following task.

Import the CA certificates into IBM Cognos components

After you obtain the certificates from the CA, you must import them to your IBM
Cognos components.

You must import the certificates on each computer where you have IBM Cognos
components installed; including Content Manager, the Application Tier
Components, the gateway, and the modeling components.

Note: The examples in this task use the default password, NoPassWordSet. If you
change the Signing key store password, the Encryption key store password, and
the Certificate Authority key store password in IBM Cognos Configuration,
ensure you use the password that you set.

Before you begin

On UNIX or Linux operating systems, ensure that you set a JAVA_HOME
environment variable before you use the ThirdPartyCertificateTool.

On Microsoft Windows installations, you can run the tool with -java:local to use
the JRE that is provided with the installation. For example,
ThirdPartyCertificateTool.bat -java:local -c -s -d ...

Procedure

1. Create a copy of the signing certificate file and name it signCertificate.cer.
2. Create a copy of the encryption certificate and name it encryptCertificate.cer.
3. Create a copy of the root CA certificate and name it ca.cer.
4. Copy the signCertificate.cer, encryptCertificate.cer, and ca.cer files to the c10_location/bin directory.

5. Import the signing certificate into the IBM Cognos signing key store by typing the following command:
   
   **On UNIX or Linux operating systems, type**
   
   ```bash
   ThirdPartyCertificateTool.sh -i -s -r signCertificate.cer -D
   ../configuration/signkeypair -p NoPassWordSet -t ca.cer
   ```
   
   **On Windows operating systems, type**
   
   ```bat
   ThirdPartyCertificateTool.bat -i -s -r signCertificate.cer -D
   ..\configuration\signkeypair -p NoPassWordSet -t ca.cer
   ```
   
   **Important:** Ensure you use the password that you entered when you exported the signing key in the previous task.

   You can safely ignore any warnings about logging.

   The command reads the signCertificate.cer and ca.cer files in the c10_location/bin directory and imports the certificates from both files into the jSignKeystore file in the signkeypair directory using the specified password.

6. Import the encryption certificate into the IBM Cognos encryption key store by typing the following command:
   
   **On UNIX or Linux operating systems, type**
   
   ```bash
   ThirdPartyCertificateTool.sh -i -e -r encryptCertificate.cer -D
   ../configuration/encryptkeypair -p NoPassWordSet -t ca.cer
   ```
   
   **On Windows operating systems, type**
   
   ```bat
   ThirdPartyCertificateTool.bat -i -e -r encryptCertificate.cer -D
   ..\configuration\encryptkeypair -p NoPassWordSet -t ca.cer
   ```
   
   **Important:** Ensure you use the password that you entered when you exported the encryption key in the previous task.

   You can safely ignore any warnings about logging.

   The command reads the encryptCertificate.cer and ca.cer files in the c10_location/bin directory and imports the certificates from both files into the jEncKeystore file in the encryptkeypair directory using the specified password.

7. Import the CA certificate into the IBM Cognos trust store by typing the following command:
   
   **On UNIX or Linux operating systems, type**
   
   ```bash
   ThirdPartyCertificateTool.sh -i -T -r ca.cer -D ../configuration/
   signkeypair -p NoPassWordSet
   ```
   
   **On Windows operating systems, type**
   
   ```bat
   ThirdPartyCertificateTool.bat -i -T -r ca.cer -D ..\configuration\signkeypair -p NoPassWordSet
   ```

   The command reads the ca.cer file and imports the contents into the jCAKeystore file in the signkeypair directory using the specified password.

**Results**

You can now configure your IBM Cognos components to use your CA certificates.
Configure IBM Cognos BI Components to use certificates generated by your CA

After you import the CA certificates, you use IBM Cognos Configuration to configure each computer where an IBM Cognos component is installed to use the certificate.

**Note:** Ensure that the key store locations and passwords in IBM Cognos Configuration match the ones that you typed in the command-line tool. For example, if you change the Signing key store password, the Encryption key store password, and the Certificate Authority key store password in IBM Cognos Configuration, ensure you use the password that you set.

**Procedure**

1. Start IBM Cognos Configuration.
2. In the Explorer window, under Security > Cryptography, click Cognos.
3. Click the Value box next to Use third party CA, and select True. When you set this property to true, all properties for the certificate authority and identity name are ignored.
4. Enter the password that you used for the signing key in Signing key store password, and enter the path for the Signing key store location. If you used the same values in the examples in the previous tasks, you do not have to change the path.
5. Enter the password that you used for the encryption key in Encryption key store password, and enter the path for the Encryption key store location. If you used the same values in the examples in the previous tasks, you do not have to change the path.
6. Enter the Certificate Authority key store password.
7. Click File > Save.
8. Restart your IBM Cognos services.

Configuring the SSL protocol for IBM Cognos components

You can use the Secure Sockets Layer (SSL) protocol for communication between IBM Cognos components in single server and distributed installations.

**Tomcat connectors**

If the internal dispatcher URI is prefixed with http but the external dispatcher URI is prefixed with https, or vice versa, both the non-SSL Coyote HTTP/1.1 and SSL Coyote HTTP/1.1 connectors are enabled in the server.xml file.

If the internal and external dispatcher URIs use different protocols or ports, the internal dispatcher port is accessible only to the components on the local computer. The internal dispatcher URI must also specify localhost.

**Single computer installations**

In a single computer installation, if you are not currently using SSL, you must stop the service before changing the protocol to https. After you save the configuration with SSL settings, you can restart the services.
Distributed installations

In distributed installation, you must first configure the default active Content Manager computer to use the SSL protocol and start the services on that computer before you configure the Application Tier and gateway components to use SSL.

Add a computer to an installation

If you add a computer to an SSL-enabled environment, you will be prompted to temporarily accept trust for a certificate when you save the configuration. Accepting the temporary certificate will allow permanent trust to be established with the existing components.

Add a component to a computer

If you add a component to an installation that has already been configured for SSL, the trust to the SSL certificates is inherited from the existing components. If you add the component to a different location on the same computer but to an environment already configured for SSL, you will be prompted to temporarily accept trust for a certificate when you save the configuration. Accepting the temporary certificate will allow permanent trust to be established with the existing components.

Configure SSL for IBM Cognos components

For IBM Cognos components, you can use SSL for internal connections, external connections, or both.

If you configure SSL for internal connections only, IBM Cognos components on the local computer will communicate using this protocol. The dispatcher listens for secure connections on a different port than for remote, HTTP requests. Therefore, you must configure two dispatcher URIs.

If you configure SSL for external connections only, communications from remote IBM Cognos components to the local computer will use the SSL protocol. You must configure the dispatcher to listen for secure, remote requests on a different port than local, HTTP requests. You must also configure the Content Manager URIs and the dispatcher URI for external applications to use the same protocol and port as the external dispatcher.

If you configure SSL for all connections, the dispatcher can use the same port for internal and external connections. Similarly, if you do not use SSL for local or remote communication, the dispatcher can use the same port for all communications.

By default, IBM Cognos BI components use an internal certificate authority (CA) to establish the root of trust in the IBM Cognos security infrastructure. This applies to both SSL and non-SSL connections. If you want to use certificates managed by another service, see "Configuring IBM Cognos components to use another certificate authority" on page 205.

In distributed installation, you must first configure the default active Content Manager computer to use the SSL protocol and start the services on that computer before you configure the Application Tier Components computer.
**Procedure**

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, type the appropriate values for the URI values:
   - To configure SSL for internal connections only, enter **https** and a port number for SSL communication in the **Internal dispatcher URI** property.
     For the **External dispatcher URI** and **Dispatcher URI for external applications** properties, leave **http** as the protocol and use the default or another available port number.
     If you use Tomcat, the **Internal dispatcher URI** property must specify **localhost**.
     The port number in the two dispatcher URIs must be different.
   - To configure SSL for external connections only, enter **https** and a port number for SSL communication in the **External dispatcher URI** and **Dispatcher URI for external applications** properties.
     For the **Internal dispatcher URI** property, leave **http** as the protocol and use the default or another available port number.
     If you use Tomcat, the **Internal dispatcher URI** property must specify **localhost**.
     The port numbers in the two dispatcher URIs must be different.
   - To configure SSL for all connections, enter the same URI for both the **Internal dispatcher URI**, **External dispatcher URI**, and **Dispatcher URI for external applications** properties. Enter **https** and a port number for SSL communication.
     Additionally, you can enter **https** and a port number for SSL communication in the **Content Manager URI** property.
     If you have installed the gateway on a separate computer, and you are using SSL for external connections, in IBM Cognos Configuration on the gateway computer, enter **https** and the port number for SSL communication in the **Dispatcher URIs for gateway** property.
4. From the **File** menu, click **Save**.
5. Restart your services.

   In a distributed environment, start the services on the Content Manager computer first, followed by the services on the Application Tier Components computers.

**Set up shared trust between IBM Cognos servers and other servers**

If you want to use the default IBM Cognos certificate authority and you want to use SSL for connections from other servers to IBM Cognos servers, you must add the IBM Cognos certificate to the trust store on the other servers.

**Note:** If you use browsers to connect to IBM Cognos components, the browsers automatically prompt users to update their trust stores.

If you want the connection between IBM Cognos servers and the other server to be mutually authenticated, you must also copy the certificate from your certificate authority to the trust store for IBM Cognos servers.
If you have configured IBM Cognos components to use another certificate authority (CA), you do not have to set up shared trust between IBM Cognos server and other servers.

**Copying the IBM Cognos certificate to another server**

The first task in adding the IBM Cognos certificate to the trust store on other servers is to copy the certificate to the server.

**Procedure**

1. Go to the `c10_location/bin` directory.
2. Extract the IBM Cognos certificate by typing the following command:
   - On UNIX or Linux operating systems, type
     ```
     ThirdPartyCertificateTool.sh -E -T -r destination_file -k
c10_location/configuration/signkeypair/jCAKeystore -p NoPasswordSet
     ```
   - On Microsoft Windows operating systems, type
     ```
     ThirdPartyCertificateTool.bat -E -T -r destination_file -k
c10_location/configuration/signkeypair/jCAKeystore -p NoPasswordSet
     ```
3. Import the certificate to the trust store on your server.
   - For information on updating the server trust store, see the documentation for your server.

**Copying the CA certificate to IBM Cognos servers**

After copying the IBM Cognos certificate to the other servers, copy the certificate from the certificate authority to the IBM Cognos server.

**Procedure**

1. Copy the certificate from your certificate authority to a secure location on the IBM Cognos server.
   - Ensure that the CA certificate is in Base-64 encoded X.509 format.
2. Import the CA certificate by typing the following command:
   - On UNIX or Linux operating systems, type the following:
     ```
     ThirdPartyCertificateTool.sh -T -i -r CA_certificate_file -k
c10_location/configuration/signkeypair/jCAKeystore -p NoPasswordSet
     ```
   - On Microsoft Windows operating systems, type
     ```
     ThirdPartyCertificateTool.bat -T -i -r CA_certificate_file -k
c10_location/configuration/signkeypair/jCAKeystore -p NoPasswordSet
     ```

**Select and rank cipher suites for Secure Socket Layer**

An SSL connection begins with a negotiation in which the client and server present a list of supported cipher suites in a priority sequence. A cipher suite provides the quality of protection for the connection. It contains cryptographic, authentication, hash, and key exchange algorithms. The SSL protocol selects the highest priority suite that the client and the server both support.

A list of supported cipher suites for SSL is provided. You can eliminate cipher suites that do not meet your requirements and then assign a priority, or preference, to the remaining cipher suites. The selected cipher suites are presented in priority sequence for the client and server sides of the negotiation. At least one of the selected cipher suites between the client and server platforms must match.

The list of supported cipher suites is dynamically generated on each computer, and depends on the Java Runtime Environment (JRE) or whether you have other
cryptographic software installed on the computer. If you have made changes to a computer, such as upgraded the JRE or installed software that has upgraded the JRE, this may affect the supported cipher suites available on that computer. If you no longer have a supported cipher suite that matches the other computers in your environment, you may have to change the JRE on the computer to match the other computers in your environment.

**Procedure**

1. Start IBM Cognos Configuration.
2. In the Explorer window, click **Cryptography > Cognos**.
3. In the Properties window, click the **Value** column for the **Supported ciphersuites** property.
4. Click the edit icon.
   - To move a cipher suite to the **Current values** list, click the check box in the **Available values** list and then click **Add**.
   - To move a cipher suite up or down in the **Current values** list, click the check box and then click the up or down arrows.
   - To remove a cipher suite from the **Current values** list, click the check box and then click **Remove**.
5. Click OK.
6. From the File menu, click Save.

### Configure IBM Cognos for SSL enabled Web servers

If you are using secure sockets layer (SSL) on your Web server, you must change the **Gateway URI** values in IBM Cognos Configuration to be able to access the portal.

To enable SSL on your Web server, you must obtain a Web server certificate signed by a Certificate Authority (CA) and install it into your Web server. The certificate must not be self-signed, because self-signed certificates will not be trusted by IBM Cognos components. For more information about using certificates with your Web server, see your Web server documentation. These certificates are not provided with IBM Cognos products.

To enable users to access the IBM Cognos portal using SSL, you must change the **Gateway URI** values in IBM Cognos Configuration for each computer where the Application Tier Components and Framework Manager are installed.

**Procedure**

1. Configure your Web server for SSL and start the Web server.
2. On each computer where the Application Tier Components or Framework Manager are installed, start IBM Cognos Configuration.
3. Under **Local Configuration**, click **Environment**, and change the **Gateway URI** value from http to https.
4. In the **Gateway URI** value, change the port number to the SSL port number defined for your Web server. For example, the default port number for SSL connections is usually 443.
5. Save your configuration, and restart your services.
Results

When you access the portal using https://servername:443/ibmcognos, you should be prompted to install a certificate.

To avoid being prompted by a security alert for each new session, install the certificate into one of your Web browser's certificate stores.

Configuring a Repository for Log Messages

The BI Bus protocol includes log message processing, an important diagnostic tool for investigating the behavior of IBM Cognos BI.

In addition to error messages, log messages provide information about the status of components and a high-level view of important events. For example, log messages can provide information about attempts to start and stop services, completion of processing requests, and indicators for fatal errors. Audit logs, which are available from a logging database, provide information about user and report activity.

The IBM Cognos services on each computer send information about errors and events to a local log server. A local log server is installed in the c10_location/logs folder on every IBM Cognos BI computer that contains Content Manager or Application Tier Components. Because the log server uses a different port from the other IBM Cognos BI components, it continues to process events even if other services on the local computer, such as the dispatcher, are disabled.

The following workflow shows the tasks that are required to prepare for logging.

- During planning, determine the logging configuration that is suitable for your environment. For example, evaluate various log message repositories, such as remote log servers and log files, such as the UNIX or Linux syslog or the Windows NT Event log, in addition to the local log file. You can also send only audit logging information to a database. Consider security, such as methods available for protecting log files from system failures and user tampering.

  For information about planning, see the IBM Cognos Business Intelligence Architecture and Deployment Guide.

- During configuration, define the startup properties for logging, such as connection settings for databases. You must also create a logging database if you plan to collect audit logs. If communication between a local log server and a remote log server must be secured, make the appropriate configuration changes on both IBM Cognos BI computers. You can also enable certain logging features, such as user-specific logging.

  For information about setting up logging, see the IBM Cognos Business Intelligence Administration and Security Guide.
For information about using log messages to solve problems and resolving logging-related issues, see the IBM Cognos Business Intelligence Troubleshooting Guide.

Guidelines for creating a logging database

You can create a database to store log messages. Creating a logging database involves the following tasks:

- Create a logging database.
  
  For DB2, Oracle, Microsoft SQL Server, or Sybase, use the same procedure that was used to create the content store database. Use the instructions in “Guidelines for creating the content store” on page 27.

  **Note:** If you are using DB2, you cannot generate a script to create the notification database in the same way as you can the content store.

- Set up the database connectivity.
  
  Use the instructions in “Database connectivity for the logging database.”

- Specify the log messages repository.
  
  Use the instructions in “Log message repositories” on page 218.

Database connectivity for the logging database

After you create a database for audit logs, additional steps are required to set up the database client if you use Oracle, DB2, Informix Dynamic Server, or Sybase as the database server.

You cannot use Cognos Content Database as a logging database.

In a distributed environment, the local log server on an Application Tier Component computer may send log messages to a remote log server, which then sends messages to the logging database. For Oracle, Sybase, and DB2, the appropriate JDBC driver and/or database client software is required only on the Application Tier Components computer with the remote log server that connects to the logging database.

Microsoft SQL Server

If you use a Microsoft SQL Server database, the JSQLConnect.jar file is installed to the appropriate location by default. The only additional step is to ensure that the Microsoft SQL Server uses TCP/IP connectivity.

Set up database connectivity for a DB2 logging database

You must set up the database client software and the JDBC driver on all Application Tier Components computers with a connection to the logging database. You must set up the JDBC driver on the Content Manager computer, unless you are using the same type of database for the log messages as you use for the content store.

The driver version must be at least JCC 3.7 for a Linux or UNIX operating system, or for a Microsoft Windows operating system version 9.1 fix pack, or JCC 3.42 for a Linux, UNIX operating system, or for a Microsoft Windows operating system version 9.5 fix pack 2.
Procedure

Copy the following files from DB2 installation\sqllib\java directory to the c10_location\webapps\p2pd\WEB-INF\lib directory:

- The universal driver file, db2jcc.jar
- The license file:
  For DB2 on Linux, UNIX, or Windows operating systems, use db2jcc_license_cu.jar.
  For DB2 on z/OS, use db2jcc_license_cisuz.jar.
  If you are connecting to DB2 on z/OS, use the driver version from Linux, UNIX, or Windows version 9.1 fix pack 5 or version 9.5 fix pack 2.

Tip: To check the driver version, run the following command:
java -cp path\db2jcc.jar com.ibm.db2.jcc.DB2Jcc -version

Set up database connectivity for an Oracle logging database

You must set up the JDBC driver on all Application Tier Components computers with a connection to the logging database. You must also set up the JDBC driver on the Content Manager computer, unless you are using the same type of database for the log messages as you use for the content store.

Procedure

1. On the computer where the Oracle client is installed, go to the ORACLE_HOME/jdbc/lib directory.
2. Copy the correct library file for your version of the Oracle client to the c10_location\webapps\p2pd\WEB-INF\lib directory on the computer where Content Manager is installed and where notification is sent to an Oracle database.
   - If you are using Oracle 10g, you must have ojdbc14.jar.
   - If you are using Oracle 11g, you must have ojdbc5.jar.
   - The files are available from an Oracle client or server install, and can also be downloaded from the Oracle technology Web site.

Set up database connectivity for an Informix logging database

You must set up the JDBC driver on all Application Tier Components computers with a connection to the logging database. You must also set up the JDBC driver on the Content Manager computer, unless you are using the same type of database for the log messages as you use for the content store.

Procedure

1. On the computer where Informix is installed, go to the Informix_location/ sqllib/java directory.
2. Copy the following files to the c10_location\webapps\p2pd\WEB-INF\lib directory on every computer where Content Manager is installed.
   - the universal driver file, db2jcc.jar
   - the license file, db2jcc_license_cisuz.jar

Set up database connectivity for a Sybase logging database

You must set up the JDBC driver on all Application Tier Components computers with a connection to the logging database. You must also set up the JDBC driver on the Content Manager computer, unless you are using the same type of database for the log messages as you use for the content store.
Procedure

1. On the computer where Sybase is installed, go to the Sybase_location/jConnect-6/classes directory.
2. Copy the jconn3.jar file to the c10_location/webapps/p2pd/WEB-INF/lib directory on every computer where Content Manager is installed and where notification is sent to a Sybase database.

Log message repositories

A local log server is automatically installed when you install Content Manager or the Application Tier Components. You can specify one or more repositories where the local log server sends log messages.

Sending log messages to a remote log server

In a distributed installation, you can configure the log server on each IBM Cognos computer to send log messages to a single remote log server, which acts as a common log server. You can then configure the common log server to send the log messages to a local file or database on the same or different computer.

If the remote log server becomes unavailable, log messages are redirected to recovery files on the local computer in the c10_location/logs/recovery/remote directory. These recovery files have timestamp information in their file names, and are not readable like regular log files. When the remote log server becomes available, an automatic recovery process moves all log information to the remote log server and deletes the local log files.

Saving log messages to a file

The log server is configured by default to send log messages to the c10_location/logs/cogserver.log file. If the default log file does not exist when the IBM Cognos service starts, it is created automatically.

You can configure the log server to send log messages to a different file. If you configure a different log file, IBM Cognos attempts to automatically create this file on startup, in addition to the default log file. If the location for the configured log file is different from the c10_location/logs directory, you must ensure the path to the log file exists before starting the IBM Cognos service. For example, if you configure the log server to send messages to the /usr/lpp/logfiles/cognos.log file, IBM Cognos attempts to automatically create the cognos.log file in the /usr/lpp/logfiles folder. If this folder does not exist, IBM Cognos does not create the cognos.log file and no log messages can be recorded in it. Note that these log messages are not recorded in the default log file. Although IBM Cognos automatically creates the default log file even when another log file is configured, the default log file is not used as a backup.

Saving log messages to a database

The log server can also send audit logs to a database on the same or another computer. Audit logs provide information about user and report activity.

The logging database has the same configuration and user account requirements as the content store database. After you configure IBM Cognos components to send messages to a logging database, and restart the IBM Cognos service, IBM Cognos components create the required tables and table fields. You can test the connection to the logging database before you restart the IBM Cognos service.
Specify the Log Messages Repository for DB2 on UNIX, Linux, or Windows

You can configure a type of repository for the log messages, and then configure properties for the specific repository. You can also configure more than one repository for log messages.

Before you begin

Before you specify a database as a repository, ensure that you
- created the logging database
- set up the database client

Procedure

1. On the computer where you installed Content Manager or the Application Tier Components, start IBM Cognos Configuration.
2. In the Explorer window, under Environment, click Logging.
3. In the Properties window, use the following table to help set the log server properties.

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use TCP between IBM Cognos components on a computer and</td>
<td>Set the Enable TCP property to True.</td>
</tr>
<tr>
<td>its local log server</td>
<td>UDP provides faster communication with a lower risk of lost connections</td>
</tr>
<tr>
<td></td>
<td>than TCP. However, the risk of losing a local TCP connection is low.</td>
</tr>
<tr>
<td></td>
<td>TCP is always used for communication between a local log server and</td>
</tr>
<tr>
<td></td>
<td>a remote log server.</td>
</tr>
<tr>
<td>Change the number of threads available to the local log</td>
<td>Type the value in the Local log server worker threads property.</td>
</tr>
<tr>
<td>server</td>
<td>Keep the default value of 10. The range is between 1 and 20.</td>
</tr>
<tr>
<td></td>
<td>However, if you have a high number of log messages, you can allocate</td>
</tr>
<tr>
<td></td>
<td>more threads to improve performance.</td>
</tr>
</tbody>
</table>

4. In the Explorer window, under Environment, right-click Logging, and click New resource > Destination.
5. In the Name box, type the name of the repository.
6. In the Type list, click the type of repository and then click OK.
7. If the repository is a file in the Properties window, type the appropriate values for the mandatory and optional properties.
8. If the repository is a remote log server in the Properties window, type the appropriate values for the mandatory and optional properties.
   If the Internal dispatcher URI of the repository computer is configured to use SSL, in the Properties window, set the Enable SSL property to True.
   You must later specify the log messages repository when you configure the remote log server.

Chapter 9. Configuration options 219
9. If the repository is a database, in the Explorer window, under Logging, specify the type of database and its properties, as follows:
   - Right-click the database name, and click New resource > Database.
   - In the Name box, type the name of the repository.
   - In the Type list, click the type of database and then click OK.
   - In the Properties window, type the appropriate values for the mandatory and optional properties.
     For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the Database server with port number or instance name property. Include the port number if you use nondefault ports. Include the instance name if there are multiple instances of Microsoft SQL Server.
     To connect to a named instance, you must specify the instance name as a JDBC URL property or a data source property. For example, you can type localhost\instance1. If no instance name property is specified, a connection to the default instance is created.
     Note that the properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:
     jdbc:JSQLConnect://localhost\instance1/user=sa/more properties as required
   - Test the connection to the new database. In the Explorer window, under Environment, right-click Logging and click Test.
     IBM Cognos components connect to the database. If you configured more than one database for logging messages, IBM Cognos components test all the databases.

10. Repeat steps 5 to 10 for each repository to which you want the log server to send messages.
11. From the File menu, click Save.
12. In the Explorer window, click IBM Cognos services > IBM Cognos.
13. From the File menu, click Restart.
    If you selected a database as the repository, IBM Cognos components create the required tables and fields in the database that you created.

Results

If the repository was a remote log server, configure and start the remote log server. Then restart the IBM Cognos service on the local computer.

If the repository was a database, you can use IBM Cognos components to run log reports from the database.

You can also set the logging level, which controls the amount of detail and type of messages that are sent to a log file or database. For instructions, see the IBM Cognos Business Intelligence Administration and Security Guide.

Specify the Log Messages Repository for Informix
You can configure a type of repository for the log messages, and then configure properties for the specific repository. You can also configure more than one repository for log messages.

Procedure
1. In the Explorer window, under Environment, click Logging.
2. In the Properties window, use the following table to help set the log server properties.

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Use TCP between IBM Cognos components on a computer and its local log server | Set the Enable TCP property to True.  
UDP provides faster communication with a lower risk of lost connections than TCP.  
TCP is used for communication between a local log server and a remote log server. |
| Change the number of threads available to the local log server       | Type the value in the Local log server worker threads property.  
Keep the default value of 10. The range is between 1 and 20. However, if you have a high number of log messages, you can allocate more threads to improve performance. |

3. In the Explorer window, under Environment, right-click Logging, and click New resource > Destination.
4. In the Name box, type the name of the repository.
5. In the Type list, click Database and then click OK.
6. In the Explorer window, under Logging, right-click the database name, and click New resource > Database.
7. In the Name box, type the name of the repository.
8. In the Type list, click Informix Dynamic Server database and then click OK.
9. In the Properties window, type the values for Database server and port number, User ID and password, and Database name.
10. If you have multiple instances of an Informix logging database, create the advanced property IPFSCRIPTIDX and specify the account under which the instance runs:
   - In the Explorer window, click Local Configuration.
   - In the Properties window, click the Value column for Advanced properties and then click the edit icon.
   - In the Value - Advanced properties dialog box, click Add.
   - In the Name column, type IPFSCRIPTIDX
   - In the Value column, type the user ID of the account under which the instance of the logging database runs.
   Use a different user account for each instance of Informix logging database.
   - Repeat in every instance of IBM Cognos Configuration that uses an instance of an Informix logging database.
11. From the File menu, click Save.
12. Test the connection to the new database. In the Explorer window, under Environment, right-click Logging and click Test.
   IBM Cognos components connect to the database. If you configured more than one database for logging messages, IBM Cognos components test all the databases.
Enabling User-specific Logging

When diagnosing problems, you can temporarily set logging to track one or more specific users instead of all users at once. After you complete the diagnosis, you can resume normal logging. To enable user-specific logging, you use IBM Cognos Configuration to configure connection information for Java Management Extensions (JMX) a technology that supplies tools to manage and monitor applications and service-oriented networks. Then you configure JMX connection information in a deployment properties file.

After enabling user-specific logging for IBM Cognos components, enable logging for a specific user by using the Remote Process service for JMX. For information, see the topic about using logging to diagnose a problem for a specific user in the IBM Cognos Business Intelligence Administration and Security Guide.

You must install Oracle Java SE Development Kit or Java Software Development Kit for IBM before you can enable user-specific logging.

Configure JMX Connection Information using IBM Cognos Configuration

You configure Java Management Extensions (JMX) connection information in IBM Cognos Configuration by specifying a cookie value and then setting the JMX port and credentials.

Procedure

1. On the computer where Content Manager is installed, start IBM Cognos Configuration.
2. In the Explorer window, click Environment.
3. In the Properties window, configure the JMX properties under Dispatcher Settings:
   - For External JMX port, type an available port number.
   - For External JMX credential, click the edit icon in the Value column, type a user ID and password, and then click OK.
     The user ID and password ensure that only an authorized user can connect to the Java environment to specify the user or users to be logged, using the port specified in External JMX port.
4. Save the configuration.

Configure JMX Connection Information in a Deployment Properties File

To support the Java Management Extensions (JMX) settings on your application server, specify the JMX port in the p2pd deployment properties file.

Procedure

1. In a text editor, open the p2pd.deploy_defaults.properties file located at c10_location/webapps/p2pd/WEB-INF.
2. Uncomment the rmiregistryport line and set the value to the External JMX port that you configured in IBM Cognos Configuration.
4. Restart the services for IBM Cognos.
Results

IBM Cognos now supports logging for one or more specific users. For more information, see the topic about using logging to diagnose a problem for a specific user in the IBM Cognos Business Intelligence Administration and Security Guide.

Changing Global Settings

By default, IBM Cognos components ensure that all locales, which may come from different sources and in various formats, use a normalized form. That means that all expanded locales conform to a language and regional code setting. Each computer has a default system locale and one user locale per user. The user locales may be different from the default system locale. If you change global settings on one Content Manager computer, you must make the same changes on the other Content Manager computers.

You change global settings

- to customize language support for the user interface
- to customize currency support
- to customize content locale support
- to map the language used in the product user interface
- to map content locales
- to add fonts to your IBM Cognos environment
- to customize the default time zone
- to change the encoding for email messages
- to customize cookie settings

Customize Language Support to the User Interface

Use the Product Locales table to add or remove the user interface language support. For example, if you do not require a German user interface, you can remove the language from the list.

If you change the user interface language of the product, data is not affected.

If you want users to see product documentation in a language other than English, you must install the Supplementary Language Documentation. For more information, see “Installing translated product documentation” on page 59.

Before you begin

Ensure that you install the appropriate fonts to support the character sets and currency symbols you use. For Japanese and Korean currency symbols to appear correctly, you must install the additional fonts from the Supplementary Language Documentation disk.

Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the Actions menu, click Edit Global Configuration.
3. Click the Product Locales tab.
   All supported locales are displayed.
4. Click Add.
Tip: To remove support, select the check box next to the Supported Locale and then click Remove.
5. In the second column, type the language portion of a locale.
6. Repeat steps 3 to 5 for other language support that you want to add.
7. Click OK.
8. From the File menu, click Save.

Customizing Currency Support
If you require additional currencies or want to remove some from the user interface, you can update the list of supported currencies in the Currencies table. If you use Japanese or Korean currencies, you must configure support so that Japanese Yan and Korean Won characters display correctly.

By default IBM Cognos components show only a subset of supported currencies in the user interface. Currencies are identified by their ISO 4217 currency code. The complete list of supported currencies that can be added are listed in the i18n_res.xml file in the c10_location/bin directory.

Adding currencies to the IBM Cognos environment does not guarantee that your computer has a font with the required characters to display the currency. Ensure that you install the appropriate fonts to support the currency symbols you use. For example, to display the Indian currency symbol (rupee) correctly, you must install a font that contains that character. In addition, for Japanese and Korean currency symbols to appear correctly, you must install the additional fonts from the Supplementary Language Documentation disk.

Add Currencies to the User Interface
You can add supported or unsupported currencies to the user interface. You add supported currencies in IBM Cognos Configuration. You add unsupported currencies to the i18n_res.xml file that is provided in IBM Cognos.

If you add a currency code that is not supported by IBM Cognos, you must manually add it to the i18n_res.xml file in the c10_location/bin directory. Copy this file to each IBM Cognos computer in your installation.

Procedure
1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the Actions menu, click Edit Global Configuration.
3. Click the Currencies tab.
4. Click Add.

Tip: To remove support, select the check box next to the supported item and then click Remove.
5. In the second column, type an appropriate value.
   The value you add must comply with ISO 4217 codes for the representation of currencies and formats. Usually the value you add is a three-letter alphabetic code. The first two characters are letters representing the ISO 3166 country or region code for the country or region the currency is from. The additional letter represents the first letter of the currency.
6. Repeat steps 3 to 5 for other types of support that you want to add.
7. From the File menu, click Save.
Customize content locale support

To ensure users see reports, data or metadata in their preferred language, or specific to their region, you can add partial locales (language) or complete locales (language-region) to the Content Locales table. This way, if content is available in different languages, or in different locales, it is rendered to users based on their user locale. By default, content locale overrides product locale in the portal for some content.

If you view reports in Thai language, digits are not supported.

Before you begin

If a locale is not required, you can remove it from the list. You must leave at least one content locale in the list for the Application Tier Components to operate.

Adding incomplete locales (languages) to the IBM Cognos environment does not guarantee that your computer has a font that can display Web pages in your preferred languages. Ensure that you install the appropriate fonts to support the character sets and currency symbols you use. For Japanese and Korean currency symbols to appear correctly, you must install the additional fonts from the Supplementary Language Documentation disk.

Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the Actions menu, click Edit Global Configuration.
3. Click the Content Locales tab.
   All supported locales are displayed.
4. Click Add.
   Tip: To remove support, select the check box next to the supported item and then click Remove.
5. In the second column, type an appropriate value.
   • To add language support for report data and metadata, type a partial local (language) setting.
   • To add support specific to a region, type a complete locale (language-region) setting.
6. Repeat steps 3 to 5 for each additional locale that you want to support.
7. From the File menu, click Save.

Content Locales

Use the Content Locale Mappings table to map user locales to a complete (language-region) or partial (language) locale. You can also map a user’s preferred language to another language if content is not available in the user’s preferred language.

For example, if a report or scorecard is not available in a preferred language, for example Vietnamese, but is available in French and German, you can use the Content Mappings table to map the preferred language (Vietnamese) to another language (French or German). This way, you see the report or scorecard in the mapped language.
By default, the Content Locale Mappings table includes locales that do not contain the region. This allows you to use only the language portion of the locale when you specify locale settings and ensures that you always see the correct information. For example, in a multilingual database, data is usually available in different languages, such as French (fr), Spanish (es) and English (en), rather than being available in different locales, such as English Canada (en-ca), English United States (en-us), or French France (fr-fr).

The following examples show the method that IBM Cognos components use to determine which report or scorecard the user sees if the multiple language versions are available.

**Example 1**

A report is available in Content Manager in two locales, such as en-us (English-United States) and fr-fr (French-France), but the user locale is set to fr-ca (French-Canadian). IBM Cognos uses the locale mapping to determine which report the user sees.

First, IBM Cognos checks to see if the report is available in Content Manager in the user's locale. If it is not available in the user's locale, IBM Cognos maps the user's locale to a normalized locale configured on the Content Locale Mapping tab. Because the user's locale is fr-ca, it is mapped to fr. IBM Cognos uses the mapped value to see if the report is available in fr. In this case, the report is available in en-us and fr-fr, not fr.

Next, IBM Cognos maps each of the available reports to a normalized locale. Therefore, en-us becomes en and fr-fr becomes fr.

Because both report and the user locale maps to fr, the user having the user locale fr-ca will see the report saved with the locale fr-fr.

**Example 2**

The user's locale and the report locales all map to the same language. IBM Cognos chooses which locale to use. For example, if a user's locale is en-ca (English-Canada) and the reports are available in en-us (English-United States) and en-gb (English-United Kingdom), IBM Cognos maps each locale to en. The user will see the report in the locale setting that IBM Cognos chooses.

**Example 3**

The report and the user locales do not map to a common language. IBM Cognos chooses the language. In this case, you may want to configure a mapping. For example, if a report is available in en-us (English-United States) and fr-fr (French-France), but the user locale is es-es (Spanish-Spain), IBM Cognos chooses the language.

**Map Content Locales**

Use the Content Locale Mappings table to map user locales to a complete (language-region) or partial (language) locale. You can also map a user's preferred language to another language if content is not available in the user's preferred language.
Procedure
1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the Actions menu, click Edit Global Configuration.
3. Click the Content Locale Mapping tab.
4. Click Add.
5. In the Key box, type the user locale:
   - To ensure all regions for a user locale see content in a specific language, type
     the language portion of the locale, followed by a dash (-) and an asterisk (*).
     For example, type fr-*
   - To ensure a user locale (language-region) sees content in a specific language,
     type the complete locale.
     For example, type fr-ch
   - To map a preferred language to another language, type the preferred
     language portion of the locale.
     For example, type zh
   Tip: To specify the locale to use for a range of keys, use the wildcard character
   (*) with the Key value and then, in the Locale Mapping box, type the locale.
   For example, if you want all the German keys to use the German locale, type
   de* in the Key box and type in the Locale Mapping box.
6. In the Locale Mapping box, type the language portion of the locale.
   User locales specified in the Key box will see content in this language.
7. Repeat steps 3 to 5 for other mappings you want to do.
8. Click OK.
9. From the File menu, click Save.

Map Product Locales
Use the Product Locale Mappings table to specify the language used in the user
interface when the language specified in the user’s locale is not available.

You can ensure that all regions for a locale use the same language, or that a
specific, complete locale (language-region) uses a particular language.

By default, the user sees the product interface in the language that matches the
language setting of the user locale.

Procedure
1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the Actions menu, click Edit Global Configuration.
3. Click the Product Locale Mappings tab.
4. Click Add.
5. In the Key box, type the user locale:
   - To ensure all regions for a locale see the user interface in a specific language,
     type the language portion of the locale, followed by a dash (-) and an
     asterisk (*).
     For example, type es-*
   - To ensure a complete locale (language-region) see the user interface in a
     specific language, type the complete locale.
     For example, type es-es
To map a preferred language to another language, type the preferred language portion of the locale.

For example, type zh

Tip: To specify which locale to use as the default, use the wildcard character (*) for the Key value and then, in the Locale Mapping box type the locale.

6. In the Locale Mapping box, type the language portion of the locale.

User locales specified in the Key box will see content in this language.

7. Repeat steps 3 to 5 for other mappings you want to do.

8. Click OK.

9. From the File menu, click Save.

Customize the Server Time Zone

You can customize the time zone used by Content Manager by selecting a different server time zone in IBM Cognos Configuration.

For UNIX installations that do not support a Java-based graphical user interface, you can view the list of acceptable time zones by opening IBM Cognos Configuration on the Windows computer where Framework Manager is installed.

Content Manager is configured to use the time zone of your operating system by default. All scheduled activities in IBM Cognos are set using this time zone. In addition, users in IBM Cognos Connection use this time zone if they set their preferences for the default time zone. For more information about setting user preferences in IBM Cognos Connection, see the IBM Cognos Business Intelligence Administration and Security Guide.

Procedure

1. Start IBM Cognos Configuration.

2. From the Actions menu, click Edit Global Configuration.

3. In the Global Configuration window, click the General tab.

4. Click the Value column for Server time zone and select another time zone from the list.

5. From the File menu, click Save.

Encoding for Email Messages

By default, IBM Cognos components use UTF-8 encoding in emails. This value sets the default encoding used by the delivery service in this instance for all email messages. You may have older email clients or send email from IBM Cognos to cell phones and PDAs that do not recognize UTF-8. If so, you can change the email encoding to a value that works on all your email clients (for example, ISO-8859-1, Shift-JIS). Each instance of IBM Cognos that has an available delivery service must be changed.

The specified encoding affects the entire message, including the subject, attachments, attachment names, and plain or HTML body text.

The encoding values are shown in the following table:

<table>
<thead>
<tr>
<th>Character set</th>
<th>Supported encoding value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTF-8</td>
<td>utf-8</td>
</tr>
</tbody>
</table>
Table 56. Supported encoding values (continued)

<table>
<thead>
<tr>
<th>Character set</th>
<th>Supported encoding value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Western European (ISO 8859-1)</td>
<td>iso-8859-1</td>
</tr>
<tr>
<td>Western European (ISO 8859-15)</td>
<td>iso-8859-15</td>
</tr>
<tr>
<td>Western European (Windows-1252)</td>
<td>windows-1252</td>
</tr>
<tr>
<td>Central and Eastern European (ISO 8859-2)</td>
<td>iso-8859-2</td>
</tr>
<tr>
<td>Central and Eastern European (Windows-1250)</td>
<td>windows-1250</td>
</tr>
<tr>
<td>Cyrillic (ISO 8859-5)</td>
<td>iso-8859-5</td>
</tr>
<tr>
<td>Cyrillic (Windows-1251)</td>
<td>windows-1251</td>
</tr>
<tr>
<td>Turkish (ISO 8859-9)</td>
<td>iso-8859-9</td>
</tr>
<tr>
<td>Turkish (Windows-1254)</td>
<td>windows-1254</td>
</tr>
<tr>
<td>Greek (ISO 8859-7)</td>
<td>iso-8859-7</td>
</tr>
<tr>
<td>Greek (Windows-1253)</td>
<td>windows-1253</td>
</tr>
<tr>
<td>Japanese (EUC-JP)</td>
<td>euc-jp</td>
</tr>
<tr>
<td>Japanese (Shift-JIS)</td>
<td>shift_jis</td>
</tr>
<tr>
<td>Traditional Chinese (Big5)</td>
<td>big5</td>
</tr>
<tr>
<td>Simplified Chinese (GB-2312)</td>
<td>gb2312</td>
</tr>
<tr>
<td>Korean (EUC-KR)</td>
<td>euc-kr</td>
</tr>
<tr>
<td>Korean (KSC-5601)</td>
<td>ksc_5601</td>
</tr>
<tr>
<td>Thai (Windows-874)</td>
<td>windows-874</td>
</tr>
<tr>
<td>Thai (TIS-620)</td>
<td>tis-620</td>
</tr>
</tbody>
</table>

Change Encoding for Email Messages

You can change the email encoding to a value that works on all your email clients.

Procedure

1. Start IBM Cognos Configuration.
2. From the Actions menu, click Edit Global Configuration.
3. In the Global Configuration window, click the General tab.
4. Click the Value column for the Email Encoding property.
5. Scroll to the desired setting and click it.
6. From the File menu, click Save.

Cookie Settings

Based on the requirements of your IBM Cognos environment, you may need to modify the settings that IBM Cognos components use to create cookies. You can use IBM Cognos Configuration to customize the cookie domain, path, and secure flag.

IBM Cognos components determine the cookie domain from the HTTP request submitted by the client, which is typically a Web browser. In most network configurations, HTTP requests pass through intermediaries such as proxy servers and firewalls as they travel from the browser to IBM Cognos components. Some
intermediaries modify the information that IBM Cognos components use to calculate the cookie domain, and IBM Cognos components then cannot set cookies. The usual symptom of this problem is that users are repeatedly prompted to log on. To avoid this problem, configure the cookie domain.

To set the correct value for the cookie domain, use the format and value that represents the widest coverage for the host, as listed in the following table.

Table 57. Cookie settings

<table>
<thead>
<tr>
<th>Host</th>
<th>Format for domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>computer or server</td>
<td>computer or server name (no dots)</td>
</tr>
<tr>
<td></td>
<td>Example: mycompany</td>
</tr>
<tr>
<td>suffix is .com, .edu, .gov,</td>
<td>.name.suffix</td>
</tr>
<tr>
<td>.int, .mil, .net, or .org</td>
<td>(two dots)</td>
</tr>
<tr>
<td></td>
<td>Example: .mycompany.com</td>
</tr>
<tr>
<td>other</td>
<td>.name1.name2.suffix</td>
</tr>
<tr>
<td></td>
<td>(three dots)</td>
</tr>
<tr>
<td></td>
<td>Example: .travelinfo.co.nz</td>
</tr>
</tbody>
</table>

Additionally, for security, administrators can set the HTTPOnly attribute to block scripts from reading or manipulating the CAM passport cookie during a user's session with their web browser. For more information about this attribute, see the IBM Cognos Business Intelligence Administration and Security Guide.

**Customize Cookie Settings**

Use IBM Cognos Configuration to customize the cookie domain, path, and secure flag.

**Procedure**

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the Actions menu, click Edit Global Configuration.
3. Click the General tab.
4. Click in the Value column under Cookie Settings for each property that you want to change and specify the new value.
   - If you leave the Domain property blank, the dispatcher derives the domain from the host name of the request.
5. Click OK.

**Change the IP Address Version**

IBM Cognos supports two IP address versions: IPv4 and IPv6. IPv4 uses 32-bit IP addresses and IPv6 uses 128-bit IP addresses. For example:

- IPv4: 192.168.0.1:80

In IBM Cognos Configuration, you can select IPv4 or IPv6 for IBM Cognos communication using the IP Version for Host Name Resolution property. By default IPv4 is employed.
The setting applies only to the computer where it is set. If you select **Use IPv4 addresses**, all outgoing IBM Cognos connections on that computer are established using IPv4 and the dispatcher accepts only incoming IPv4 connections. If you select **Use IPv6 addresses**, all outgoing IBM Cognos connections on that computer are established using IPv6 and the dispatcher accepts both incoming IPv4 and IPv6 connections.

IPv4 client computers can communicate with dispatcher computers that are configured for IPv6.

Hostnames specified within a URI are resolved based on the value of the **IP Version for Host Name Resolution** property. However, if a URI has been specified with a numeric address, it has precedence over this setting and communication takes place using IPv4.

For IBM Cognos Configuration to accept IPv6 addresses in the local URI properties, you must start IBM Cognos Configuration with the `-ipv6` option. You can specify the option each time you open IBM Cognos Configuration from the command line.

On Windows, you can set the option permanently by adding the option to the Start menu shortcut.

### Setting the IP version

Use IBM Cognos Configuration to select the IP version.

**Procedure**

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. Click the **Value** box for **IP Version for Host Name Resolution** and click **Use IPv4 addresses** or **Use IPv6 addresses**.
4. From the **File** menu, click **Save**.
5. Close IBM Cognos Configuration.

### Manually configuring IBM Cognos Configuration to start with the IPv6 option

You can manually configure IBM Cognos Configuration to use the IPv6 option by specifying the option in the start command.

**Procedure**

1. Go to the `c10_location/bin` or the `c10_location/bin64` directory.
2. Start IBM Cognos Configuration by including the IPv6 option in the command, as follows:
   - On Windows, type
     
     `cogconfig.bat -ipv6`
   - On UNIX or Linux, type
     
     `./cogconfig.sh -ipv6`
3. Edit the URI properties that use IPv6 format, specify the values, and then from the **File** menu, click **Save**.
Configuring IBM Cognos Configuration to always start with the IPv6 option on Windows

You can configure IBM Cognos Configuration to always use the IPv6 option on Microsoft Windows operating systems by setting the option in the Start menu shortcut.

**Procedure**

1. From the *Start* menu, select *Programs > IBM Cognos 10*, and then right-click *IBM Cognos Configuration, Properties*.
2. On the *Shortcut* tab, in the *Target* box, type "c10_location\bin\cogconfigw.exe -ipv6"
3. Click OK.

File Location Properties on Windows Vista

If you install IBM Cognos client components in an environment that includes Windows Vista, you must change file locations properties in IBM Cognos Configuration so that IBM Cognos can use a single data location for all users. The changes must be made on all computers where IBM Cognos client components are installed.

Windows Vista has a security enhancement that restricts multiple users from sharing data locations. You can define environment variables and use them in IBM Cognos Configuration when specifying file locations. This allows you to direct applicable files to an area that will be accessible by IBM Cognos users. On Windows, two environment variables are preset for users: one for all users and one for the specific user.

Because the environment variables represent system root locations, also include the root directory name of the installation location when you specify file locations in IBM Cognos Configuration. The default root directory for IBM Cognos is c10.

Update File Location Properties on Windows Vista

You must change file locations properties in IBM Cognos Configuration so that IBM Cognos can use a single data location for all users. The changes must be made on all computers where IBM Cognos client components are installed.

**Procedure**

1. Start IBM Cognos Configuration.
2. In the *Explorer* window, click *Environment*.
3. In the *Properties* window, click *Deployment files location*.
4. Replace the relative path element, "./", with the appropriate environment variable and root directory:
   - For a single file location per user, %LOCALAPPDATA%
   - For a single file location for all users on the computer, %PUBLIC%

   For example,
   To set a single file location per user, specify the path %LOCALAPPDATA%/c10/deployment.
5. Repeat step 4 for the following properties:
   - Under *Environment*,
     - Data files location
- Map files location
- Temporary files location
  • Under Environment, Logging, File,
    - Log file location
  • Under Cryptography,
    - Common symmetric key store location
  • Under Cryptography, Cognos,
    - Certificate location
    - Signing key store location
    - Encryption key store location
6. From the File menu, click Save.

Results

The environment variables are resolved when the file locations are accessed during system activities.

Change Configuration Settings for the IBM Cognos Series 7 Migration Service

If necessary, you can change service port number used by the IBM Cognos Series 7 migration service.

Procedure

1. Go to the s7_location/migs7 directory.
2. Locate the migs7service_configuration.xml file and remove the read-only attribute from the file properties.
3. Open the file in an XML editor or a plain-text editor such as Notepad.
4. Change the settings in the file to match your environment.
5. Save the file.
6. Restart the migration service:
   • On Windows, restart the migration service using the IBM Cognos Migration Series 7 Service entry in the Services list under Administrative Tools.
   • On UNIX, stop and then start the migration service by typing the following commands in the migs7service directory: ./configure.sh --stop
     ./configure.sh --start

Assign a User Account to the PowerPlay and Migration Services for Migration

By default, the IBM Cognos PowerPlay Enterprise Server service and the migration service use a system account. If multiple PowerPlay servers will share data locations during migration, you must first assign a user account to the services.

A user account must be set up on every Windows computer where Series 7 Migration Components or the PowerPlay component are installed.
Before you begin

Before you assign the user account to the services, ensure that a user account is set up with a password that never expires.

Procedure

1. In the Windows Control Panel, under Administrative Tools, click Services.
2. Click the IBM Cognos PowerPlay Enterprise Server service and click Startup.
3. In the Log On As panel, click This Account.
4. From the list, select the user account that you set up for the service.
5. Type the password for the account in the Password text box and the Confirm Password text box.
6. Click OK.
7. Repeat steps 2 to 5 for the Series 7 migration service.
Chapter 10. Configuring Portal Services

Portal Services provides a set of IBM Cognos portlets that you can use in IBM Cognos Connection and in other portals. You can use the portlets to navigate, search, and view IBM Cognos reports in your working environment. Other users can view IBM Cognos information without needing to know how to use IBM Cognos products.

For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.

Portal Services is installed automatically with IBM Cognos components. In a distributed environment, it is included with the Application Tier Components. The installation includes the deployment files for:

- IBM WebSphere Portal
- Oracle WebCenter Interaction Portal
- SharePoint Portal

For some deployments of Portal Services, you must modify some Portal Services property settings and prepare the IBM Cognos environment to support the other portal.

When used in another portal, Portal Services can authenticate users in only one namespace. If IBM Cognos components are configured with more than one namespace, you must install a separate gateway for each namespace that will be used to authenticate portal users. You must configure each gateway to use the appropriate namespace and then configure the deployed portlets to use that gateway.

After you configure the required properties, you must deploy the Cognos portlets to the other portal. For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.

To use Portal Services with IBM Cognos components, do the following:

- Specify the location of the applications.xml file if required.
- Install and test the portlets on the other portal.
  For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.
- Configure security for the other portal environment.

Specify the Location of the Applications.xml File

If you use the applications.xml file as part of a custom application portlet, all Application Tier Components computers in a distributed environment must reference the same applications.xml file. If you have multiple instances of the applications.xml file, they must be identical.

Note: The steps are required only if you want to use the Extended Applications portlet, which is included with the IBM Cognos Business Intelligence software development kit.
Procedure

1. On the Application Tier Components computer, start IBM Cognos Configuration.
2. In the Explorer window, under Environment, click Portal Services.
3. In the Properties window, click the Value next to Location of 'applications.xml'.
4. Replace localhost with a valid host name or IP address and, if necessary, replace the default port number.
5. From the File menu, click Save.

Results

You can now deploy the IBM Cognos portlets to your portal server. For instructions, see the IBM Cognos Business Intelligence Administration and Security Guide.

Configuring Security for Portal Services

When using Portal Services in another portal, you must enable single signon to provide seamless integration between the other portal and IBM Cognos components.

Portal Services uses single signon to authenticate users. This means that users do not have to log on to other applications separately through the portal.

You must configure a URI into IBM Cognos components for each portlet in Portal Services.

To enable security between IBM Cognos components and the other portal, do the following:

- Disable anonymous access to IBM Cognos components.
  If your security infrastructure requires you to use another method for single signon, use one of the following methods:
  - Enable single signon for the other portal using shared secret
  - Configure IBM Cognos components for SSL access, if required.

Disable Anonymous Access to IBM Cognos Components

Portal Services uses single signon for authentication. If anonymous logon is enabled in IBM Cognos components, Portal Services logs all portal users as anonymous. You must ensure that anonymous access is disabled in IBM Cognos components for single signon in Portal Services to be successful. However, you can test the Portal Services connections using anonymous logon to ensure that the portlets are working in the other portal.

If Portal Services fails to authenticate a user, the user receives an error message at the other portal.

Procedure

1. Start IBM Cognos Configuration.
2. In the Explorer window, under Security > Authentication, click Cognos.
3. In the Properties window, ensure that Allow anonymous access is set to False.
4. From the File menu, click Save.
5. Repeat steps 1 to 4 on all servers where you installed IBM Cognos components.

**Enable Single Signon Using Shared Secret**

You can use shared secret for single signon between IBM Cognos portlets and IBM Cognos components. The Cognos portlets send a message that contains an encrypted version of the portal user ID. The encryption key is determined by the value of a secret character string shared between the portlets and the custom Java security provider on the IBM Cognos server.

You can use shared secret for the other portal only if portal user IDs can be looked up in an authentication namespace that is shared by IBM Cognos components.

IBM Cognos components must have access to a directory server that contains user IDs for all your portal users. Using IBM Cognos Configuration, you must configure an authentication namespace so that the portal and IBM Cognos components share the same authentication source.

You must also create a Custom Java Provider namespace to register the shared secret Java provider that is provided with IBM Cognos components. Within the portlets or iViews, you must link the portlets or iViews to the Custom Java Provider namespace within your respective portal:
- Cognos Portlet Application (WebSphere Portal)
- remote server (Oracle WebCenter Interaction Portal)
- Cognos Web Part (SharePoint Portal)

You are not required to configure access to the Portal Services Web content. However, if you deploy the portlets to another portal, you can configure access to an alternate URI for Portal Services images and Web content.

**Configure the Required Namespaces**

IBM Cognos components must have access to a directory server that contains user IDs for all your portal users. Using IBM Cognos Configuration, you must configure an authentication namespace so that the portal and IBM Cognos components share the same authentication source.

**Procedure**

1. In IBM Cognos Configuration, configure a namespace to authenticate portal users.
2. For an LDAP namespace, configure the following properties:
   - For the **Use external identity** property, change the setting to **True**.
   - For the **External identity mapping** property, set it to:
     - (uid=${environment("REMOTE_USER")})
     - For SharePoint Portal, if SharePoint is on a different machine from the LDAP server, set **External identity mapping** to
       - (uid=${replace(${environment("REMOTE_USER")},"SharePoint_Server\",""}))
3. For an IBM Cognos Series 7 namespace, map the portal user IDs to IBM Cognos Series 7 user IDs using OS signons.
   - For more information, see the IBM Cognos Series 7 documentation.
4. In IBM Cognos Configuration, create and configure a Custom Java Provider namespace.
   - For the **Namespace ID** property, specify any new ID.
     - For example, `cpstrusted`
This new ID must be used in the portlet configuration settings.

- For the **Java class name** property, type
  
  com.cognos.cps.auth.CPSTrustedSignon
  
  Java class names are case-sensitive.

5. In IBM Cognos Configuration, under **Environment > Portal Services**, configure the following properties:

- For **Trusted Signon Namespace ID**, type the ID of the namespace that you configured in step 1.

  **Tip**: The trusted signon namespace acts as an intermediary and must be attached to a real directory-based namespace.

- For **Shared Secret**, type the key to be used for single signon.

  This parameter represents the authorization secret that must be shared between the Cognos portlets and the IBM Cognos server. Consider this as a secret password. You must use the same character string when you configure the portlet application. You must use a single word as the key.

  For security reasons, specify a non-null value.

6. Under **Environment**, for **Gateway Settings**, set the **Allow Namespace Override** property to **true**.

7. From the **File** menu, click **Save**.

8. Restart the IBM Cognos service.

**Configure Access to the Portal Services Web Content**

After creating the required namespaces, you must configure access so that users can access the Web content.

**Procedure**

1. On the computer where you installed the Application Tier Components, start IBM Cognos Configuration.

2. In the **Explorer** window, under **Environment**, click **Portal Services**.

3. In the **Properties** window, click the **Value** box next to **Web Content URI**.

4. Specify the host name or IP address of the gateway and a port number using the format

    host_or_IP_address:port

5. From the **File** menu, click **Save**.

**Configure the Cognos iViews for SAP EP**

Within the iViews, you must link the iViews to the Custom Java Provider namespace within your respective portal.

**Configure the Cognos Portlets for WebSphere Portal**

Within the portlets, you must link the portlets to the Custom Java Provider namespace within your respective portal.

**Procedure**

1. For each Cognos portlet application, click the edit value icon.

2. For the **cps_auth_secret** property, enter the secret character string that you used for the **Shared Secret** property when you configured the Custom Java Provider namespace.

3. For the **cps_auth_namespace** property, enter the Custom Java Provider namespace ID.
4. For the **CPS Endpoint** property, enter the URL path to access Portal Services components through the gateway.

The format of the URL is as follows:

- For Cognos content portlets
  
  *Gateway_URI*/wsrp/cps4/portlets/nav?wsdl&b_action=cps.wsdl

  Example for a CGI gateway:
  
  http://myserver/ibmcognos/cgi-bin/cognos.cgi/wsrf/cps4/portlets/nav?wsdl&b_action=cps.wsdl

  Example for a servlet gateway:
  

- For Cognos Extended Applications
  
  *Gateway_URI*/wsrp/cps4/portlets/sdk?wsdl&b_action=cps.wsdl

  Example for a CGI gateway:
  
  http://myserver/ibmcognos/cgi-bin/cognos.cgi/wsrf/cps4/portlets/sdk?wsdl&b_action=cps.wsdl

  Example for a servlet gateway:
  

- For Metrics Manager Watchlist portlets
  
  *Gateway_URI*/wsrp/cps4/portlets/cmm?wsdl&b_action=cps.wsdl

  Example for a CGI gateway:
  
  http://myserver/ibmcognos/cgi-bin/cognos.cgi/wsrf/cps4/portlets/cmm?wsdl&b_action=cps.wsdl

  Example for a servlet gateway:
  

**Configure the Remote Server for Oracle WebCenter Interaction Portal**

Within the portlets, you must link the portlets to the Custom Java Provider namespace within your respective portal.

**Procedure**

1. Using a plain ASCII editor, such as Notepad, edit the cpsalui.properties file in the c10_location/cps/oracle/webapps/gadgets/WEB-INF/classes directory.

2. Configure the settings shown in the following table.
Table 58. Settings for the cpsalui.properties file

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>cps_endpoint</td>
<td>The URL to connect to the Application Tier Components and extract the WSDL information. Specify the URI to the gateway. For a servlet or ISAPI gateway, replace the localhost/ibmcognos/cgi-bin/cognos.cgi portion with the values to target the gateway. For example, http://host_name/ibmcognos/cgi-bin/cognosapi.dll/wsrf/cps4/portlets/[package]?wsdl&amp;b_action=cps.wsdl</td>
</tr>
<tr>
<td>forward_cookies=</td>
<td>The names of the cookie that should be sent to the Application Tier Components for single signon. Leave blank.</td>
</tr>
<tr>
<td>cps_auth_secret</td>
<td>The shared secret code IBM Cognos uses to encrypt an HTTP header variable that carries the user identity. This parameter represents the authorization secret that must be shared between the Cognos portlets and the IBM Cognos server. Consider this as a secret password. Use the same value that you used for Shared Secret in IBM Cognos Configuration. For security reasons, specify a non-null value.</td>
</tr>
<tr>
<td>cps_auth_namespace</td>
<td>The namespace ID for the Custom Java Provider.</td>
</tr>
</tbody>
</table>

3. Go to the **c10_location/cps/oracle** directory and run the following build file:
   - On UNIX or Linux operating systems, **build.sh**
   - On Microsoft Windows operating system, **build.bat**
   This creates a **cps-wci.war** file in the **c10_location/cps/oracle/gadgets** directory.

4. If IBM Cognos BI components are using Tomcat,
   - Stop IBM Cognos BI.
   - Copy the **cps-wci.war** file to the **c10_location/webapps** directory.
     Tomcat automatically expands the WAR file and starts the remote server.
   - Start IBM Cognos BI.

5. If IBM Cognos BI components are running under another type of application server, copy the **cps-wci.war** file to the application server.
   For instructions, see the administration guide for your application server.
Results

Single signon is configured.

Configure Properties for the Cognos Web Part for SharePoint Portal
Within the portlets, you must link the portlets to the Custom Java Provider namespace within your respective portal.

Procedure
1. Using a plain ASCII editor, such as Notepad, edit the web.config file in the \drive\inetpub\wwwroot\wss\VirtualDirectories\virtual_directory_sharepoint_is_running_under.
2. Find the following string:
   `<SSO cps_auth_namespace="" cps_auth_secret="" />`
3. Set cps_auth_namespace to the namespace ID for the Custom Java Provider namespace.
4. Set cps_auth_secret to the value that you used for Shared Secret in IBM Cognos Configuration.

Enable single signon with Sharepoint using Kerberos authentication

To use the Kerberos protocol for your web applications, you must configure Internet Information Services (IIS), Sharepoint Portal, Microsoft SQL Server, your web browser, and IBM Cognos BI.

Configuration summary

Use the following table to help you enable single signon with Sharepoint using Kerberos authentication.

Table 59. Configuration summary for enabling single signon with Sharepoint using Kerberos authentication

<table>
<thead>
<tr>
<th>Software</th>
<th>Configuration tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows server</td>
<td>Allow users to be trusted for delegation.</td>
</tr>
</tbody>
</table>
| Microsoft Internet Information Services (IIS) | • Associate the website that is used for Cognos BI with an application pool, and ensure that the application pool is run by a domain service account that has delegation enabled.  
• Ensure that Anonymous authentication is disabled.  
• Enable Windows authentication  
• Enable the Kerberos authentication provider for Windows authentication.  
• Disable Kernel-mode authentication.  
• Set up the Service Principal Names (SPN) for the IIS web server. |
| Microsoft Internet Explorer           | Ensure that the URLs for the web applications are in the intranet zone or a zone that is configured to automatically authenticate with Integrated Windows Authentication. |
| Firefox                               | Enable support for Kerberos authentication in your Firefox web browser.              |
Table 59. Configuration summary for enabling single signon with SharePoint using Kerberos authentication (continued)

<table>
<thead>
<tr>
<th>Software</th>
<th>Configuration tasks</th>
</tr>
</thead>
</table>
| Active Directory          | • Create service accounts for the IIS application pool for the web applications.  
                            • Register the Service Principal Names (SPN) for the web applications on the service account that is created for the IIS application pool for the web application.  
                            • Configure Kerberos constrained delegation for service accounts.  
| SharePoint web application | To enable Kerberos authentication in SharePoint, you must:  
                            • Create SharePoint Server managed accounts and ensure that the domain service account is registered as a managed account.  
                            • Set the Service Principal Names (SPN) on the SharePoint server.  
                            • Associate the SharePoint site with an application pool, ensure that the application is run by a domain service account, and ensure that the domain account has delegation enabled.  
                            • Use SharePoint Central Administration to indicate that Kerberos authentication is used to define how users interact with a network service to gain access to network resources.  
                            • Disable Anonymous authentication.  
                            • Disable Kernel-mode authentication.  
                            For more information about enabling Kerberos authentication in SharePoint, see the Microsoft SharePoint documentation (technet.microsoft.com/en-us/library/ee806870.aspx).  
| Microsoft SQL Server      | • Ensure that services are running using the domain account.  
                            • Grant users appropriate permissions to the data source.  
                            • Set the SPN on the SQL server.  
| IBM Cognos BI             | • Create an authentication namespace and disable Anonymous Access.  
                            • Create a data source and secure it against the active namespace.  

**Configuring IBM Cognos BI to use an Active Directory namespace for Kerberos authentication**

You can use the Active Directory server as your authentication source and for single signon by using Kerberos delegation. Use IBM Cognos Configuration to configure the namespace for Kerberos authentication.
About this task

By default, the Active Directory provider uses Kerberos delegation and integrates with the Microsoft IIS web server for single signon if integrated authentication (formerly named NT Challenge Response) on a Microsoft Windows operating system is enabled on the IIS web server.

Set up the computers, or the user account under which SharePoint runs, to be trusted for delegation. When you are setting up the computers by using the Active Directory user tool, do not select the Account attribute, which is sensitive and cannot be delegated.

Procedure

1. In every location where SharePoint is installed, open IBM Cognos Configuration.
2. In the Explorer window, under Security, right-click Authentication, and click New resource, Namespace.
3. In the Name box, type a name for your authentication namespace.
4. In the Type list, click Active Directory and then click OK.
   The new authentication provider resource is displayed in the Explorer window, under the Authentication component.
5. In the Properties window, for the NamespaceID property, specify a unique identifier for the namespace.
   Restriction: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that IBM Cognos can locate and use your existing authentication provider.
7. Click File > Save.
8. Test the connection to a new namespace. In the Explorer window, under Authentication, right-click the new authentication resource and click Test.
9. To disable Anonymous authentication, complete the following steps:
   a. In the Explorer window, under Security, Authentication, click the authentication namespace that you created.
   b. In the Properties window, ensure that Allow anonymous access is set to False.
   c. Click File > Save.
   d. Repeat steps a to c on all web application servers that use Kerberos authentication.

Creating a Kerberos-enabled data source

You can create a data source authenticated by the Kerberos protocol by using IBM Cognos Administration. A data source defines the physical connection to a database. The data source specifies the parameters that are needed to connect to the database, including sign-on.

Procedure

1. In IBM Cognos Connection, select Launch > IBM Cognos Administration.
2. On the Configuration tab, select Data Source Connections.
3. Select the New data source button.
4. In the Name and Description page, type a unique name for the data source.
5. In the **Connection** page, from the **Type** menu, select the type of data source that you want to create, such as Microsoft SQL Server or Microsoft Analysis Services.

6. Under **Isolation level**, select **Use the default object gateway**, and click **OK**.

7. Specify the connection parameters for the Microsoft SQL Server data source. For information about connection parameters for the data source, see the *IBM Cognos Business Intelligence Administration and Security Guide*.

8. Under **Signon**, select **An external namespace**, and choose the namespace that you created to authenticate users against the Kerberos data source.

   The credentials that are used to authenticate to the data source are taken from the specified namespace to which the user authenticated previously.

9. To test whether the parameters are correct, click **Test the connection**, and then click **Test**.

   In the **Status** column, you can see whether the connection was successful. If it was unsuccessful, click **Close**, return to the previous steps, and verify your connection parameters.

**Results**

The new Kerberos-enabled data source is displayed in the **Data Source Connections** list on the **Configuration** tab, and can be selected when you are using the Metadata wizard in Framework Manager.

### Enable Single Signon for WebSphere Portal Using the Application Server

The Portal Services portlets can use the Active Credentials objects provided by WebSphere Portal to connect to IBM Cognos components. Portal Services supports the following Active Credentials objects: HttpBasicAuth, LtpaToken, SiteMinderToken, and WebSealToken.

Credentials for the portal user are passed to the gateway using this object. For more information about Active Credential objects, see the documentation for IBM WebSphere Portal.

To use application server single signon, see the documentation for IBM WebSphere Application Server.

### Enable Single Signon for Oracle WebCenter Interaction Portal Using Basic Authentication

You can configure a portlet in WebCenter Interaction Portal to send the username and password as an HTTP Basic authentication header. The header can be used with an authentication namespace to provide single signon.

**Procedure**

1. In IBM Cognos Configuration, configure a namespace to authenticate portal users.

2. Install an alternate CGI or ISAPI or servlet gateway in IBM Cognos.

3. Configure the gateway.

4. In the administration console of the Web server, configure the virtual directories to access the gateway.

   For more information, see the documentation for your Web server.
5. Configure the WebCenter Interaction remote server to access IBM Cognos BI:
   - Edit the cpsalui.properties file in the c10_location/cps/oracle/webapps/gadgets/WEB-INF/classes directory.
   - Change the cps_endpoint property to indicate the URL of the gateway. For a CGI gateway, you can use the default setting if the gateway and the remote server are on the same computer. Otherwise, replace the localhost portion with host_name:port. For a servlet or ISAPI gateway, replace the localhost/ibmcognos/cgi-bin/cognos.cgi portion with the values to target the gateway. For example, http://host_name:port/ibmcognos/cgi-bin/cognosisapi.dll/wsrp/cps4/portlets/[package]?wsdl&b_action=cps.wsdl
   - Set the cps_auth_namespace property to the namespace that you want to use for authentication.

Enable Single Signon for Oracle WebCenter Interaction Portal Using CA SiteMinder

If you use CA SiteMinder to provide single signon in your security infrastructure, you can also use it for single signon with WebCenter Interaction Portal.

You must configure a CA SiteMinder authentication namespace in IBM Cognos BI. WebCenter Interaction Portal sends the CA SiteMinder active authentication token to the remote server, which sends the token to the IBM Cognos gateway.

Procedure
1. In IBM Cognos Configuration, configure a CA SiteMinder authentication namespace.
2. Configure the remote server to forward the authentication token:
   - Edit the cpsalui.properties file in the c10_location/cps/oracle/webapps/gadgets/WEB-INF/classes directory.
   - Change the forward_cookies property to include the name of the active authentication token that CA SiteMinder provides.
   - Change the cps_endpoint property to indicate the URL of the gateway. For a CGI gateway, you can use the default setting if the gateway and the remote server are on the same computer. Otherwise, replace the localhost portion with host_name:port. For a servlet or ISAPI gateway, replace the localhost/ibmcognos/cgi-bin/cognos.cgi portion with the values to target the gateway. For example, http://host_name:port/ibmcognos/cgi-bin/cognosisapi.dll/wsrp/cps4/portlets/[package]?wsdl&b_action=cps.wsdl
   - Change the cps_auth_namespace property to the namespace that you want to use for authentication.
Chapter 11. Using an application server other than Tomcat

IBM Cognos Business Intelligence installs and uses Tomcat as the application server by default. However, you can choose to run IBM Cognos BI in another supported application server instead.

The application servers you can use to run IBM Cognos BI in include the following:

- IBM WebSphere Application Server
- Oracle WebLogic Server
- Red Hat JBoss

For IBM Cognos BI for Linux on System z, IBM WebSphere Application Server is supported.

To ensure that your product works properly, apply all minimum required operating system patches and use only the versions of other software that are supported for an IBM Cognos product.

You can also choose to run the IBM Cognos Servlet Gateway on a supported application server instead of using a Web server. When using the servlet gateway, your environment does not require a Web server. The application server and the servlet gateway replace the functions provided by the Web server and other IBM Cognos gateways.

To set up IBM Cognos BI to run on your application server, do the following:

- Create a separate JVM instance if necessary.
- Check that IBM Cognos components are properly set up.
- Back up any existing IBM Cognos data and encryption keys if required.
- Set environment variables.
- Configure IBM Cognos components to run within the application server.
- Identifying the JDK for WebLogic 9 on AIX, if necessary.
- Change the application server startup script if necessary.
- Configure application server properties and deploy IBM Cognos BI.
- Enable SSL if required.
- Configure the web server.
- Unregister dispatchers that are no longer used.

Create a separate JVM instance

When possible, IBM Cognos Business Intelligence must be installed in a Java Virtual Machine (JVM) instance that is separate from the application server admin processes to isolate both IBM Cognos BI and the administrative functions of the application server.

Running IBM Cognos BI in a separate JVM instance eliminates potential Java class or system resource conflicts and ensures that IBM Cognos BI does not affect any existing customer applications.
An isolated JVM instance can be established by creating one of the following:
- a separate server instance in IBM WebSphere
- a separate managed server in Oracle WebLogic
- a separate server instance for Red Hat JBoss

If you are using the IBM Cognos Servlet Gateway, it must be run in an instance that is separate from IBM Cognos BI.

**Set JVM parameters for performance**

To improve performance of IBM Cognos BI in your application server, you can apply some or all of the following Java virtual machine (JVM) settings.

You do not need to change these settings if you are using Tomcat as the application server.

For example, you can:
- Include the `-Xcompressedrefs` option if you are using a 64-bit application server. This option causes object references to be stored as a 32-bit representation, which reduces the 64-bit object size to be the same as a 32-bit object.
- Include the `-Xdump` option to control how dump agents and dumps are used. For example, include the following options:
  - `-Xdump:heap+system:none`
  - `-Xdump:system:events=gpf+abort,range=1..2,request=serial+compact+prepwalk`
  - `-Xdump:system:events=systhrow+throw,filter=java/lang/OutOfMemory*,range=1..2,request=serial+compact+prepwalk`

**Check the setup of IBM Cognos components**

Ensure that the following is done before you set up IBM Cognos components to run on the application server:
- IBM Cognos components are installed.
- Before you start IBM Cognos Business Intelligence, the database for the content store must be set up. Install and configure the database clients, if required, and then test the database connectivity.
- The application server is installed and operational on each computer where IBM Cognos components are installed.
  For more information about installation, see your application server documentation.
- The fully qualified installation location of all fonts is specified on all Application Tier Component computers. You specify this location in IBM Cognos Configuration. By default, the installation location does not use a fully qualified path.
- The application server user account has full access permissions for the IBM Cognos installation.

**Tip:** Create a new UNIX or Linux operating system group named cognos. This group must contain the user that starts the application server and the user that owns the IBM Cognos files. Change the group ownership of the IBM Cognos files to the cognos group and change the file permissions for all IBM Cognos files to GROUP READABLE/WRITEABLE/EXECUTABLE. For simplicity, you can also use the application server user account to install and run IBM Cognos components.
Back up existing IBM Cognos information

You must back up existing IBM Cognos information if IBM Cognos Business Intelligence components are running on an application server (including Tomcat) and you are changing to an application server that ships with its own JVM. You must also back up existing IBM Cognos information if you must change the JVM you are using.

**Note:** You must back up existing IBM Cognos information within the working environment prior to upgrade.

Before configuring IBM Cognos BI components to run on the new application server or JVM, you must back up

- content store data by creating a deployment export.
- configuration information by exporting it. Any encrypted data is decrypted during the export.
- cryptographic keys by saving them to an alternate location. New cryptographic keys must be created using the same JVM that the application server uses. Because these keys can be created only if the previous keys are deleted, it is important to back up the previous keys.

To ensure the security and integrity of your IBM Cognos data, back up the content store, configuration information, and cryptographic keys to a directory that is protected from unauthorized or inappropriate access.

**Tip:** To check if any cryptographic keys exist, look in the `c10_location/configuration` directory. Cryptographic keys exist if this directory includes the following subdirectories: `csk`, `encryptkeypair` or `signkeypair`.

**Procedure**

1. If data exists in the content store, start the IBM Cognos service and export the entire content store using the Deployment tool.
   For more information, see the topic about creating an export deployment specification in the *IBM Cognos Business Intelligence Administration and Security Guide*.
2. In IBM Cognos Configuration, from the **File** menu, click **Export As** and save the configuration information in a decrypted format. When naming the file, use a name such as `decrypted.xml`.
   Export the data to a directory that is protected from unauthorized or inappropriate access because passwords are stored in plain text. You are prompted to acknowledge that the export is an unsecure operation.
3. Stop the IBM Cognos service:
   - If you use Tomcat, stop the IBM Cognos service and close IBM Cognos Configuration.
   - If you use an application server other than Tomcat, shut down IBM Cognos BI in your environment.
4. Back up any existing cryptographic keys by saving the appropriate files and directories to an alternate location that is secure.
   The files are:
   - `c10_location/configuration/cogstartup.xml`
   - `c10_location/configuration/caSerial`
   - `c10_location/configuration/cogconfig.prefs`
The directories are:
- c10_location/configuration/coglocale.xml
- c10_location/configuration/csk
- c10_location/configuration/encryptkeypair
- c10_location/configuration/signkeypair

5. Delete the caSerial and cogconfigprefs files and the three directories: csk, encryptkeypair, and signkeypair.

6. Replace the c10_location/configuration/cogstartup.xml file with the file that contains the data exported from IBM Cognos Configuration (for example, decrypted.xml).
   In the c10_location/configuration directory, the file must use the name cogstartup.xml.
   The information in this file will be automatically re-encrypted using new cryptographic keys when you save the configuration in IBM Cognos Configuration.

**Set environment variables**

You must set environment variables to identify the location of the Java Virtual Machine (JVM) environment and the library path.

You can set environment variables using any of the following methods:
- On Microsoft Windows operating system, set a system or user variable, or edit the application server's startup script.
  If you set a user variable, ensure that you set it for the user account that will run the application server, or administration console.
- On UNIX and Linux operating systems, set an environment variable in the user profile, or edit the application server's startup script.

For information about editing an application server's startup script, see "Change the application server startup script" on page 255.

**Tip:** Most application server versions ship with a script specifically intended for setting environment variables. For example, some IBM WebSphere versions ship with setupCmdLine.bat or setupCmdLine.sh. These scripts can be modified to set appropriate values for use with IBM Cognos components. Most of these scripts set the JAVA_HOME environment variable by default.

**Procedure**

1. Set the JAVA_HOME environment variable to point to the JVM used by the application server.
   **Tip:** If the application server ships with a JVM, then the JAVA_HOME environment variable must be set to reference it.
   IBM Cognos Configuration uses this variable to create encryption keys for IBM Cognos components that are compatible with the JVM used by the application server.
   For example, for WebLogic under Windows, the JVM used by the application server is specified as:
   `drive:/WebLogic_location/jdkversion`

2. Append c10_location/bin to the appropriate environment variable from the following table.
Table 60. Application server environment variables

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Environment variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>PATH</td>
</tr>
<tr>
<td>AIX</td>
<td>LIBPATH</td>
</tr>
<tr>
<td>Solaris and Linux</td>
<td>LD_LIBRARY_PATH</td>
</tr>
<tr>
<td>HP-UX</td>
<td>SHLIB_PATH</td>
</tr>
</tbody>
</table>

The library path environment variable is used to locate the IBM Cognos library files.

**Note:** Ensure that the 32-bit or 64-bit library files are set in your environment variables. For a 64-bit version of IBM Cognos BI, the 64-bit library files must be listed first. For a 32-bit version, the 32 bit library files must be listed first.

**Tip:** To install multiple instances of IBM Cognos Business Intelligence on a single server, set the PATH, LIBPATH, LD_LIBRARY_PATH, or SHLIB_PATH variable within the application server instance scope and not as a global variable to ensure that each instance has a unique value.

---

**Adjusting the default connection time-out value for IBM Cognos Business Intelligence**

The default setting for the connection time-out value used in IBM Cognos Business Intelligence is 25 seconds. Some application servers, such as IBM WebSphere, use a shorter value. To avoid conflicts between the connection time-out settings, change the connection time-out value in IBM Cognos BI. The value must be smaller than the setting that is configured in the application server.

**Procedure**

1. Open the `c10_location/configuration/BIBusTK_Config.xml` file in a text editor.
2. Find the following string:
   
   `<BIBUSTK_CONNECTION_TIMEOUT>25000</BIBUSTK_CONNECTION_TIMEOUT>`
3. Change the value to 90% of the value specified for the application server.
   
   For example, WebSphere uses a default connection time-out value of 30 seconds. Calculate 90% of 30 seconds, which is 27 seconds. Change the string to:
   
   `<BIBUSTK_CONNECTION_TIMEOUT>27000</BIBUSTK_CONNECTION_TIMEOUT>`
4. Save the file.
5. Repeat these steps in each location where you installed IBM Cognos BI.

---

**Configure IBM Cognos components to run within the application server**

IBM Cognos Business Intelligence must be configured with the application server configuration information, and the configuration must be saved to create new cryptographic keys. IBM Cognos Configuration uses the Java Virtual Machine (JVM) that is defined by the JAVA_HOME environment variable.

You must set the JAVA_HOME environment variable to the JVM supplied or used by the application server before you run IBM Cognos Configuration.
If you are using IBM WebSphere, you can use the Build Application Wizard to create the application as well as install it. You do not have to use the IBM WebSphere administration console to set properties or install the application. For more information, see “Use the Build Application Wizard to build and install IBM Cognos on IBM WebSphere Application Server” on page 253.

**Procedure**

1. Stop the IBM Cognos service if it is running.
2. Start IBM Cognos Configuration:
   
   If you have existing incompatible encryption keys, you will be prompted to automatically generate new ones at this time.

   **Tip:** Ensure that the existing keys are backed up to a secure location before proceeding. There is no undo action available after you generate new keys.

3. Use the Build Application Wizard to create the application file that will be deployed to the application server. To launch the Build Application Wizard from IBM Cognos Configuration, under **Actions**, click **Build Application Files**. The wizard allows you to select the type of application to build and the context root used to access the application.

   You must build the application file on the same computer on which you will be deploying the file.

   The context root value entered in the wizard must be the same as is entered in the Environment tab, and used to deploy to the application server. For IBM Cognos BI, the default context root and application directory name is `p2pd`, which can be used in most cases. For the IBM Cognos Servlet Gateway, the default context root and application directory name is `ServletGateway`. Other default application deployment values, such as the application name, may be changed to better suit your environment.

   **Tip:** It is not necessary to rebuild or redeploy the archive file when you make configuration changes because configuration information is stored externally to the application.

   For WebLogic and JBoss, you can use the Build Application wizard in IBM Cognos Configuration to build the application to an expanded directory.

   For example, for WebLogic, you put the application in `C:\bea\user_projects\domains\apps\p2pd`, where `p2pd` is the name of the application. When deploying the application from the WebLogic Administration Console, you would select the `p2pd` directory.

   For JBoss, if you use the Expand files into a folder option, you must include the `.war` extension in the name of the folder where the wizard will create the `p2pd` application. When the wizard prompts for the folder location, go to `JBoss_location/server/instance_name/deploy` and create a folder named `p2pd.war`.

   For information about which type of application file, WAR, EAR or expanded directory, is supported in your environment, see your application server documentation.

4. In the **Explorer** window of IBM Cognos Configuration, expand **Environment** and then change the following properties to use the port number and host name or IP address of the server where the IBM Cognos BI component and application server are installed.

   - All URIs for the dispatcher, including
     - **Dispatcher URIs for Gateway**
– External dispatcher URI
– Internal dispatcher URI
– Dispatcher URI for external applications
• Gateway URI
• Content Manager URIs

The application server must be configured to listen on the host name or IP address entered in the URI. For more information, see your application server documentation.

If you change the context root from the default value of p2pd, you must change the context root portion of the URI as well.

5. Under Environment > IBM Cognos services, right-click IBM Cognos, and then click Delete.

The entry for the IBM Cognos service is used to configure environment settings for running under Tomcat. The entry is not required when using a different application server.

6. Complete other required configuration changes such as
   • specifying properties for the Content Manager database
   • entering user IDs and passwords

   If you used the default settings for the IBM Cognos installation, you may only have to make minor changes to the default configuration settings.

7. Save the configuration.

   New cryptographic keys are created using the JVM that is defined by the JAVA_HOME variable.

8. Close IBM Cognos Configuration.

Use the Build Application Wizard to build and install IBM Cognos on IBM WebSphere Application Server

Use the Build Application Wizard to build, install, and configure your IBM Cognos application on IBM WebSphere Application Server.

You can perform all of the actions in sequence, or you can perform them individually. The following task describes the process in sequence.

Before you begin

IBM WebSphere Application Server must be installed on the same computer as you have installed IBM Cognos BI.

You must set the JAVA_HOME environment variable to the JVM supplied or used by the application server before you run IBM Cognos Configuration.

IBM WebSphere Application Server does not need to be running to use the Build Application Wizard to install IBM Cognos BI.

Procedure

1. Start IBM Cognos Configuration.
2. In the Explorer window, under IBM Cognos services, right-click IBM Cognos, and click Delete.
4. Enter a Name, and select WebSphere in the Type box.
5. Click OK.
6. In the **WebSphere Application Server location** box, click the browse icon, and select the location of your IBM Websphere Application Server installation.
7. In the **Profile** box, select the name of the profile into which you want IBM Cognos BI installed.
   You can enter a new name in the **Profile** box. IBM Cognos Configuration will create a new profile using the name you enter.
   If a previous installation of IBM Cognos exists in the profile you select, the Build Application Wizard will allow you to uninstall the previous installation before installing the new one.
8. In the **Server Instance** box, select the server instance for your IBM WebSphere profile.
9. Right-click the name you gave your IBM WebSphere configuration, and click **Build**.
   The **Build Application Wizard** appears. Follow the instructions in the wizard and click the **Help** icon for more information for each page. The wizard will allow you to build the application, and install it to the IBM WebSphere profile.
   The application will be configured to run. For example, the path values will be added and the correct JVM settings will be applied.
   On the **Configure IBM Cognos for WebSphere** page, ensure that you enter the correct port numbers for the IBM WebSphere profile. The values are provided in the page. These values will be applied to the IBM Cognos Configuration **Environment** settings.
   **Tip:** To test your IBM WebSphere configuration, right-click the name you gave your IBM WebSphere configuration, and click **Test**. The dialog will show any configuration errors. Click the **Details** icon to view any messages.
10. Restart your IBM WebSphere profile.

You can uninstall your IBM Cognos application from IBM WebSphere from IBM Cognos Configuration. Right-click the name you gave your IBM WebSphere configuration, and click **Uninstall**.

---

**Identifying the JDK for WebLogic 9 on AIX**

WebLogic 9 requires Java Development Kit (JDK) 1.5. If you use WebLogic Server 9 on AIX, you must update the Java options in the commEnv.sh file to specify the appropriate serial version unique identifier (UID). If you do not make this update, a serial version UID mismatch occurs when using WebLogic Server 9 with IBM Java 5.

**Procedure**

1. Open the `WebLogic9_location/common/bin/commEnv.sh` file.
2. Modify the file to include the following command:
   ```bash
   JAVA_OPTIONS="${JAVA_OPTIONS}
   -Dcom.sun.xml.namespace.QName.useCompatibleSerialVersionUID=1.0"
   export JAVA_OPTIONS
   ```
3. Save and close the commEnv.sh file.
Change the application server startup script

Some application servers have specific requirements that you must meet before you can run IBM Cognos Business Intelligence. Depending on the application server, you may have to define environment variables, copy files, and add or change code in files.

If you are using Red Hat JBoss or Oracle WebLogic Server, you must make changes to the application server startup script.

If you are using IBM WebSphere Application Server, you do not have to change the startup script unless you want to add the environment variable changes. If you do make changes, use the administration console.

If your environment contains a JRE that you are using for other products, the JRE folder may contain .jar files that are not compatible with the .jar files that are provided with IBM Cognos BI. This may result in a failure to start IBM Cognos BI on your application server. In this situation, direct IBM Cognos BI to use the endorsed .jar files by including the following parameter in the Java command line:

-Djava.endorsed.dirs=${ibmcognos_home}/tomcat[version]/common/endorsed

Change the application server startup script for WebLogic

If you are using Oracle WebLogic Server, the startup script must be modified to specify Java Virtual Machine (JVM) settings. For WebLogic 9, use the Administration Console to modify the WebLogic environment.

Procedure

1. Create a WebLogic Server (WLS) domain for IBM Cognos BI.
   If you are configuring the IBM Cognos Servlet Gateway, create a second domain for this application.
   For information about creating domains, see the WebLogic documentation.

2. Go to the $WebLogic9_location/user_projects/domains/domain_name/bin directory and open the application server startup script in an editor.
   The name of the startup script may vary depending on the type of WebLogic installation performed. For example, in a managed server installation, the name of the startup script is startManagedWebLogic.sh or startManagedWebLogic.cmd.

3. For non-IBM JRE versions, select the JVM run mode, and change the default setting from JAVA_VM= to JAVA_VM=-server.

4. Modify the JAVA_OPTIONS to set the appropriate XML parser for IBM Cognos BI. Add the third line, as shown in this example:
   
   JAVA_OPTIONS=
   -Dweblogic.security.SSL.trustedCAKeyStore= %WL_HOME%/server\lib\cacerts
   -Dorg.xml.sax.driver=org.apache.xerces.parsers.SAXParser

5. Set the minimum and maximum memory used by the JVM.
   Typically, the memory is set using two JVM parameters: -Xms and -Xmx. A minimum of 256 MB and a maximum of 768 MB are suggested starting values. You can change these values to suit your environment.
   The MaxPermSize parameter must also be set. Here is an example:

   -XX:MaxPermSize=128m
For information about JVM parameters, see the JVM or application server documentation.

6. Ensure that the production mode is enabled by changing PRODUCTION_MODE= to PRODUCTION_MODE=true.

7. Save and close the file.

**Change the application server startup script for JBoss**

If you are using Red Hat JBoss, the startup script must be modified to specify Java Virtual Machine (JVM) settings. You must also specify a log4j argument.

For Red Hat JBoss, create a copy of the default server instance so that you can use the original default server instance as a backup. Give the copy a name that does not use spaces, such as cognos.

**Procedure**

1. Go to the JBoss_location/bin directory and open run.bat or run.sh in an editor.

2. Go to the JAVA_OPTS variable and add the following parameters:
   -Xms512m -Xmx1024m
   -XX:PermSize=64m -XX:MaxPermSize=256m
   -Dorg.jboss.resolver.warning=true
   -Dsun.rmi.dgc.client.gcInterval=3600000
   -Dsun.rmi.dgc.client.gcInterval=3600000
   -DLog4j.defaultInitOverride=true

   The minimum and maximum memory settings are suggested starting values. You can change these values to suit your environment. For information about these parameters, see the JVM or application server documentation.

3. For HP Itanium 64 bit, also add the following parameters:
   -Djava.library.path=/install_location/bin64
   -d64
   -Xss4m

   If SSL is enabled, increase the Java thread stack to 12 MB. For example, -Xss12m.

4. Save and close the file.

**Configure application server properties and install IBM Cognos components**

You must configure application server properties and install the IBM Cognos components on your application server.

**Install IBM Cognos on WebSphere**

Follow these steps to install on WebSphere.

**Procedure**

1. Start the WebSphere Application Server, and then access the WebSphere Administrative Console.

2. Create a new server instance into which the IBM Cognos Business Intelligence application will be deployed, if this option is available in the version you are running.

   If you are deploying the IBM Cognos Servlet Gateway, create a second separate server instance.
3. Install a new Enterprise Application using the application file that was built by IBM Cognos Configuration.

For IBM Cognos BI, the default context root is p2pd, which can be used in most cases. For the IBM Cognos Servlet Gateway, the default context root is ServletGateway. Other default application deployment values, such as the application name, may be changed to better suit your environment. The context root value used to deploy the application must be the same as the context root value entered in IBM Cognos Configuration when running the Build Application wizard.

4. Set the memory used by the JVM.

Usually, the memory is set by adding or changing the initial and maximum Java heap size. For information about these parameters, see the JVM or application server documentation.

**Tip:** A minimum of 256 MB and a maximum of 768 MB are suggested starting values. You can change these values to suit your environment.

5. Set other JVM options, if required.

The JVM process can be tuned by specifying various options as arguments to the Java process. For information about the possible parameters, see the JVM documentation.

6. In the server properties, add an environment variable, as listed in the following table, that references the `installation_location/bin` directory.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Environment variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows</td>
<td>PATH</td>
</tr>
<tr>
<td>AIX</td>
<td>LIBPATH</td>
</tr>
<tr>
<td>Solaris</td>
<td>LD_LIBRARY_PATH</td>
</tr>
<tr>
<td>HP-UX</td>
<td>SHLIB_PATH</td>
</tr>
</tbody>
</table>

Ensure that you use the appropriate library files for the version of the IBM Cognos BI server that you install. IBM Cognos BI requires 32-bit library files when running in a 32-bit application server and it requires 64-bit library files when running in a 64-bit application server. Depending on the version of DB2 that you have installed, you may have to change the library files or change the order in which the library files are listed so that IBM Cognos BI server can find the correct files. Whichever version of library files are needed must be listed first.

7. Stop and then restart the WebSphere application server instance used for IBM Cognos components.

8. Verify that IBM Cognos components are running by looking for the following message in the application server admin console or in the application server log file:

   The dispatcher is ready to process requests.

**Install IBM Cognos on WebLogic**

Follow these steps to install on WebLogic.
**Procedure**

1. If you used the expanded directory option when building the application in IBM Cognos Configuration, go to step 2. If you created a WAR file, expand the application manually:
   - Create a directory in a location that is accessible to the application server, giving the directory the same name as the context root.
     For IBM Cognos BI, the default context root and application directory name is p2pd, which can be used in most cases. For the IBM Cognos Servlet Gateway, the default context root is ServletGateway. Other default application deployment values, such as the application name, may be changed to better suit your environment. The context root value used to deploy the application must be the same as the context root value entered in IBM Cognos Configuration.
   - From the directory you just created, extract the application WAR file to the WebLogic installation using the following command from a command prompt:
     ```
     WebLogic_location/jdk_version/bin/jar xvfm "installation_location/application.war"
     ```
     A space and then a period are required at the end of the command. In this command, the period does not refer to the current directory.

2. Start the WebLogic Administration Server and the WebLogic Managed Server associated with the IBM Cognos domain.
   Node Manager must be started before you can start and stop Managed Server instances using the Administration Console.

3. You must modify the environment in the WebLogic Administration Console before deploying IBM Cognos BI. Logon to the Administration Console and navigate to the Managed Server instance that will host the IBM Cognos BI application. Select the **Server Start** tab for the Managed Server instance and enable edit mode.

4. In the **Java Home** box, enter the path for the JVM. This value must be the same as is used for IBM Cognos BI. You must use the JVM that is included with the WebLogic installation.

5. Set the Java arguments.
   - The Java arguments include all JVM settings, such as memory settings specified using two JVM parameters: -Xms and -Xmx.
   - The MaxPermSize must also be set. You must also set the appropriate XML parser for IBM Cognos BI.
   - For example, in the **Arguments** box, type
     ```
     -Xms768m -Xmx768m -XX:MaxPermSize=128m
     -Dorg.xml.sax.driver=org.apache.xerces.parsers.SAXParser
     ```
     If you use WebLogic on AIX, you must also specify the appropriate serial version UID in the Java arguments. If you do not make this update, a serial version UID mismatch occurs when using WebLogic with Java 5 because WebLogic requires JDK 1.5.
     - For example, in the **Arguments** box, type
     ```
     -Xms768m -Xmx768m -XX:MaxPermSize=128m
     -Dorg.xml.sax.driver=org.apache.xerces.parsers.SAXParser
     -Dcom.sun.xml.namespace.QName.useCompatibleSerialVersionUID=1.0
     ```
   - For information about JVM parameters, see the JVM or application server documentation.

6. Save and apply the changes.
You can now start and stop the Managed Server instance from the Control tab.

7. Start the server instance. The server instance must be started before deploying IBM Cognos BI or IBM Cognos Servlet Gateway.

8. Deploy the IBM Cognos BI or IBM Cognos Servlet Gateway application in the WebLogic console using a new Web application as follows:
   - Set the application name.
     For example, ibmcognos
   - Set the path to the directory where the expanded application files are located.

   **Note:** IBM Cognos BI uses a custom loader. You must use the expanded directory option when deploying.
   - Select the target server instance.
     Use the Administration Server only for WebLogic administration tasks and deploy the IBM Cognos BI application to its own Managed Server instance.

9. After the deployment has completed successfully, set the reload period for the Web application to -1 to improve performance. This will prevent WebLogic from checking for updated application files that are used only in a development environment.

10. Stop and then restart the WebLogic Managed Server associated with the IBM Cognos domain to activate the changes.

11. Verify that IBM Cognos components are running by looking for the following message in the application server console window or in the application server log file:
   
   The dispatcher is ready to process requests.

---

**Install IBM Cognos on SAP NetWeaver**

Follow these steps to install on SAP NetWeaver.

**Procedure**

1. Open the configuration tool by typing
   
   drive:\usr\sap\sapid\JCxx\j2ee\configtool\configtool.bat

   For example, if the SAP ID is J2E and the installation is on drive D, you would type
   
   D:\usr\sap\J2E\JC00\j2ee\configtool\configtool.bat

2. When prompted to use the default DB settings, click Yes.

3. Under **cluster-data, instance_IDxxxxxx, Dispatcher_IDxxxxxx, services**, where xxxxxxx is the ID number for your installation, highlight http.

4. Under **Global Properties**, highlight KeepAliveTimeout and type a higher number and then click Set.

   **Tip:** We suggest an initial KeepAliveTimeout number of at least 60.


6. Set the memory used by the JVM.
   
   Follow the recommendations from SAP. For more information, see SAP Note 723909 in the SAP Support Portal.
   
   If your computer has less than 1.5 GB of memory, you may have issues when you run SAP NetWeaver. We suggest a minimum value of 768 MB.

7. In the Java parameters box, set the XML parser as follows:
8. For IBM Cognos BI environments that use Report Studio, under cluster-data, instance_IDxxxxxx, highlight Server_IDxxxxxx, services, and highlight http.

9. Under Global Properties, highlight CompressedOthers, type false, and then click Set.

10. Save the changes.
    You are prompted to restart the server.

11. Restart the server by using the SAP Management Console or by restarting the services in Services.

12. Use the Deploy tool to create a new project.

13. Load the IBM Cognos application file you created using IBM Cognos Configuration. By default, the file is named p2pd.ear for IBM Cognos BI and ServletGateway.ear for IBM Cognos Servlet Gateway.

14. Using the Deploy tool, connect to the Administration tool and deploy the application file.

15. When you are prompted to start the application, click Yes.

16. Save the project.

Install IBM Cognos on JBoss

Follow these steps to install on JBoss.

Procedure

1. If you do not want to use the default port of 8080, open the 
   JBoss_location/server/instance_name/deploy/jbossweb-tomcat55.sar/server.xml 
   file.

2. In the server.xml file, change the default port number of 8080 used by the server instance to the port specified in IBM Cognos Configuration. For example,

   <Service name="jboss.web" 
   className="org.jboss.web.tomcat.tc5.StandardService"> 
   <!-- A HTTP/1.1 Connector on port 8080 --> 
   <Connector port="8080" address="${jboss.bind.address}" 
   maxThreads="250" strategy="ms" maxHttpHeaderSize="8192" 
   emptySessionPath="true" 
   enableLookups="false" redirectPort="8443" acceptCount="100" 
   connectionTimeout="20000" disableUploadTimeout="true"/>

3. Save and close the server.xml file.

4. Put the p2pd application in the JBoss_location/server/instance_name/deploy 
   folder, if it is not already in this location.

5. Start the application server.
    For jBoss 5.0, the default behaviour is to bind its services to the localhost (127.0.0.1). However, this may cause errors when you access your IBM Cognos BI application. To avoid these errors, add the -b attribute when you start the server. For example, use a command like

    run.bat -c <server_name> -b #.#.#.#

    In a test environment, to run jBoss 5.0 with legacy behaviour, you can use -b 0.0.0.0, which binds to all available interfaces.

Important: For a production environment, ensure that you secure your application server properly and do not use -b 0.0.0.0 as the binding address. For more information, see the jBoss documentation.
The p2pd application is automatically detected and started by the application server.

6. Verify that IBM Cognos components are running by looking for the following message in the application server console window or in the application server log file:
   The dispatcher is ready to process requests.

Enabling the secure socket layer

If you use the Secure Socket Layer (SSL) for IBM Cognos components, you must also enable SSL in the application server environment. You then identify the SSL server certificate to Cognos components.

Before you begin

On UNIX or Linux operating systems, ensure that you set a JAVA_HOME environment variable before you use the ThirdPartyCertificateTool.

On Microsoft Windows operating systems, run the tool with -java:local to use the JRE that is provided with the installation. For example,

ThirdPartyCertificateTool.bat -java:local -T -i -r ...

Procedure

1. Configure the application server to use SSL.
   An SSL server certificate is generated by another certificate authority (CA). The certificate of the CA that generated the SSL server certificate is also provided.
   For more information about configuring the application server to use SSL, refer to the application server documentation. For information about using CA certificates with your application server, see the CA documentation.

2. Copy the CA certificate to the c10_location/bin directory and rename the file to ca.cer.
   This file must be Base-64 encoded X.509 format.

3. From the c10_location/bin directory:
   • On Microsoft Windows operating system, type:
     ThirdPartyCertificateTool.bat -T -i -r ca.cer -k ../configuration/signkeypair/jCAKeystore -p NoPassWordSet
   • On UNIX or Linux operating systems, type:
     ThirdPartyCertificateTool.sh -T -i -r ca.cer -k ../configuration/signkeypair/jCAKeystore -p NoPassWordSet

Restriction: Ensure that the user who runs the script has read access to the directory where the certificate is stored and read access to the certificate file. Otherwise, you might see an error similar to the following error message:
Exception in thread "main" java.lang.NullPointerException error when you import the certificate.

You must type jCAKeystore as the name of the CA keystore.

Configuring web communication

For most types of supported application servers, you use a web server and an IBM Cognos gateway for Web communication.
For information about configuring the web server, see “Configuring the web server” on page 73.

For information about configuring the WebSphere Web server plugin, see the IBM Cognos Customer Center (http://www.ibm.com/software/data/cognos/customercenter/).

If you are using SAP NetWeaver on Microsoft Windows and you are not using a Web Server and an IBM Cognos gateway for web communication, follow the steps to configure a virtual directory.

Configure virtual directory for SAP NetWeaver

If you are using SAP NetWeaver and you are not using a web Server and an IBM Cognos gateway for web communication, you must create a virtual directory, also known as a web alias.

This virtual directory is required to allow the static content (html pages, images, and so on) to load. When building the IBM Cognos application file, select the option to include the static files from the webcontent folder. Create a virtual directory that uses the context root value as a name (by default, p2pd for IBM Cognos Business Intelligence or ServletGateway for the IBM Cognos Servlet Gateway). Ensure the virtual directory points to the c10_location/webcontent folder.

Procedure

Create the virtual directory listed in the following table:

<table>
<thead>
<tr>
<th>Alias</th>
<th>Location</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>context_root (for example, p2pd)</td>
<td>c10_location/webcontent</td>
<td>Read</td>
</tr>
</tbody>
</table>

Unregister dispatchers that were configured for Tomcat

If you are installing IBM Cognos BI to an application server after you have already started the product with Tomcat, you will have dispatchers registered in the content store. You must unregister any dispatchers that were previously registered for Tomcat.

You remove dispatchers using IBM Cognos Administration.

Procedure

1. Open IBM Cognos Connection by connecting to the IBM Cognos Business Intelligence portal and clicking IBM Cognos Content on the Welcome page.
2. Click Launch > IBM Cognos Administration.
3. On the Configuration tab, click Dispatchers and Services.
4. For the dispatcher you want to unregister, from the Actions column, click More.
5. Click Unregister.
6. In the confirmation dialog box, click OK.
Upgrade to IBM Cognos BI in an application server environment

If you are upgrading from a supported release to IBM Cognos Business Intelligence, perform the following steps.

Procedure

1. **Back up your existing IBM Cognos information**
2. Use the administrative tools for your application server to undeploy the existing IBM Cognos application.
   
   For information about undeploying applications, see your application server documentation.
   
   If the directory to which the existing IBM Cognos application was originally deployed is not removed during the undeploy process, delete the directory.
   
   Also, remove any IBM Cognos .jar files that are cached in your application server environment.
3. Uninstall the existing version.
4. Install the new version of IBM Cognos BI.
5. Follow the appropriate instructions in this chapter for changing to your application server.
   
   Most installations must perform the following:
   
   • "Configure IBM Cognos components to run within the application server" on page 251
   
   • Configure application server properties and deploy IBM Cognos BI
6. To activate new features after upgrading, save the configuration in IBM Cognos Configuration, and then restart the services.
Chapter 12. Using an unattended installation and configuration

Use an unattended installation and configuration to do the following:
• install an identical configuration across several computers on your network
• automate the installation and configuration process by specifying options and settings for users
• install and configure components in a UNIX or Linux environment that does not have XWindows

Before you set up an unattended installation and configuration, ensure that all the system requirements and prerequisites are met and that all other software that you need is installed and configured.

You can also set up an unattended uninstallation.

Procedure
1. Configure a transfer specification file (.ats) to specify installation options.
2. Run the installation tool in silent mode.
3. Use a pre configured configuration file from another computer.
4. Run the configuration tool in silent mode.

Results
After you complete these tasks, ensure that the IBM Cognos Business Intelligence installation directory on all computers is protected from unauthorized or inappropriate access. Then you will be ready to use IBM Cognos BI.

Unattended installations
You use a transfer specification file to copy IBM Cognos BI components to your computer without being prompted for information.

Each time you install IBM Cognos BI components using the installation wizard, the options you select are recorded in a transfer specification file. Therefore, if you already installed IBM Cognos BI components on a sample computer, you can use the generated transfer specification file as a template for unattended installations on different computers.

If you do not use the installation wizard to install components, you can use the default transfer specification file named response.ats. You must modify the response.ats file for your environment before you can use it for an unattended installation.

You can check if the unattended installation was successful by checking the return status. A value of zero (0) indicates success and all other values indicate that an error occurred.
Use a response file from an installation on another computer

Use the following steps to duplicate an installation from one computer to another without being prompted for information.

**Procedure**

1. Use the installation wizard to install IBM Cognos BI components on one computer.
2. After the installation has completed, go to `c10_location/instlog`.
3. Locate the transfer specification file (.ats) that was generated during the installation.
   The filename format is `ts-product_code-version-yyyyymmdd_hhmm.ats`.
   Where `product_code` is as listed in the following table:

<table>
<thead>
<tr>
<th>Product_code</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>BISRVR</td>
<td>IBM Cognos BI Server</td>
</tr>
<tr>
<td>CRNSRVR</td>
<td>IBM Cognos BI Reporting Server</td>
</tr>
<tr>
<td>BIMODEL</td>
<td>IBM Cognos Framework Manager</td>
</tr>
<tr>
<td>BISAMPLES</td>
<td>Samples</td>
</tr>
<tr>
<td>LP</td>
<td>Supplementary Language Documentation</td>
</tr>
</tbody>
</table>

4. Copy the generated transfer specification file to the computer where you plan to install IBM Cognos BI.
5. On the computer where you plan to install the software, do one of the following:
   - Insert the appropriate product installation disk, and copy the contents of the disk to your computer.
   - Copy the product installation files you downloaded to your computer.
6. Open the transfer specification file in a text editor.
7. In the License Agreement dialogs, change the I Agree property to y.
   This action means that you are accepting the license agreement. To read the terms of the license agreement, see the `LA_language_code` and notices files in either of these locations:
   - on the product disk in the root installation directory for the operating system
   - on the computer from which you copied the transfer specification file in the `c10_location\license\product` directory
8. Save the transfer specification file in the directory where you copied the installation files.
9. In a command or terminal window, go to the operating system directory where you copied the installation files.
10. Type the following command:
    - On Windows, type the following, where `location` is the directory where you copied the `filename.ats` file:
      ```
      issetup -s location\filename.ats
      ```
    - On UNIX or Linux, type:
      ```
      ./issetup -s location/filename.ats
      ```
    - On UNIX or Linux where you do not have XWindows, type:
Results

If a return status other than zero (0) is returned, check the log files for error messages. Errors are recorded in the c10_location\instlog directory in a summary error log file. The filename format is tl-product_code-version-yyyymmdd-hhmm_summary-error.txt.

If errors occur before sufficient initialization occurs, log messages are sent to a log file in the Temp directory. The filename format is tl-product_code-version-yyyymmdd-hhmm.txt.

After all errors are resolved, you can **set up an unattended configuration**

Modifying a response file

Generate and modify a response file to specify and record your installation preferences. You can also modify the response file template that is provided.

Procedure

1. On the computer where you plan to install the software, do one of the following:
   - Insert the appropriate product installation disk, and copy the contents of the disk to your computer.
   - Copy the product installation files you downloaded to your computer.
2. Use a response.ats file.
   - To use the response file that is provided with the installation, go to the directory for your operating system and find the response.ats file.
   - On UNIX computers, to generate the a response.ats file, go to the directory for your operating system and type ./issetup -ats filename
   - On Windows computers, to generate the a response.ats file, go to the directory for your operating system and type issetup -ats filename
3. Open the response.ats file in a text editor.
   Each section in the file corresponds to a dialog box in the installation wizard.
4. In the License Agreement dialogs, change the I Agree property to y.
   This action means that you are accepting the license agreement. To read the terms of the license agreement, see the LA_language_code and notices files in either of these locations:
   - on the product disk in the root installation directory for the operating system
   - on the computer from which you copied the transfer specification file in the c10_location\license\product directory
5. Type the installation location in APPDIR=location.

**Tip:** There should be no space on either side of the equal sign, (=).
6. In the [Component List] section, enter 1 for each component you want to install. Enter 0 if you do not want to install the component.
7. For a Windows installation, for the APPFOLDER= property, type a name for the Start menu shortcut.

**Tip:** To ensure that the shortcut folder is visible to all users, type 1 for the ALLUSERS_FLAG= property.
8. For the install information in the [Install Conditions] section, enter 1 if the condition is true. Enter 0 if the condition is false.

9. Save the response.ats file to a local directory after you make the necessary changes.

What to do next

When you are ready to run the silent installation, go to "Starting an unattended installation."

Starting an unattended installation

You can start an unattended installation and either choose to display or not display messages during the installation process.

Procedure

1. Go to the directory where you saved the response.ats file.
2. At the command prompt, type one of the following commands:
   - On Windows, type the following, where location is the directory where you copied the filename.ats file:
     ```
     isetup -s location\filename.ats
     ```
     To bypass displaying messages on the screen, you can add the -nomsgboxes option to the isetup command. For example, to start a silent installation by using the default response.ats file with no messages displayed during the installation, type: isetup -s -nomsgboxes.
   - On UNIX or Linux, type:
     ```
     ./isetup -s location/filename.ats
     ```
   - On UNIX or Linux where you do not have XWindows:
     ```
     ./isetupnx -s location/filename.ats
     ```

   Note: In a UNIX or Linux environment, to view the status of the installation on the screen, you can add the -displayLog option to the isetupnx command. For example, to start a silent installation by using the default response.ats file and display the status, type: ./isetup -s -displayLog.

Results

If a return status other than 0 (zero) is returned, check the log files for error messages. Errors are recorded in the c10_location\instlog directory in a summary error log file. The filename format is t1-product_code-version-yyyyymmdd-hhmm_summary-error.txt.

If errors occur before sufficient initialization occurs, log messages are sent to a log file in the Temp directory. The filename format is t1-product_code-version-yyyyymmdd-hhmm.txt.

After all errors are resolved, you can set up an unattended configuration.

Use an unattended configuration

To use an unattended configuration, you must export a configuration from an existing installation that has the same IBM Cognos BI components installed. You can then run IBM Cognos Configuration in silent mode.
The exported configuration contains the properties of the IBM Cognos BI components that you installed on one computer. If you made changes to the global configuration settings, you must also copy the global configuration file to the computer where you plan to use the unattended configuration. Global configuration includes such settings as content locale, product locale, currencies, fonts, and cookie settings.

For more information, see “Changing Global Settings” on page 223.

**Before you begin**

Ensure that the configuration settings on the computer where you are exporting the configuration are appropriate to use on another computer with the same installed components. For example, if you changed the host name portion of the Gateway URI property from localhost to an IP address or computer name, ensure this setting is appropriate for the new computer’s configuration.

**Procedure**

1. In IBM Cognos Configuration, from the File menu, click Export as.
2. When prompted about exporting decrypted content, click Yes.
3. If you want to export the current configuration to a different folder, in the Look in box, locate and open the folder.
4. In the File name box, type a name for the configuration file.
5. Click Save.
6. Copy the exported configuration file to the c10_location/configuration directory on the computer where you plan to use the unattended configuration.
7. Rename the file to cogstartup.xml.
8. If you changed the global configuration on the source computer, copy the coglocale.xml file to the c10_location/configuration directory on the computer where you plan to do the unattended configuration.
9. Go to c10_location/bin or c10_location/bin64 directory.
10. Type the following command:
   - On UNIX or Linux, type ./cogconfig.sh -s
   - On Windows, type cogconfig.bat -s

   **Tip:** To view log messages that were generated during an unattended configuration, see the cogconfig_response.csv file in the c10_location/logs directory.

   You can check if the unattended configuration was successful by checking the return status. A value of zero (0) indicates success and all other values indicate that an error occurred.

**Results**

IBM Cognos Configuration applies the configuration settings specified in the cogstartup.xml file, encrypts credentials, generates digital certificates, and if applicable, starts IBM Cognos service or process.
Use an unattended uninstallation

Use an unattended uninstallation to automate the removal of components on several computers that have the same components or remove components on a UNIX or Linux environment that does not have XWindows.

Procedure

1. Go to the c10_location/uninstall directory.
2. Open the file named uninst.ini in a text editor.
3. In the section named [Package List], enter 1 for each component you want to uninstall. Enter 0 if you want to leave the component installed.
   By default, all installed components are set to be removed.
   The packages listed in the [Package List] section are described in the following table:

<table>
<thead>
<tr>
<th>Package code</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>BISRVR</td>
<td>IBM Cognos BI Server</td>
</tr>
<tr>
<td>CRNSRVR</td>
<td>IBM Cognos BI Reporting Server</td>
</tr>
<tr>
<td>BIMODEL</td>
<td>Framework Manager</td>
</tr>
<tr>
<td>BISAMPLES</td>
<td>Samples</td>
</tr>
<tr>
<td>LP</td>
<td>Supplementary Language Documentation</td>
</tr>
</tbody>
</table>

4. Save and close the file.
5. From the command line, go to the c10_location\uninstall directory.
6. At the command prompt, type the following command:
   • On Windows, type
     uninst -u -s
   • On UNIX or Linux, type
     ./uninst -u -s
   • On UNIX or Linux without XWindows, type
     ./uninstnx -u -s
Chapter 13. Performance Maintenance

This section includes topics about using IBM Cognos Business Intelligence and other tools and metrics to maintain the performance of your IBM Cognos Business Intelligence environment.

System Performance Metrics

IBM Cognos BI provides system metrics that you can use to monitor the health of the entire system and of each server, dispatcher, and service. You can also set the thresholds for the metric scores. Some examples of system performance metrics are the number of sessions in your system, how long a report is in a queue, how long a Java Virtual Machine (JVM) has been running, and the number of requests and processes in the system.

System performance metrics reside in the Java environment, but can be monitored in IBM Cognos Administration through IBM Cognos Connection. For more information about monitoring system performance metrics, see the IBM Cognos Business Intelligence Administration and Security Guide.

You can take a snapshot of the current system metrics so that you can track trends over time or review details about the state of the system at a particular time. For more information, see the topic about the metric dump file in the IBM Cognos Business Intelligence Troubleshooting Guide.

You can also monitor system metrics externally to IBM Cognos Administration by using Java Management Extensions (JMX), a technology that supplies tools to manage and monitor applications and service-oriented networks.

Monitoring System Metrics Externally

You can monitor system metrics outside of IBM Cognos Administration by using industry standard Java Management Extensions (JMX). First, you configure two JMX properties in IBM Cognos Configuration to enable secure access to the metrics in the Java environment. Then you use a secure user ID and password to connect to the metrics through a JMX connection tool.

Before you begin

You must install Oracle Java SE Development Kit or the Java Software Development Kit from IBM before you can use the external monitoring feature.

Procedure

1. In the location where Content Manager is installed, start IBM Cognos Configuration.
2. In the Explorer window, click Environment.
3. In the Properties window, under Dispatcher Settings, click External JMX port.
4. In the Value column, type an available port number.
5. Click External JMX credential.
6. In the Value column, click the edit icon, type a user ID and password, and then click OK.
The user ID and password ensure that only an authorized user can connect to
the system metrics data in the Java environment, using the port specified in
**External JMX port**.

7. Save the changes and restart the service.

8. To access the system metrics data, specify the following information in the JMX
connection tool:
   - the URL to connect to the system metrics data
     For example,
     ```
     service:jmx:rmi://Content_Manager_server/jndi/rmi://
     monitoring_server:<JMXport>/proxyserver
     ```
     where JMXport is the value that you typed for **External JMX port**, and
     **Content_Manager_server** and **monitoring_server** are machine names. Do not use
     localhost, even if connecting locally.
   - the user ID and password to secure the connection
     Use the same values that you configured for **External JMX credential**.

**Enabling Only Services That are Required**

If some IBM Cognos BI services are not required in your environment, you can
disable them to improve the performance of other services.

For example, to dedicate a computer to running and distributing reports, you can
disable the presentation service on an Application Tier Components computer.
When you disable the presentation service, the performance of the Application Tier
Components will improve.

**Note:**
- The Presentation service must remain enabled on at least one computer in your
  IBM Cognos BI environment.
- If you want to use Query Studio, you must enable the Presentation service.
- If you want to use Analysis Studio, you must enable the Report service.
- If some IBM Cognos BI components are not installed on a computer, you should
disable the services associated with the missing components. Otherwise the IBM
  Cognos BI components will randomly fail.

**IBM Cognos services**

After you install and configure IBM Cognos BI, one dispatcher is available on each
computer by default. Each dispatcher has a set of associated services, listed in the
following table.

**Table 65. IBM Cognos services**

<table>
<thead>
<tr>
<th>Service</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent service</td>
<td>Runs agents. If the conditions for an agent are met when the agent runs, the agent service asks the monitor service to run the tasks.</td>
</tr>
<tr>
<td>Annotation service</td>
<td>Enables the addition of commentary to reports via the IBM Cognos Workspace. These comments persist across versions of the report.</td>
</tr>
</tbody>
</table>
### Table 65. IBM Cognos services (continued)

<table>
<thead>
<tr>
<th>Service</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batch report service</td>
<td>Manages background requests to run reports and provides output on behalf of the monitor service.</td>
</tr>
<tr>
<td>Content Manager cache service</td>
<td>Enhances the overall system performance and Content Manager scalability by caching frequent query results in each dispatcher.</td>
</tr>
</tbody>
</table>
| Content Manager service       | • Performs object manipulation functions in the content store, such as add, query, update, delete, move, and copy  
<pre><code>                           | • Performs content store management functions, such as import and export |
</code></pre>
<p>| Data movement service         | Manages the execution of data movement tasks in IBM Cognos BI. Data movement tasks, such as Builds and JobStreams, are created in Data Manager Designer and published to IBM Cognos BI. |
| Delivery service              | Sends emails to an external SMTP server on behalf of other services, such as the report service, job service, agent service, or data integration service |
| Event management service      | Creates, schedules, and manages event objects that represent reports, jobs, agents, content store maintenance, deployment imports and exports, and metrics |
| Graphics service              | Produces graphics on behalf of the Report service. Graphics can be generated in 4 different formats: Raster, Vector, Microsoft Excel XML or PDF |
| Human task service            | Enables the creation and management of human tasks. A human task such as report approval can be assigned to individuals or groups on an ad hoc basis or by any of the other services. |
| Index data service            | Provides basic full-text functions for storage and retrieval of terms and indexed summary documents. |
| Index search service          | Provides search and drill-through functions, including lists of aliases and examples. |
| Index update service          | Provides write, update, delete, and administration functions. |
| Job service                   | Runs jobs by signaling the monitor service to run job steps in the background. Steps include reports, other jobs, import, exports, and so on. |</p>
<table>
<thead>
<tr>
<th>Service</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Log service          | Records log messages generated by the dispatcher and other services. The log service can be configured to record log information in a file, a database, a remote log server, Windows Event Viewer, or a UNIX system log. The log information can then be analyzed by customers or by Cognos Software Services, including:  
  - security events  
  - system and application error information  
  - selected diagnostic information |
| Metadata service     | Provides support for data lineage information displayed in Cognos Viewer, Report Studio, Query Studio, and Analysis Studio. Lineage information includes information such as data source and calculation expressions. |
| Metric Studio service| Provides the Metric Studio user interface for monitoring and entering performance information                                                                                             |
| Migration service    | Manages the migration from IBM Cognos Series 7 to IBM Cognos BI.                                                                              |
| Monitor service      |  
  - Manages the monitoring and execution of tasks that are scheduled, submitted for execution at a later time, or run as a background task  
  - Assigns a target service to handle a scheduled task. For example, the monitor service may ask the batch report service to run a report, the job service to run a job, or the agent service to run an agent.  
  - Creates history objects within the content manager and manages failover and recovery for executing entries |
| PowerPlay service    | Manages requests to run PowerPlay reports.                                                                                               |
| Presentation service |  
  - Transforms generic XML responses from another service into output format, such as HTML or PDF  
  - Provides display, navigation, and administration capabilities in IBM Cognos Connection                                                  |
| Query service        | Manages Dynamic Query requests and returns the result to the requesting batch or report service.                                            |
| Report data service  | Manages the transfer of report data between IBM Cognos BI and applications that consume the data, such as IBM Cognos BI for Microsoft Office and IBM Cognos Mobile. |
Table 65. IBM Cognos services (continued)

<table>
<thead>
<tr>
<th>Service</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report service</td>
<td>Manages interactive requests to run reports and provides output for a user in IBM Cognos Connection or a studio.</td>
</tr>
<tr>
<td>Repository service</td>
<td>Manages requests to retrieve archived report output from an archive repository or object store.</td>
</tr>
</tbody>
</table>

**Tuning a DB2 Content Store**

If you use a DB2 database for the content store, you can take steps to improve the speed with which requests are processed.

By default, DB2 assigns tables that contain large objects (LOBS) to a database-managed tablespace. As a result, the LOBS are not managed by the DB2 buffer pools. This results in direct I/O requests on the LOBS, which affects performance. By reassigning the tables that contain LOBS to a system-managed tablespace, you reduce the number of direct I/O requests.

Before changing a DB2 content store, allocate sufficient log space to restructure the database.

To reconfigure the DB2 content store, do the following:

- Export the data from the tables that contain at least one large object (LOB).
- Create the tables in a system-managed table space.
- Import the data into the tables.

**Adjusting the Memory Resources for the IBM Cognos Service**

To improve performance in a distributed environment, you can change the amount of resources that the IBM Cognos service uses.

By default, the IBM Cognos service is configured to use minimal memory resources to optimize startup time.

The configuration settings for the IBM Cognos service apply only to Tomcat, the application server that IBM Cognos BI uses by default. If you want to configure IBM Cognos BI to run on another application server, do not use IBM Cognos Configuration to configure the resources. Instead, configure the resources within that application server environment.

The IBM Cognos service is available only on the computers where you installed Content Manager or the Application Tier Components.

**Procedure**

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, expand **Environment > IBM Cognos services**, and then click **IBM Cognos**.
3. In the **Properties** window, change the value for **Maximum memory in MB**.
   - To reduce the startup time, memory footprint, and resources used, use the default setting of 768.
To balance between fast startup time and quick operating speeds, type a value about 1.5 times the default value, such as 1152.

To maximize operating speeds and if performance is more important than fast startup time, and if your computer has a lot of resources, type a value about double the default value, such as 1536.

4. From the File menu, click Save.

Reducing the number of requests per process

Use the following steps to reduce the number of requests per process for an instance of the IBM Cognos service.

Procedure
1. Go to the c10_location/webapps/p2pd/WEB-INF/services directory.
2. Open the reportservice.xml file in an XML editor.
3. Change the value for default_process_use_limit from 0 (unlimited) to a fixed number of requests.
4. Save the file.
5. Restart the IBM Cognos service.
6. If you deployed IBM Cognos BI to an application server, rebuild the application file and deploy it to the application server.
   For example, for WebSphere, regenerate the EAR file and deploy it to the WebSphere application server.

Tune Apache Tomcat settings for 64-bit installations

If you are using Apache Tomcat on a 64-bit installation, you can edit the maxThreads and acceptCount settings to improve performance.

Procedure
1. Go to the c10_location/tomcat/conf directory.
2. Open the server.xml file.
3. Find the line <Connector port="9300" protocol="HTTP/1.1".
4. In that section, change the following values:
   a. Change maxThreads="500" to maxThreads="1500"
   b. Change acceptCount="500" to acceptCount="100"
5. Save the file.
6. Restart your IBM Cognos services.

Increase the Request-handling Capacity for Cognos Content Database

Cognos Content Database is configured for use with a small system. If you use Cognos Content Database in a large system, where the number of simultaneous requests is greater than ten, you must adjust the default JVM memory settings and increase the page cache size for Derby.

Procedure
1. On the computer where you have installed the Cognos Content Database component, go to the c10_location\bin directory.
2. Open the derby.bat file (on Windows) or derby.sh file (on UNIX or Linux).
3. Find the following line:
set MEM_SETTINGS=-Xmx256m
and change it to the following:
set MEM_SETTINGS="-Xmx1152m -XX:MaxPermSize=128M -XX:MaxNewSize=576m
-XX:NewSize=288m"

4. In the c10_location/configuration directory, rename derby.properties.sample to derby.properties.
5. In the same directory, open the derby.properties file.
6. Comment out the following line:
derby.storage.pageCacheSize=15000

---

**Improve Metric Store Database Performance**

IBM Cognos BI provides a script called cmm_update_stats that updates your metric store database indexes, which improves performance. Typically, you use this script before or after loading data when the volume or distribution of data has changed significantly. For example, performance may improve if you run this script after increasing the number of scorecards from 100 to 1000.

**Procedure**

1. Ensure that there is no activity in the metric store database.
2. Go to the following directory:
c10_location/configuration/schemas/cmm
3. Go to the appropriate database directory.
4. Depending on the database type, run one of the following scripts from the command line:
   - For Microsoft SQL Server or DB2:
cmm_update_stats host_name metric_store_name Admin_user_name password
   - For Oracle:
cmm_update_stats metric_store_name Admin_user_name password

---

**Reduce Delivery Time for Reports in a Network**

Reports that are distributed globally take longer to open in remote locations than to open locally. In addition, HTML reports take longer than PDF reports to open because more requests are processed for HTML reports.

You can reduce the amount of time for reports to open in remote locations in two ways. You can reduce the number of requests between the browser and the server by running the report in PDF format. If HTML reports are required, you can speed up the delivery of the report by configuring additional gateways in some of the remote locations. Static content, such as graphics and style sheets, will be delivered faster.

---

**Increase Asynchronous Timeout in High User Load Environments**

If you have a high user load (over 165 users) and interactive reports are running continuously in a distributed installation, you may want to increase the asynchronous timeout setting to avoid getting error messages. The default is 30000.

You may also want to set the Queue Time Limit setting to 360. For information, see the *IBM Cognos Business Intelligence Administration and Security Guide*.
To resolve this problem, increase the wait timeout.

**Procedure**

1. Go to the following directory:
   
   `c10_location/webapps/p2pd/WEB-INF/services/`

2. Open the `reportservice.xml` file in a text editor.
3. Change the `async_wait_timeout_ms` parameter to 120000.
4. Save the file.
5. Restart the service.
Chapter 14. Manually configuring IBM Cognos Business Intelligence on UNIX and Linux operating systems

The console attached to the UNIX or Linux operating system computer on which you are installing IBM Cognos Business Intelligence may not support a Java-based graphical user interface.

You must perform the following tasks manually:

- Change default configuration settings by editing the cogstartup.xml file, located in the $c10_location/configuration directory.
- Change language or currency support, or locale mapping by editing the coglocale.xml file, located in the $c10_location/configuration directory.
- Apply the configuration and the locale settings to your computer by running IBM Cognos Configuration in silent mode.

For all installations, some configuration tasks are required so that IBM Cognos BI works in your environment. If you distribute IBM Cognos BI components across several computers, the order in which you configure and start the computers is important.

Other configuration tasks are optional and depend on your reporting environment. You can change the default behavior of IBM Cognos BI by editing the cogstartup.xml file to change property values. You can also use sample files that enable IBM Cognos BI to use resources that already exist in your environment.

Manually change default configuration settings

If the console attached to your UNIX or Linux operating system computer does not support a Java-based graphical user interface, you must edit the cogstartup.xml file to configure IBM Cognos Business Intelligence to work in your environment.

Important: Some configuration settings are not saved in the cogstartup.xml file unless you use the graphical user interface. For example, the server time zone is not set for your IBM Cognos components when you modify the cogstartup.xml file directly and then run IBM Cognos Configuration in silent mode. In this case, other user settings that rely on the server time zone may not operate as expected.

If you want IBM Cognos BI to use a resource, such as an authentication provider that already exists in your environment, you can add a component to your configuration. You do this by copying the required XML code from the sample files into the cogstartup.xml file and then edit the values to suit your environment.

By default, the cogstartup.xml file is encoded using UTF-8. When you save the cogstartup.xml file, ensure that you change the encoding of your user locale to match the encoding used. The encoding of your user locale is set by your environment variables.

When you edit the cogstartup.xml file, remember that XML is case-sensitive. Case is important in all uses of text, including element and attribute labels, elements and values.

Before you edit the cogstartup.xml file, ensure that you
• make a backup copy
• create the content store on an available computer in your network
• review the configuration requirements for your installation type

Procedure
1. Go to the c10_location/configuration directory.
2. Open the cogstartup.xml file in an editor.
3. Find the configuration setting you want to change by looking at the help and
description comments that appear before the start tag of the <crn:parameter>
elements.
4. Change the value of the <crn:value> element to suit your environment.
   **Tip:** Use the type attribute to help you determine the data type for the
   configuration property.
5. Repeat steps 3 to 4 until the configuration values are appropriate your
   environment.
6. Save and close the file.

Results
You should now use a validating XML editor to validate your changes against the
rules in the cogstartup.xsd file, located in the c10_location/configuration.

Adding a component to your configuration
The cogstartup.xml file contains configuration settings used by IBM Cognos
Business Intelligence and by default components. You can change the components
that IBM Cognos BI uses by copying XML elements from sample files into the
cogstartup.xml file. You can then edit the configuration values to suit your
environment.

For example, to use an Oracle database for the content store, you can use the
ContentManager_language_code.xml sample file to replace the default database
connection information.

IBM Cognos BI can use only one instance at a time of the following elements:
• The database for the content store
• A cryptographic provider
• A configuration template for the IBM Cognos service

You should be familiar with the structure of XML files before you start editing
them.

Procedure
1. Go to the c10_location/configuration/samples directory.
2. Choose a sample file to open in an editor:
   • To use Oracle, DB2, or Sybase for the content store, open the
     ContentManager_language_code.xml file.
   • To use an authentication provider, open the
     Authentication_language_code.xml file.
   • To use a cryptographic provider, open the Cryptography_language_code.xml
     file.
• To send log messages somewhere other than a file, open the Logging_language_code.xml file.
• To use a medium or large template for the amount of resources the IBM Cognos BI process uses, open the CognosService_language_code.xml file.

3. Copy the elements that you need.

   Tip: Ensure that you copy the code including the start and end tags for the <crn:instance> element.
   For example, look for the (Begin of) and (End of) comments:
   <!--
   (Begin of) DB2 template
   -->
   <crn:instance ...>
   ...
   </crn:instance>
   <!--
   End of) DB2 template
   -->

4. Go to the c10_location/configuration directory.
5. Open the cogstartup.xml file in an editor.
6. Paste the code from the sample file to the cogstartup.xml file and replace the appropriate <crn:instance> element.
7. Change the values of these new elements to suit your environment.
   For the <crn:instance> element, do not change the class attribute. You can change the name attribute to suit your environment.
   For example, if you use an Oracle database for the content store, change only the name attribute to suit your environment.
   <crn:instance class="Oracle" name="MyContentStore">
8. Save and close the file.
9. Run IBM Cognos Configuration in silent mode by typing the following command:
   ./cogconfig.sh -s
   This ensures that the file is valid and that passwords are encrypted.

### Changing manually encrypted settings

You can manually change encrypted settings, such as passwords and user credentials, in the cogstartup.xml file.

To prompt IBM Cognos Configuration to save an encrypted setting, you change the value and then set the encryption flag to false.

**Procedure**

1. Go to the c10_location/configuration directory.
2. Open the cogstartup.xml file in an editor.
3. Find the encrypted setting you want to change by looking at the help and description comments that appear before the start tag of the <crn:parameter> elements.
4. Change the value of the <crn:value> element to suit your environment.
Tip: Use the type attribute to help you determine the data type for the configuration property.

5. Change the encryption value to false.
   For example,
   `<crn:value encrypted="false">`

6. Repeat steps 3 to 5 until the configuration values are appropriate for your environment.

7. Save and close the file.

8. Type the following configuration command:
   `./cogconfig.sh -s`

Results

The new settings are saved and encrypted.

Global settings on UNIX and Linux operating systems

If the console attached to your UNIX or Linux operating system computer does not support a Java-based graphical user interface, you must manually edit the `coglocale.xml` file.

You can change global settings
- to specify the language used in the user interface when the language in the user’s locale is not available
- to specify the locale used in reports when the user’s locale is not available
- to add currency or locale support to report data and metadata
- to add language support to the user interface

By default, IBM Cognos BI components ensure that all locales, which may come from different sources and in various formats, use a normalized form. That means that all expanded locales conform to a language and regional code setting.

Before you can add language support to the user interface, you must install the language files on all computers in your distributed installation. For more information, contact your support representative.

Example 1

A report is available in Content Manager in two locales, such as en-us (English-United States) and fr-fr (French-France), but the user locale is set to fr-ca (French-Canadian). IBM Cognos uses the locale mapping to determine which report the user sees.

First, IBM Cognos checks to see if the report is available in Content Manager in the user’s locale. If it is not available in the user’s locale, IBM Cognos maps the user’s locale to a normalized locale configured on the Content Locale Mapping tab.

Because the user’s locale is fr-ca, it is mapped to fr. IBM Cognos uses the mapped value to see if the report is available in fr. In this case, the report is available in en-us and fr-fr, not fr.

Next, IBM Cognos maps each of the available reports to a normalized locale. Therefore, en-us becomes en and fr-fr becomes fr.
Because both report and the user locale maps to fr, the user having the user locale fr-ca will see the report saved with the locale fr-fr.

Example 2

The user's locale and the report locales all map to the same language. IBM Cognos chooses which locale to use. For example, if a user's locale is en-ca (English-Canada) and the reports are available in en-us (English-United States) and en-gb (English-United Kingdom), IBM Cognos maps each locale to en. The user will see the report in the locale setting that IBM Cognos chooses.

Example 3

The report and the user locales do not map to a common language. IBM Cognos chooses the language. In this case, you may want to configure a mapping. For example, if a report is available in en-us (English-United States) and fr-fr (French-France), but the user locale is es-es (Spanish-Spain), IBM Cognos chooses the language.

Changing manually the global settings on UNIX and Linux operating systems

Use the following steps to change global settings on UNIX and Linux operating systems using the coglocale file.

Procedure

1. On every computer where you installed Content Manager, go to the c10_location/configuration directory.
2. Open the coglocale.xml file in an editor.
3. Add or modify the required element and attribute between the appropriate start and end tags.

The elements, attributes, and start and end tags are listed in the following table.

<table>
<thead>
<tr>
<th>Type of element</th>
<th>Start tag</th>
<th>End tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>&lt;supportedProductLocales&gt;</td>
<td>&lt;/supportedProductLocales&gt;</td>
</tr>
<tr>
<td>Content Locales</td>
<td>&lt;supportedContentLocales&gt;</td>
<td>&lt;/supportedContentLocales&gt;</td>
</tr>
<tr>
<td>Currency</td>
<td>&lt;supportedCurrencies&gt;</td>
<td>&lt;/supportedCurrencies&gt;</td>
</tr>
<tr>
<td>Product Locale Mapping</td>
<td>&lt;productLocaleMap&gt;</td>
<td>&lt;/productLocaleMap&gt;</td>
</tr>
<tr>
<td>Content Locale Mapping</td>
<td>&lt;contentLocaleMap&gt;</td>
<td>&lt;/contentLocaleMap&gt;</td>
</tr>
<tr>
<td>Fonts</td>
<td>&lt;supportedFonts&gt;</td>
<td>&lt;/supportedFonts&gt;</td>
</tr>
<tr>
<td>Cookie settings, archive location for reports</td>
<td>&lt;parameter name=&quot;setting&quot;&gt;</td>
<td>&lt;/parameter&gt;</td>
</tr>
</tbody>
</table>

Tip: To remove support, delete the element.
4. Save and close the file.
Results

Tip: Use a validating XML editor to validate your changes against the rules in the cogstartup.xsd file, located in the c10_location/configuration.

If you add a currency code that is not supported, you must manually add it to the i18n_res.xml file in the c10_location/bin/ directory. Copy this file to each IBM Cognos computer in your installation.

Starting and stopping Cognos BI in silent mode on UNIX and Linux operating systems

You run IBM Cognos Configuration in silent mode to apply the configuration settings and start the services on UNIX or Linux operating system computers that do not support a Java-based graphical user interface.

Before you run the configuration tool in silent mode, you should ensure the cogstartup.xml file is valid according to the rules defined in the cogstartup.xsd file. The cogstartup.xsd file is located in the c10_location/configuration directory.

Starting Cognos BI in silent mode on UNIX and Linux operating systems

Use the following steps to start the IBM Cognos Business Intelligence software in silent mode.

Procedure

1. Ensure that the cogstartup.xml file, located in the c10_location/configuration directory, has been modified for your environment.

   For more information, see “Manually change default configuration settings” on page 279.

2. Go to the c10_location/bin64 directory.

3. Type the following command

   ./cogconfig.sh -s

   Tip: To view log messages that were generated during an unattended configuration, see the cogconfig_response.csv file in the c10_location/logs directory.

Results

IBM Cognos Configuration applies the configuration settings specified in the cogstartup.xml file, encrypts credentials, generates digital certificates, and if applicable, starts the Cognos service or process.

Stopping Cognos BI in silent mode on UNIX and Linux operating systems

Use the following steps to stop the IBM Cognos Business Intelligence software in silent mode.
**Procedure**

1. Go to the `c10_location/bin64` directory.
2. Type the following command
   ```bash
   ./cogconfig.sh -stop
   ```

---

**Manually create an IBM Cognos application file**

IBM Cognos Business Intelligence and the servlet gateway must be packaged into an application file for deployment to supported application servers. IBM Cognos Business Intelligence provides a Build Application wizard that you can use to create the application file.

You can create a Web archive (.war) file, an Enterprise archive (.ear) file, or an expanded directory that includes all the files necessary for the application. For information about WAR and EAR files or expanded directories and to determine what is supported by your application server, see the documentation provided with the application server.

If you choose not to use the Build Application wizard, you must complete the following steps to create the application file.

If the application server is not being used as a Web server, you do not need to include the IBM Cognos static content (html pages, images, and so on) in the application file. Excluding the static content when creating the application file reduces the size of the file.

---

**Creating an IBM Cognos application file for the Business Intelligence software**

If you choose not to use the Build Application wizard, you must complete the following steps to create the application file.

**Procedure**

1. Stop the IBM Cognos service if it is running.
2. Go to the `c10_location/war/p2pd` directory.
3. Run the build script by using the following command syntax:
   ```bash
   build.bat file_type
   build.sh file_type
   ```
   where `file_type` can be one of the values listed in the following table:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>war</td>
<td>WAR file with static content</td>
</tr>
<tr>
<td>war_without_webcontent</td>
<td>WAR file with no static content</td>
</tr>
<tr>
<td>war_without_docsamples</td>
<td>WAR file with static content and with no documentation and sample files</td>
</tr>
</tbody>
</table>

*Table 67. A list of file type options and descriptions for an application file for the Business Intelligence software*
and where option can be one or more of the values listed in the following table:

Table 68. A list of options, values, and descriptions for an application file for the Business Intelligence software

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Dappserver_type=value</td>
<td>jboss</td>
<td>Perform actions for a JBoss application server</td>
</tr>
<tr>
<td></td>
<td>other (default)</td>
<td>Perform actions for a non-JBoss application server</td>
</tr>
<tr>
<td>-Dcontext_root=value</td>
<td>p2pd (default)</td>
<td>Preset a context root value for the application</td>
</tr>
<tr>
<td>-Dwar_name=value</td>
<td>path/filename</td>
<td>Path and name of the WAR file to be created</td>
</tr>
<tr>
<td></td>
<td>Default is ../../../p2pd.war</td>
<td>Path and name of the EAR file to be created</td>
</tr>
<tr>
<td>-Dear_name=value</td>
<td>path/filename</td>
<td>Path and name of the EAR file to be created</td>
</tr>
<tr>
<td></td>
<td>Default is ../../../p2pd.ear</td>
<td>Path to directory where the application files are to be expanded</td>
</tr>
</tbody>
</table>

Creating an IBM Cognos application file for a servlet gateway

If you choose not to use the Build Application wizard, you must complete the following steps to create the application file.
Procedure
1. Stop the IBM Cognos service if it is running.
2. Go to the c10_location/war/gateway directory.
3. Run the build script by using the following command syntax:
   - For Windows,
     build.bat file_type option
   - For UNIX or Linux,
     build.sh file_type option

   where file_type can be one of the values listed in the following table:

   Table 69. File type values and descriptions for an application file for a servlet gateway

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gateway_war</td>
<td>WAR file with static content</td>
</tr>
<tr>
<td>gateway_war_without_docsamples</td>
<td>WAR file with static content and with no documentation and sample files</td>
</tr>
<tr>
<td>gateway_ear</td>
<td>EAR file with static content</td>
</tr>
<tr>
<td>gateway_ear_without_docsamples</td>
<td>EAR file with static content and with no documentation and sample files</td>
</tr>
<tr>
<td>expand</td>
<td>directory containing the application with static content</td>
</tr>
<tr>
<td>expand_without_docsamples</td>
<td>directory containing the application with static content and with no documentation and sample files</td>
</tr>
</tbody>
</table>

   and where option can be one or more of the values listed in the following table:

   Table 70. Option values and descriptions for an application file for a servlet gateway

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Dappserver_type=value</td>
<td>jboss</td>
<td>Perform actions for a JBoss application server</td>
</tr>
<tr>
<td>-Dappserver_type=value</td>
<td>other (default)</td>
<td>Perform actions for a non-JBoss application server</td>
</tr>
<tr>
<td>-Dcontext_root=value</td>
<td>ServletGateway (default)</td>
<td>Preset a context root value for the application</td>
</tr>
<tr>
<td>-Dwar_name=value</td>
<td>path/filename</td>
<td>Path and name of the WAR file to be created</td>
</tr>
<tr>
<td></td>
<td>Default is</td>
<td>.../../ServletGateway.war</td>
</tr>
<tr>
<td>-Dear_name=value</td>
<td>path/filename</td>
<td>Path and name of the EAR file to be created</td>
</tr>
<tr>
<td></td>
<td>Default is</td>
<td>.../../ServletGateway.ear</td>
</tr>
</tbody>
</table>
Table 70. Option values and descriptions for an application file for a servlet gateway (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Dexpand_location=</td>
<td>path/directory</td>
<td>Path to directory where the application files are to be expanded</td>
</tr>
<tr>
<td>value=</td>
<td>Default is ..../temp/expand</td>
<td></td>
</tr>
</tbody>
</table>

Chapter 15. Uninstalling IBM Cognos BI

It is important to use uninstall programs to completely remove all files and modifications to system files. To uninstall IBM Cognos Business Intelligence, you uninstall server components and modeling tools.

If you are running IBM Cognos BI in an application server environment, use the administration tool provided with the application server to stop the application if it is running and undeploy the Java portion of IBM Cognos BI components. Many application servers do not completely remove all deployed application files or directories during an undeployment; therefore, you may have to perform this action manually. After you have undeployed IBM Cognos BI components, complete the steps in this section to uninstall on UNIX and Microsoft Windows operating systems.

Important: Do not delete the configuration and data files if you are upgrading to a new version of IBM Cognos BI and you want to use the configuration data with the new version.

Important: If you are using Cognos Content Database, the default location for the database files is in the `c10_location/contentstore` directory. If you want to keep your database after uninstalling, do not delete this directory.

Uninstall IBM Cognos Business Intelligence on UNIX or Linux operating systems

If you no longer require IBM Cognos Business Intelligence or if you are upgrading on your UNIX or Linux operating system, uninstall IBM Cognos BI.

Uninstalling does not remove any files that changed since the installation, such as configuration and user data files. Your installation location remains on your computer, and you retain these files until you delete them manually.

Procedure
1. If the console attached to your computer does not support a Java-based graphical user interface, determine the process identification (pid) of the IBM Cognos BI process by typing the following command:
   ```bash
   ps -ef | grep cogbootstrapservice
   ```
2. Stop the IBM Cognos BI process:
   - If you run XWindows, start IBM Cognos Configuration, and from the Actions menu, click Stop.
   - If you do not run XWindows, type:
     ```bash
     kill -TERM pid
     ```
3. To uninstall IBM Cognos BI, go to the `c10_location/uninstall` directory and type the appropriate command:
   - If you use XWindows, type:
     ```bash
     ./uninst -u
     ```
   - If you do not use XWindows, do an unattended uninstallation. For more information, see the IBM Cognos Business Intelligence Installation and Configuration Guide.
4. Follow the prompts to complete the uninstallation.
5. Delete all temporary Internet files from the Web browser computers.

**Uninstall IBM Cognos Business Intelligence on Microsoft Windows operating systems**

If you no longer require IBM Cognos Business Intelligence or if you are upgrading, uninstall all IBM Cognos BI components and the IBM Cognos service.

If you installed more than one component in the same location, you can choose the packages to uninstall using the uninstall wizard. All components of the package will be uninstalled. You must repeat the uninstallation process on each computer that contains IBM Cognos BI components.

It is not necessary to back up the configuration and data files on a Microsoft Windows operating system. These files are preserved during the uninstallation.

Close all programs before you uninstall IBM Cognos BI. Otherwise, some files may not be removed.

Uninstalling does not remove any files that changed since the installation, such as configuration and user data files. Your installation location remains on your computer, and you retain these files until you delete them. Do not delete the configuration and data files if you are upgrading to a new version of IBM Cognos BI and you want to use the configuration data with the new version.

**Procedure**

1. From the **Start** menu, click **Programs, IBM Cognos 10, Uninstall IBM Cognos, Uninstall IBM Cognos**.
   The **Uninstall** wizard appears.

   **Tip:** IBM Cognos BI is the default name of the Program Folder that is created during the installation. If you chose another name, go to that folder to find the program.

   On Microsoft Windows 8 or 2012 Server, go to the `c10_location\uninstall` directory, and double-click **Uninstall IBM Cognos**.

2. Follow the instructions to uninstall the components.
   The `cognos_uninst_log.htm` file records the activities that the Uninstall wizard performs while uninstalling files.

   **Tip:** To find the log file, look in the Temp directory.

3. Delete all temporary Internet files from the Web browser computers.
   For more information, see your Web browser documentation.
Appendix A. Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products. See the IBM Accessibility Center (http://www.ibm.com/able) for more information about the commitment that IBM has to accessibility.

Keyboard Shortcuts for the Installation Wizard

Keyboard shortcuts, or shortcut keys, provide you with an easier and often faster method of navigating and using software.

The installation wizard uses standard Microsoft Windows operating system navigation keys in addition to application-specific keys.

**Note:** The following keyboard shortcuts are based on US standard keyboards.

The following table lists the keyboard shortcuts that you can use to perform some of the main tasks in the installation wizard on the Windows operating system.

*Table 71. List of keyboard shortcuts on a Windows operating system*

<table>
<thead>
<tr>
<th>To do this</th>
<th>Press</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move to the next field on a page</td>
<td>Tab</td>
</tr>
<tr>
<td>Return to the previous field on a page</td>
<td>Shift+Tab</td>
</tr>
<tr>
<td>Close the installation wizard</td>
<td>Alt+F4</td>
</tr>
<tr>
<td>Move to the next configuration step</td>
<td>Alt+N</td>
</tr>
<tr>
<td>Return to the previous configuration step</td>
<td>Alt+B</td>
</tr>
<tr>
<td>Move to the next selection in a list</td>
<td>Down arrow</td>
</tr>
<tr>
<td>Move to the previous selection in a list</td>
<td>Up arrow</td>
</tr>
</tbody>
</table>

The following table lists the keyboard shortcuts you can use to perform some of the main tasks in the installation wizard on the UNIX or Linux operating system.

*Table 72. List of keyboard shortcuts on a UNIX or Linux operating system*

<table>
<thead>
<tr>
<th>To do this</th>
<th>Press</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move to the next field on a page</td>
<td>Tab</td>
</tr>
<tr>
<td>Return to the previous field on a page</td>
<td>Shift+Tab</td>
</tr>
<tr>
<td>Close the installation wizard</td>
<td>Alt+F4</td>
</tr>
<tr>
<td>Move to the next selection in a list</td>
<td>Down arrow</td>
</tr>
<tr>
<td>Move to the previous selection in a list</td>
<td>Up arrow</td>
</tr>
</tbody>
</table>

The following table lists the keyboard shortcuts you can use to perform some of the main tasks in the License Agreement page of the installation wizard.
Table 73. List of keyboard shortcuts on the License Agreement page

<table>
<thead>
<tr>
<th>To do this</th>
<th>Press</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the license agreement</td>
<td>Alt+A</td>
</tr>
<tr>
<td>Decline the license agreement</td>
<td>Alt+D</td>
</tr>
<tr>
<td>Quit the installation wizard</td>
<td>Alt+x</td>
</tr>
</tbody>
</table>

The following table lists the keyboard shortcuts you can use to perform some of the main tasks in IBM Cognos Configuration on a Windows operating system.

Table 74. List of keyboard shortcuts for IBM Cognos Configuration on a Windows operating system

<table>
<thead>
<tr>
<th>To do this</th>
<th>Press</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save the current configuration</td>
<td>Ctrl+S</td>
</tr>
<tr>
<td>Close IBM Cognos Configuration</td>
<td>Alt+F4</td>
</tr>
<tr>
<td>Rename the selected item</td>
<td>F2</td>
</tr>
<tr>
<td>Display the File menu</td>
<td>Alt+F</td>
</tr>
<tr>
<td>Display the Edit menu</td>
<td>Alt+E</td>
</tr>
<tr>
<td>Display the View menu</td>
<td>Alt+V</td>
</tr>
<tr>
<td>Display the Actions menu</td>
<td>Alt+A</td>
</tr>
<tr>
<td>Display the Help menu</td>
<td>Alt+H</td>
</tr>
</tbody>
</table>

The following table lists the keyboard shortcuts you can use to perform some of the main tasks in IBM Cognos Configuration on a UNIX or Linux operating system.

Table 75. List of keyboard shortcuts for IBM Cognos Configuration on a UNIX or Linux operating system

<table>
<thead>
<tr>
<th>To do this</th>
<th>Press</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save the current configuration</td>
<td>Ctrl+S</td>
</tr>
<tr>
<td>Close IBM Cognos Configuration</td>
<td>Alt+F4</td>
</tr>
<tr>
<td>Rename the selected item</td>
<td>F2</td>
</tr>
</tbody>
</table>
Appendix B. IBM Cognos Configuration command-line options

Use command-line options with the configuration command to modify the behavior of IBM Cognos Configuration when it starts.

Table 76. Command line options and descriptions

<table>
<thead>
<tr>
<th>Option</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>Displays commands for IBM Cognos Configuration.</td>
</tr>
<tr>
<td>-s</td>
<td>Runs IBM Cognos Configuration in silent mode.</td>
</tr>
<tr>
<td></td>
<td>Uses property values specified in the cogstartup.xml file to configure installed components and then starts all services.</td>
</tr>
<tr>
<td></td>
<td>./cogconfig.sh -s</td>
</tr>
<tr>
<td></td>
<td>cogconfig.bat -s</td>
</tr>
<tr>
<td>-stop</td>
<td>Stops all IBM Cognos services.</td>
</tr>
<tr>
<td></td>
<td>./cogconfig.sh -stop</td>
</tr>
<tr>
<td></td>
<td>cogconfig.bat -stop</td>
</tr>
<tr>
<td>-startupfile path/filename.xml</td>
<td>Runs IBM Cognos Configuration using a file other than the cogstartup.xml file in the $c10_location/configuration directory.</td>
</tr>
<tr>
<td>-test</td>
<td>Uses property values specified in the cogstartup.xml file to test configuration settings.</td>
</tr>
<tr>
<td></td>
<td>./cogconfig.sh -test</td>
</tr>
<tr>
<td></td>
<td>cogconfig.bat -test</td>
</tr>
<tr>
<td>-notest</td>
<td>Starts IBM Cognos Configuration with the automatic testing tasks disabled.</td>
</tr>
<tr>
<td></td>
<td>./cogconfig.sh -notest</td>
</tr>
<tr>
<td></td>
<td>cogconfig.bat -notest</td>
</tr>
<tr>
<td></td>
<td>This option should not be used for the first time you start the product or if you are making configuration changes.</td>
</tr>
<tr>
<td>-utf8</td>
<td>Saves the configuration in UTF-8 encoding.</td>
</tr>
<tr>
<td></td>
<td>./cogconfig.sh -s -utf8</td>
</tr>
<tr>
<td></td>
<td>cogconfig.bat -s -utf8</td>
</tr>
<tr>
<td>Option</td>
<td>Descriptions</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>-l language ID</code></td>
<td>Runs IBM Cognos Configuration using the language specified by the language identifier.</td>
</tr>
<tr>
<td></td>
<td>To run the configuration tool in silent mode using Simplified Chinese</td>
</tr>
<tr>
<td></td>
<td>./cogconfig.sh -l zh-cn</td>
</tr>
<tr>
<td></td>
<td>cogconfig.bat -l zh-cn</td>
</tr>
<tr>
<td><code>-e filename.xml</code></td>
<td>Exports the current configuration settings to the specified file.</td>
</tr>
<tr>
<td></td>
<td>./cogconfig.sh -e filename.xml</td>
</tr>
<tr>
<td></td>
<td>cogconfig.bat -e filename.xml</td>
</tr>
<tr>
<td><code>-log</code></td>
<td>Creates a <code>cogconfig.timestamp.log</code> error log file in the <code>cognos_location/logs</code> directory.</td>
</tr>
<tr>
<td></td>
<td>./cogconfig.sh -log</td>
</tr>
<tr>
<td></td>
<td>cogconfig.bat -log</td>
</tr>
<tr>
<td>`-java:{local</td>
<td>env}`</td>
</tr>
<tr>
<td></td>
<td>• env: environmentally using the <code>JAVA_HOME</code> environment variable</td>
</tr>
<tr>
<td></td>
<td>• local: locally from the <code>c10_location/bin/jre</code> directory</td>
</tr>
<tr>
<td></td>
<td>If you do not set this flag, IBM Cognos uses the <code>JAVA_HOME</code> environment variable setting.</td>
</tr>
<tr>
<td></td>
<td>To run IBM Cognos Configuration in silent mode, using the local JVM, type the following command:</td>
</tr>
<tr>
<td></td>
<td>./cogconfig.sh -s -java:local</td>
</tr>
<tr>
<td></td>
<td>cogconfig.bat -s -java:local</td>
</tr>
</tbody>
</table>

You can use more than one command-line option at a time. For example, you can run IBM Cognos Configuration in silent mode and send all error messages to a log file.
Appendix C. Troubleshooting

Use this troubleshooting reference information and these solutions as a resource to help you solve specific problems you may encounter during or after the installation of IBM Cognos Business Intelligence components.

Problems are characterized by their symptoms. Each symptom can be traced to one or more causes by using specific troubleshooting tools and techniques. After being identified, each problem can be fixed by implementing a series of actions.

When you are troubleshooting, log files can help you. Another valuable troubleshooting tool is the Knowledge Base, which is available on the IBM Support Portal [http://www-01.ibm.com/software/analytics/support/finding-answers/kb.html]. The Knowledge Base is a database of problems and solutions for all IBM Cognos products.

When you cannot resolve a problem, the final resource is your technical support representative. To analyze a problem, your technical support representative requires information about the situation and the symptoms that you are experiencing. To help isolate the problem, collect the necessary data before you contact your representative.

Troubleshooting a problem

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead to a resolution of the problem.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is “What is the problem?” This question might seem straightforward; however, you can break it down into several focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is the problem a loop, hang, crash, performance degradation, or incorrect result?
**Where does the problem occur?**

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and the hardware. Confirm that you are running within an environment that is supported; many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

**When does the problem occur?**

Develop a detailed timeline of events leading up to a failure, especially for cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as an upgrade or an installation of software or hardware?

**Under which conditions does the problem occur?**

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to occur for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.
Can the problem be reproduced?

Problems that you can reproduce are often easier to solve. However, problems that you can reproduce can have a disadvantage. If the problem as a significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation. Answer the following questions:

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the information center for IBM Cognos, but sometimes you need to look beyond the information center to resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

- Find the content that you need by using the IBM Support Portal. The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the.ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.

- Search for content about IBM Cognos by using one of the following additional technical resources:
  - IBM Cognos BI APARs (problem reports)
  - Searching technote.
  - IBM Cognos forums and communities

- Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field on any ibm.com page.

- Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.
Tip: Include “IBM” and the name of the product in your search if you are looking for information about an IBM product.

Getting fixes
A product fix might be available to resolve your problem.

Procedure

To find and install fixes:
1. Determine which fix you need [Fix Central](http://www.ibm.com/support/fixcentral/)
2. Download the fix. Open the download document and follow the link in the “Download package” section.
3. Apply the fix by following the instructions in the “Installation Instructions” section of the download document.
4. Subscribe to receive weekly email notifications about fixes and other IBM Support information.

Contacting IBM Support
IBM Support provides access to a variety of IBM resources for help with software questions.

Before you begin
After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company must have an active IBM maintenance contract, and you must be authorized to submit problems to IBM. You should also have the following information at hand:

- Your customer identification number
- Your service request number, if it is an ongoing service request
- The phone number where you can be reached
- The version of the software you use
- The version of the operating environment you use
- A description of what you were doing when the problem occurred
- The exact wording of any error messages that display
- Any steps you took to attempt to solve the problem

For information about the types of available support, see the Support portfolio topic in the Software Support Handbook (opens in new window).

Procedure

Complete the following steps to contact IBM Support with a problem:
1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support (opens in new window) topic in the Software Support Handbook.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
• Using IBM Support Assistant (ISA): Use this feature to open, update, and view an Electronic Service Request with IBM. Any data that has been collected can be attached to the service request. This expedites the analysis and reduces the time to resolution.

• Online through the [IBM Support Portal](opens in new window): You can open, update, and view all your Service Requests from the Service Request portlet on the Service Request page.

• By phone: For the phone number to call, see the [Directory of worldwide contacts](opens in new window) web page.

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support Web site daily, so that other users who experience the same problem can benefit from the same resolution.

Exchanging information with IBM

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system.

In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Sending information to IBM Support

To reduce the time that it takes to resolve your problem, you can send trace and diagnostic information to IBM Support.

Procedure

To submit diagnostic information to IBM Support:

1. Open a problem management record (PMR). You can use the [IBM Support Assistant](opens in new window) or the [IBM Service Request tool](opens in new window).

2. Collect the diagnostic data that you need. Diagnostic data helps reduce the time that it takes to resolve your PMR. You can collect the diagnostic data manually or automatically.

3. Compress the files by using the TRSMAIN or AMATERSE program. Download the free utility from the IBM to the IBM Cognos BI system and then install the utility using the TSO RECEIVE command.

4. Transfer the files to IBM. You can use one of the following methods to transfer the files to IBM:
   • [The Service Request tool](opens in new window)
   • Standard data upload methods: FTP, HTTP
   • Secure data upload methods: FTPS, SFTP, HTTPS
   • Email

If you are using an IBM Cognos product and you use ServiceLink / IBMLink to submit PMRs, you can send diagnostic data to IBM Support in an email or by using FTP.
All of these data exchange methods are explained on the IBM Support site (opens in new window).

**Receiving information from IBM Support**

Occasionally an IBM technical-support representative might ask you to download diagnostic tools or other files. You can use FTP to download these files.

**Before you begin**

Ensure that your IBM technical-support representative provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

**Procedure**

To download files from IBM Support:

1. Use FTP to connect to the site that your IBM technical-support representative provided and log in as anonymous. Use your email address as the password.

2. Change to the appropriate directory:
   a. Change to the /fromibm directory.
      
   b. Change to the directory that your IBM technical-support representative provided.
      
3. Enable binary mode for your session.

4. Use the `get` command to download the file that your IBM technical-support representative specified.

5. End your FTP session.

**Subscribing to Support updates**

To stay informed of important information about the IBM products that you use, you can subscribe to updates.

**About this task**

By subscribing to receive updates, you can receive important technical information and updates for specific Support tools and resources. You can subscribe to updates by using one of two approaches:

**RSS feeds and social media subscriptions**

The following RSS feeds and social media subscriptions are available for IBM Cognos BI:

- RSS feed for a developerWorks® forum (opens in new window).
- RSS feed for the Support site for IBM Cognos Business Intelligence (opens in new window)

For general information about RSS, including steps for getting started and a list of RSS-enabled IBM web pages, visit the IBM Software Support RSS feeds (opens in new window).
My Notifications

With My Notifications, you can subscribe to Support updates for any IBM product. You can specify that you want to receive daily or weekly email announcements. You can specify what type of information you want to receive, such as publications, hints and tips, product flashes (also known as alerts), downloads, and drivers. My Notifications enables you to customize and categorize the products that you want to be informed about and the delivery methods that best suit your needs.

Procedure

To subscribe to Support updates:

1. Subscribe to the Product RSS feeds.
2. To subscribe to My Notifications, begin by going to the IBM Support Portal (opens in new window) and clicking My Notifications in the Notifications portlet.
3. If you have already registered for My support, sign in and skip to the next step. If you have not registered, click Register now. Complete the registration form using your email address as your IBM ID and click Submit.
4. Click Edit profile.
5. Click Add products and choose a product category; for example, Software.
6. In the second list, select a product segment; for example, Data & Information Management.
7. In the third list, select a product subsegment, for example, Databases.
8. Select the products that you want to receive updates for.
9. Click Add products.
10. After selecting all products that are of interest to you, click Subscribe to email on the Edit profile tab.
11. Select Please send these documents by weekly email.
12. Update your email address as needed.
13. In the Documents list, select the product category; for example, Software.
14. Select the types of documents that you want to receive information for.
15. Click Update.

Results

Until you modify your RSS feeds and My Notifications preferences, you receive notifications of updates that you have requested. You can modify your preferences when needed (for example, if you stop using one product and begin using another product).

Log Files

Log files can help you troubleshoot problems by recording the activities that take place when you work with a product.

Operations performed in IBM Cognos BI are recorded in various log files for tracking purposes. For example, if you experienced problems installing IBM Cognos BI, consult the transfer log file to learn what activities the installation wizard performed while transferring files.
Before you begin viewing log files, ensure that they contain the information that you need. The number of log files and the information they contain are set by parameters in IBM Cognos Connection and in IBM Cognos Configuration.

Use IBM Cognos Administration to set the level of detail to log for each category.

For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.

Use IBM Cognos Configuration to specify the size, number, and location of log files, and to configure the properties of the log server.

When troubleshooting, the following files can assist you:

**The Transfer Log File**

This file records the activities that the installation wizard performed while transferring files.

The transfer log file is located in the `c10_location\instlog` directory. The file name identifies the product name, version, and build number, and includes a time stamp. The following is an example of the file name format:

`t1-BISRVR-8.1-0.0-20080901_1122.txt`

**The Transfer Summary-Error Log File**

This file records the components you installed, disk space information, the selections you made in the transfer dialogs, and any errors the installation wizard encountered while transferring components.

The transfer summary-error log file is located in the `c10_location\instlog` directory. The file name identifies the product name, version, and build number, and includes a time stamp. The following is an example of the file name format:

`t1-BISRVR-8.1-0.0-20080901_1122_summary_error.txt`

**The Startup Configuration File**

This file records your configuration choices each time you save your property settings. The file name is `cogstartup.xml`.

If you are unable to save your configuration, or are having problems you can revert to a previously saved configuration file. The backup configuration files are located in the `c10_location/configuration` directory. The following is an example of the file name format for backup configuration files:

`cogstartup_200811231540.xml`

**The Startup Configuration Lock File**

This file is created each time you open IBM Cognos Configuration. It prevents you from opening more than one IBM Cognos Configuration window.

If you experience problems opening IBM Cognos Configuration, you can check the `c10_location/configuration` directory for the `cogstartup.lock` file. If the file exists
and IBM Cognos Configuration is not open, it means that IBM Cognos Configuration did not shut down properly the last time you used it. You can delete the lock file and then open IBM Cognos Configuration.

**The Locale Configuration File**

This file records the configuration choices you make in IBM Cognos Configuration for product and content locales, locale mapping, and currency support.

If you experience problems with language support in the user interface or in reports, use these files to track your changes. The backup configuration files are located in the `c10_location/configuration` directory. The following is an example of the file name format:

`coglocale_200811231540.xml`

**The Runtime Log File**

The default IBM Cognos log file, named `cogserver.log`, or other log files that you configure to receive log messages from the log server, record information after you start the IBM Cognos BI service. They are located in the `c10_location/logs` directory. If you configured another destination for log messages, check the appropriate file or database.

Some log messages indicate problems. Most messages provide information only, but others can help you to diagnose problems in your runtime environment.

**The Gateway Log File**

The gateways record errors in the gateway log file, which is located in the `c10_location/logs` directory.

You can use the gateway log file to troubleshoot problems that prevent the gateway from processing requests or from using encryption. Symptoms of these problems are as follows:

- User IDs and passwords do not work
- Single signon does not work
- The dispatcher is running but users receives an error message advising that the IBM Cognos BI server is not available

The gateway log file uses the following naming format, where `gateway_interface` is `cgi`, `mod2` (Apache 2.0 module), or `isapi`.

`ggateway_interface.log` (for example, `gw cgi.log`)

**The Uninstallation Log File**

This file records the activities that the Uninstall wizard performed while uninstalling files. The log file is named `cognos_uninst_log.htm` and is located in the Temp directory. You can use the log file to troubleshoot problems related to uninstalling IBM Cognos BI components.
The Silent Mode Log File

This file records the activities that IBM Cognos Configuration performed while running in silent mode. This log file is named cogconfig_response.csv and is located in the c10_location/logs directory.

Cannot run issetup on Linux operating systems

You run issetup to install IBM Cognos BI but you receive the following error message:
Error while loading shared libraries: libXm.so.4: cannot open shared object file:
No such file or directory.

Procedure
1. Go to the /usr/lib directory.
2. Create a symbolic link to another version of libXm.so and name the symbolic link libXm.so.4.
   For example, create a symbolic link to libXm.so.3 as shown in the following command:
   ```bash
   ln -s libXm.so.3 libXm.so.4
   ```
3. Run issetup again.

Problems starting IBM Cognos Business Intelligence

You can perform the following tasks when encountering problems starting IBM Cognos Business Intelligence.

You may encounter problems when you try
• to start the IBM Cognos BI service
• to open the Welcome page for the IBM Cognos BI portal for the first time
• to start an application server, such as WebLogic or WebSphere

The following table shows some common symptoms and their solutions.

<table>
<thead>
<tr>
<th>Symptoms</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>You do not see the splash screen for the IBM Cognos BI portal when you start IBM Cognos BI.</td>
<td>Check your Web server configuration.</td>
</tr>
<tr>
<td>The service starts, but no tables are created in the content store database.</td>
<td>Check your content store configuration.</td>
</tr>
<tr>
<td>The service does not start.</td>
<td>Ensure that you wait a few moments before submitting a request.</td>
</tr>
<tr>
<td>The application server does not start.</td>
<td>Check the file permissions and directory names of the application server installation location.</td>
</tr>
</tbody>
</table>

To review an up-to-date list of environments that are supported by IBM Cognos Business Intelligence products, including information on operating systems, patches, browsers, web servers, directory servers, database servers, and application servers, see the IBM Software Product Compatibility Reports (SPCR) page (www.ibm.com/support/docview.wss?uid=swg27037784).
**CFG-ERR-0106 error when starting the IBM Cognos service in IBM Cognos Configuration**

When you start the IBM Cognos Business Intelligence service, you receive CFG-ERR-0106 error message.

The error message appear as:

- CFG-ERR-0106. IBM Cognos Configuration received no response from the IBM Cognos service in the allotted time. Check that the IBM Cognos service is available and properly configured.
- Unable to start IBM Cognos service. Execution of the external process returns an error code value of '-1'.

There are three possible causes for this problem:

- IBM Cognos service needs more time to start.
- A standby Content Manager computer is configured incorrectly.
- A 32-bit version of IBM Cognos BI was installed against a 64-bit version of Java.

**Changing the wait time for the IBM Cognos service**

If you received the CFG-ERR-0106 error because the IBM Cognos service needs more time to start, change the amount of time that IBM Cognos Configuration waits to receive a response from the IBM Cognos service.

By default, IBM Cognos Configuration checks the progress of the start request every half second for three minutes. If IBM Cognos Configuration does not receive a response within this time, the error message is displayed.

The amount of time that IBM Cognos Configuration waits to receive a response from the IBM Cognos service is controlled by the ServiceWaitInterval and ServiceMaxTries properties.

The ServiceWaitInterval property represents the time interval, in milliseconds, at which IBM Cognos Configuration checks the progress of the start request. By default, its value is 500, which is equivalent to half a second.

The ServiceMaxTries property represents the number of times that IBM Cognos Configuration checks the progress of the start request. By default, its value is 360.

**Procedure**

1. Using IBM Cognos Configuration, stop the IBM Cognos service.
2. Open the cl0_location/configuration/cogconfig.prefs file in an editor.
   
   This file is created automatically the first time you open IBM Cognos Configuration.
3. Add the following code to the file:
   
   ```
   ServiceWaitInterval=number of milliseconds
   ServiceMaxTries=number of times
   ```

   **Tip:** Add the numeric values that correspond to your configuration needs.
4. Save the file.
5. Using IBM Cognos Configuration, start the IBM Cognos service.
Changing the location where symmetric keys are stored

If you received the CFG-ERR-0106 error on a standby Content Manager computer, configure the computer to store the symmetric keys locally.

The setting for storing the symmetric keys may be incorrect.

Procedure
1. On the standby Content Manager computer, start IBM Cognos Configuration.
2. In the Explorer window, under Security, click Cryptography.
3. In the Properties window, under CSK settings, set Store symmetric key locally to True.
4. From the File menu, click Save.
5. From the Actions menu, click Start.

Using an appropriate version of Java

If you received the CFG-ERR-0106 error because a 32-bit version of IBM Cognos Business Intelligence service was installed against a 64-bit version of Java, you must either rename JAVA_HOME or set it to point to a supported 32-bit version of Java.

A 32-bit version of IBM Cognos BI service must be installed against a compatible 32-bit version of Java. You cannot configure a 32-bit version of IBM Cognos BI service to run against a 64-bit version of Java.

Before you begin

To review an up-to-date list of environments that are supported by IBM Cognos Business Intelligence products, including information on operating systems, patches, browsers, web servers, directory servers, database servers, and application servers, see the IBM Software Product Compatibility Reports (SPCR) page (www.ibm.com/support/docview.wss?uid=swg27037784).

Procedure
1. Even though it did not start properly, stop the IBM Cognos service, and exit the IBM Cognos Configuration tool.
2. Delete the contents of the C10_location\temp directory.
3. Take one of the following steps:
   a. Rename JAVA_HOME
   b. Set JAVA_HOME to point to a supported 32-bit version of Java.
4. If necessary, restart your computer.
5. In IBM Cognos Configuration, start the IBM Cognos service.

Cryptographic error when starting IBM Cognos Business Intelligence

If the following error occurs when you try to start the IBM Cognos Business Intelligence service after installing server or client components, then your Java Runtime Environment (JRE) is missing the encryption and decryption routines.
If you receive this error, then you must copy the Java Archive (.jar) file that is provided to your JRE director since it is required by IBM Cognos BI.

[Cryptography]
1. [ERROR] java.lang.NoClassDefFoundError:
   javax/net/ServerSocketFactory:

Your Java Runtime Environment (JRE) is missing the encryption and decryption routines that are required by IBM Cognos BI. You must copy the Java Archive (.jar) file that is provided to your JRE directory.

Procedure

Copy bcprov-jdkversion.jar from the c10_location/bin/jre/version/lib/ext directory to the JRE_location/lib/ext directory.
If you are using 64-bit components, copy the files from c10_location/bin64.

Unable to start the IBM Cognos service because the port is used by another process

You may not be able to start the IBM Cognos Business Intelligence service or process if one of the default ports is used by another process.

Tip: To view the current network TCP/IP network connections, use the netstat command.

Use IBM Cognos Configuration to change the default port that IBM Cognos BI uses.

When you change the port used by the local dispatcher, you must change the value of the Dispatcher URI properties. Because the change affects all the URIs that are based on the local dispatcher, you must change the URLs of all local components. By default, local components contain localhost in the URI.

For example, if you install all components on one computer and you want to change the dispatcher port, replace 9300 in all dispatcher and Content Manager URLs with the new port number.

Procedure
1. Start IBM Cognos Configuration.
2. In the Explorer window, click the appropriate group or component:
   • To access the port number in the dispatcher and Content Manager URLs, click Environment.
   • To access the port number for the local log server, under Environment, click Logging.
   • To access the shutdown port number, under Environment, click IBM Cognos services > IBM Cognos BI.
   • To access the port number for the location of the applications.xml file used by Portal Services, under Environment, click Portal Services.
3. In the Properties window, click the Value box next to the property that you want to change.
4. Change the value from 9300 to the new value.
   Ensure that you change the ports in all URLs that contain localhost:9300.
5. From the File menu, click Save.
6. From the Action menu, click Start.
IBM Cognos service does not start or fails after starting

You start the IBM Cognos Business Intelligence service but services either do not start correctly or are very slow to start. After services start, the system fails a short time afterwards. While services are starting, Java uses 100 percent of the CPU time.

You may also receive multiple occurrences of error messages such as the following:

- DPR-DPR-1035 Dispatcher detected an error.
- CAM-CRP-1157 Unable to synchronize the local common symmetric key store with Content Manager.

Procedure

If you use a DB2 database for the content store, ensure that the database version and Java version are compatible.

For DB2 version 8.2, Java 1.5 is not supported. For DB2 version 9, Java 1.5 is supported on all operating systems except HP-UX and Solaris.

IBM Cognos Business Intelligence server fails to start and gives no error message

An IBM Cognos BI server may fail to start after an upgrade or new installation, but no error message displays. This may occur when a previously running or new IBM Cognos BI server is configured to use a large amount of memory.

If the server on which IBM Cognos BI is installed contains version 1.0 of Microsoft security update 921883, there may be an issue when a lot of contiguous memory is requested by an application.

This is a known issue with version 1.0 of Microsoft security patch 921883. Microsoft distributed a second version of the patch to fix the problem. As a workaround, uninstall the first security patch, or install version 2.0 of the patch. Alternatively, you can configure the IBM Cognos BI server to use less memory.

For more information, see the Microsoft knowledge base article about programs using a lot of contiguous memory failing, at the Microsoft support Web site.

Server not available when starting IBM Cognos Business Intelligence

After you configure IBM Cognos components and start the IBM Cognos services, when you connect to the IBM Cognos Business Intelligence portal, the following error message may display:

_The Cognos Gateway is unable to connect to the Cognos BI server._

_The server may be unavailable, or the gateway may not be correctly configured._

Check the IBM Cognos server log file for more information. By default, the cogserver.log file is located in the c10_location/logs directory. If you configured another destination for log messages, check the appropriate file or database.

Content Manager may not be able to connect to the content store if the content store is not configured properly. This may occur if

- the content store uses an unsupported character encoding
- the content store uses a database collation sequence that is case sensitive
the configuration settings you specified in IBM Cognos Configuration are not valid

**Unsupported character encoding**

If the following messages display in the log file, the database you created for the content store does not use a supported character encoding:

- For Oracle:
  
  CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.
  
  CM-SYS-5121 Content Manager cannot start because the database character set for the content store is not supported.
  
  CM-SYS-5126 The content store database server uses the character set US7ASCII.
  
  CM-SYS-5125 The content store database client uses the character set US7ASCII.

- For DB2 UDB:
  
  CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.
  
  CM-SYS-5121 Content Manager cannot start because the database character set for the content store is not supported.
  
  CM-SYS-5124 The content store database server uses the code page 1252.

- For Sybase:
  
  CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.
  
  CM-SYS-5121 Content Manager cannot start because the database character set for the content store is not supported.

For Content Manager to connect to the content store, the content store must use the appropriate character encoding, as listed in the following table.

**Table 78. Character encoding used by the content store to connect to a specific database type**

<table>
<thead>
<tr>
<th>Database</th>
<th>Character encoding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle 9i</td>
<td>AL32UTF8</td>
</tr>
<tr>
<td></td>
<td>AL32UTF16</td>
</tr>
<tr>
<td>DB2 UDB</td>
<td>Codeset UTF-8</td>
</tr>
<tr>
<td>Sybase ASE</td>
<td>UTF-8</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>UTF8</td>
</tr>
<tr>
<td></td>
<td>UTF16</td>
</tr>
</tbody>
</table>

To resolve this problem, you must recreate the content store database using the correct character encoding, or convert the character encoding. For more information, see the database documentation.
Case-sensitive collation sequence

If the following messages are in the log file, the database you created for the content store uses a database collation sequence that is case sensitive:

CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

CM-SYS-5122 The content store database has a default collation that is case-sensitive. Content Manager requires a content store that has a case-insensitive collation.

CM-SYS-5123 The content store database server uses the collation <parameter>.

CM-SYS-5007 Content Manager build @cm_build_version@ failed to start! Review the Content Manager log files and then contact your system administrator or customer support.

To resolve this problem, you must recreate the content store database using a database collation sequence that is not case sensitive. For more information, see the database documentation.

Invalid configuration settings

If the following or similar messages are in the log file, you did not configure the content store correctly in IBM Cognos Configuration.

- For Microsoft SQL Server:
CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.
CM-CFG-5036 Content Manager failed to connect to the content store. The connection string is "jdbc:JSQLConnect://localhost:1433/cm".

- For DB2:
CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.
CM-SYS-5003 Content Manager is unable to access the content store. Verify your database connection parameters and then contact your database administrator.
[IBM][CLI Driver] SQL1013N The database alias name or database name "CM123" could not be found.

- For Oracle:
CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.
CM-CFG-5036 Content Manager failed to connect to the content store. The connection string is "jdbc:oracle:thin:@localhost:1521:pb1".
ORA-01017: invalid username/password; logon denied.

- For Sybase:
CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.
CM-CFG-5036 Content Manager failed to connect to the content store. The connection string is "jdbc:sybase:Tds:localhost:5000/cm".
JZ006: Caught IOException: java.net.ConnectException: Connection refused: connect.
If you are using an Oracle database, do not use illegal characters, such as an underscore in IBM Cognos Configuration for the Service Name property. If the Service Name includes illegal characters, tables are not created in the content store database when the IBM Cognos service is started.

**Configuring a content store in IBM Cognos Configuration**

If you received a CM-CFG-5036 or CM-CFG-5063 error code, the content store might not be configured correctly.

To resolve the issue, reconfigure the content store (see "Setting database connection properties for a Microsoft SQL Server, Oracle, Informix, or Sybase content store" on page 68).

**Related concepts:**

"Set up database connectivity for the content store database” on page 60

If you are using a database other than Cognos Content Database or Microsoft SQL Server as the content store, you may have to install database client software, or Java Database Connectivity (JDBC) drivers, or both, on each computer where you install Content Manager. Doing this allows Content Manager to access the content store database.

**Cannot log on to a namespace when using IBM Cognos Connection**

You open IBM Cognos Business Intelligence through IBM Cognos Connection. However, when you attempt to create a data source and log on to a namespace, the following error messages display:

- **PRS-CSE-1255** Exception error encountered in data decryption.
- **CAM-CRP-1064** Unable to process the PKCS #7 data because of an internal error.
  

This issue might occur if you do not have the necessary permissions for the following directories:

- c10_location/configuration
- c10_location/configuration/csk
- c10_location/configuration/encryptkeypair
- c10_location/configuration/signkeypair

Enable the read and execute permissions on these listed directories for anyone who must start the IBM Cognos service.

**IBM Cognos services fail to restart after a network outage**

The IBM Cognos Bootstrap Service restarts IBM Cognos services after a network outage.

For Tomcat installations where a network IP address is specified in the internal dispatcher URI, the IBM Cognos services may not initialize successfully during the restart. This requires a manual restart after the network is restored.

**Procedure**

To resolve the problem, configure the **Internal dispatcher URI** property in IBM Cognos Configuration to use localhost or the network host name.
No warning that installing later version will automatically update earlier version of content store

You have a version of IBM Cognos BI installed on your computer. You install a later version into a new location. You use the same database for the content store for both versions. After you configure the later version and start the IBM Cognos service, the earlier version of IBM Cognos BI no longer works because all content is automatically upgraded.

If you want to use different versions of IBM Cognos BI after you upgrade, ensure that before you install the later version, you:
• back up the database you use for the content store
• restore the backup to a new location

Alternatively, you can choose to use the deployment tool to import the entire content store from an earlier version to the later version. All existing content in the content store database is replaced by the imported content. You receive a warning message about this.

Download of resource fails

If the download resource fails, it may be caused by recent Microsoft XMLHTTP upgrades if you do not have a language preference set in Internet Explorer.

You start Report Studio in Internet Explorer and the following error message displays:

_The download of the specified resource has failed._

Procedure

To resolve the problem, specify a language preference in Internet Explorer.

DB2 returns SQL1224N error when connecting from AIX

If your content store is a DB2 database and you receive an SQL1224N error on AIX, check the db2diag.log file for additional information about the error.

If the error includes reason code 18, you might need to change the DB2 configuration to accept more connections. For more information, see the IBM DB2 support pages for the error SQL1224N.

Content Manager error when starting IBM Cognos Business Intelligence

After starting IBM Cognos BI, no BIBUSTKSERVMA process is started. There are errors listed in the pogo******.log and cogserver.log files. Users receive errors in the browser when connecting to the IBM Cognos BI portal.

In the pogo******.log file, an error related to Content Manager displays.

In the cogserver.log file, the following error displays:

_An attempt to register the dispatcher in Content Manager was unsuccessful. Will retry periodically._
When connecting to http://computer name/ibmcognos, the following error messages display in the browser:

- DPR-ERR-2058 The dispatcher cannot service the request at this time. The dispatcher is still initializing
- SoapSocketException: Connection Refused

IBM Cognos Configuration uses a user ID to bind to the LDAP database. If this user ID is moved to another group, IBM Cognos Configuration can no longer locate it.

Procedure

To correct the problem, move the user ID back to the original group.

**Content Manager fails to start or takes a long time to start**

On Microsoft Windows, you try to start the service on the computer where you installed Content Manager. As the service is starting, the details include errors similar to the following:

DPR-CMI-4006 Unable to determine the active Content Manager. Will retry periodically.

CM-SYS-5007 Content Manager build x.x.x.x failed to start!

Details within the error log may also include references to OutOfMemoryError.

To resolve this problem, start the service using the DuseCMLargeResultSet parameter. You can add the parameter to the bootstrap configuration file and then start the service using IBM Cognos Configuration or you can add the parameter to the startup configuration file and then run the file.

**Resolving an out-of-memory error using the bootstrap configuration file**

Start the IBM Cognos service by adding the DuseCMLargeResultSet parameter to the bootstrap configuration file.

Procedure

1. Go to the c10_location\bin directory and open bootstrap_win32.xml in an XML editor.
2. Find the section that begins with <param>"${install_path}.
3. Add the DuseCMLargeResultSet parameter to that section, in the location shown by the bold text in the following example.
   
   `<param>-Dcatalina.base=${install_path}/tomcat</param>
   `<param>-Dcatalina.home=${install_path}/tomcat</param>
   `<param>-Djava.io.tmpdir=${temp}</param>
   `<param>-DuseCMLargeResultSet=true</param>`
4. Save and close the file.
5. Start IBM Cognos Configuration and start the service.

**Resolving an out-of-memory error using the startup configuration file**

Start the IBM Cognos service by adding the DuseCMLargeResultSet parameter to the startup configuration file.
Procedure
1. Go to the c10_location\bin directory and open startup.bat in a text editor.
2. Find the following line:
   set CATALINA_OPTS=-Xmx768m -XX:MaxNewSize=384m -XX:NewSize=192m
   -XX:MaxPermSize=128m
   %DEBUG_OPTS%
3. Append the DuseCMLargeResultSet parameter to the line, as shown by the bold text in the following example:
   set CATALINA_OPTS=-Xmx768m -XX:MaxNewSize=384m -XX:NewSize=192m
   %DEBUG_OPTS%-DuseCMLargeResultSet=true
4. Save and close the file.
5. Start the service by running the startup.bat file.

DPR-ERR-2014 error displays in log file on Content Manager computer
If Content Manager is installed on a separate computer and the event management service on the Content Manager computer is disabled.

The following error message may be in the cogserver.log file:

DPR-ERR-2014 Unable to load balance the request because no nodes in the cluster are available, or no nodes are configured for the service: eventManagementService

To correct the problem, turn off the event management service.

Procedure
1. Start IBM Cognos Configuration on the Content Manager computer.
2. In the Explorer pane, go to Environment > IBM Cognos services.
3. Set the Event management service enabled property to False.

Non-ASCII characters in installation directory cause run-time errors
On all operating systems, if you use non-ASCII characters in the installation directory for IBM Cognos Business Intelligence, it causes run-time errors. It also causes some product functions, such as report execution, to fail.

Install IBM Cognos BI in the default directory or use a directory name that contains only ASCII Latin-1 characters.

Cannot Open a Microsoft Cube or PowerCube
You are unable to open a Microsoft Cube or PowerCube, or you can open an Microsoft Cube but only metadata is shown. For an Microsoft Cube, you may receive the following error message:

MO-ERR-0030

Cannot connect to the datasource. Please set the service to run as a domain user with the correct privileges.

To solve this problem, ensure that the user running the IBM Cognos Business Intelligence service has access rights to the cube.
PowerCubes are accessed through mapped drives or UNC path names.

**Assigning access rights to Microsoft cubes**
For a user account to open Microsoft cubes, it must be assigned the appropriate privileges in the system administrative tools.

**Procedure**
1. Add the domain user account that starts the IBM Cognos service to the Act as part of the operating system privilege:
   - Under Administrative Tools, select Local Security Policy.
   - Expand Security Settings, Local Policies and click User Rights Assignment.
   - Right-click the Act as part of the operating system policy and select Properties.
   - Click Add User or Group and add the user account that starts the IBM Cognos service.
2. If you use the domain userID and password method of authentication, add the user account that starts the IBM Cognos service to the domain that includes Content Manager, the Application Tier Components, IIS Web server, and the data source server (Microsoft SQL Server or Microsoft Analysis Server).
3. If you use an external namespace, such as Active Directory Server, for authentication, add the user account that starts the IBM Cognos service to the domain that includes the authentication provider.
   This domain must also include Content Manager, the Application Tier Components, IIS Web server, and the data source server (Microsoft SQL Server or Microsoft Analysis Server).
   For more information about configuring external namespaces for authentication, see the topics about authentication providers in the IBM Cognos Business Intelligence Installation and Configuration Guide.

**Assigning access rights to PowerCubes**
For a user account to open PowerCubes, it must be assigned the appropriate privileges in IBM Cognos Administration.

**Procedure**
Ensure that the IBM Cognos user profile has sufficient operating system or domain access rights to open the PowerCube file.
For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.

**The page cannot be found when starting IBM Cognos Business Intelligence in Windows 2003**

Installing IBM Cognos Business Intelligence on Microsoft Windows operating system 2003 may cause an error message when you try to start IBM Cognos BI.

The following error is caused by a security feature in Windows 2003 Internet Information Services (IIS). This security feature does not allow unknown cgi file extensions.

*The page cannot be found. The page you are looking for might have been removed, had its name changed, or is temporarily unavailable. HTTP Error 404 - File or Directory not found.*
Procedure

To resolve this problem, add a new file extension in IIS for the cognos.cgi file. For more information, see the IIS documentation.

The page is not shown when opening a portal after installing IBM Cognos Business Intelligence

After you install and configure IBM Cognos Business Intelligence, you are unable to connect to the Cognos BI portal.

This may be because the Web server is not properly configured. For example, the virtual directories required for IBM Cognos BI may not exist or they may point to the wrong physical folders.

For information about configuring the Web server, see the IBM Cognos Business Intelligence Installation and Configuration Guide.

DPR-ERR-2058 Error Displays in Web Browser When Starting IBM Cognos Business Intelligence

After you start the services in IBM Cognos Configuration and then try to open the portal, a message similar to one of the following may display:

DPR-ERR-2058 The dispatcher encountered an error while servicing a request.
XTS handler must be initialized before being invoked.
DPR-ERR-2058 The dispatcher cannot service the request at this time.
The dispatcher is still initializing. Please try again or contact your administrator.

These error messages usually occur when the dispatcher cannot communicate with the Content Manager. To help you determine the specific cause, look in the cogserver.log file in the <c10_location>/logs directory. The following are the most common causes with their solutions.

IBM Cognos Services are Not Done Initializing

After you start the services in IBM Cognos Configuration and the configuration tool shows that the services are running, wait a few minutes for all services to start before you open the portal.

Content Manager is Not Available

In a distributed installation, ensure that Content Manager is installed, configured, and running. Ensure also that the other IBM Cognos computers are configured with the correct Content Manager URI.

The Content Store is Not Available or is Not Configured Properly

Ensure that the content store database was created and that you configured it correctly in IBM Cognos Configuration.

Tables are Not Created in the Content Store

Ensure that you are using a version of DB2, Microsoft SQL Server, Oracle, or Sybase that is supported by IBM Cognos components.

The Logon Credentials for the Content Store Are Incorrect

Check whether the information changed. For example, DB2 reads information from the NT user management. If the password for the NT account changed, you must also change the logon credentials for the content store in IBM Cognos Configuration.
Check for special characters in the logon password. Occasionally, the JDBC driver does not accept characters that are reserved for xml, such as %, !, <, and >.

The User Does not Have Appropriate Permissions
Ensure that the user has the appropriate permissions.

Out of Memory on HP-UX
If you are using Tomcat, you can determine the issue is related to HP-UX server configuration. You may be exceeding the expected maximum number of simultaneously active threads per process.

Increasing the maximum number of threads per process on HP-UX:

If you are exceeding the expected maximum number of simultaneously active threads per process on HP-UX, increase the number of active threads.

**Procedure**

1. Have your system administrator change the Kernel parameter as follows:
   - max_thread_proc = 512
   - nkthread = 1024
2. Ensure that the ulimit settings are unlimited.

Checking for an HP-UX configuration problem:

If increasing the maximum number of active threads per process does not resolve the out-of-memory error on HP-UX, perform the following steps.

**Procedure**

1. In the /bin/startup.sh file, find
   
   ../tomcat/bin/catalina.sh start "$@

   Change it to the following:

   ../tomcat/bin/catalina.sh run "$@

   The run command causes the Tomcat output to display in the console window for IBM Cognos BI.
2. Stop and restart IBM Cognos BI using the ./shutdown.sh and ./startup.sh commands.
3. If the following error message displays in the console window for any of the application servers, the issue is an HP-UX configuration problem:

   OutofMemoryException error: Unable to create new native thread on HP-UX.

   The problem is that the default values for HP-UX 11.0 and 11i are set too low for most Java applications.

   **Tip:** You can check the number of threads in your process by using the -eprof option available in JDK 1.1.8 and by analyzing the Java.eprof file using HPjmeter by selecting the threads metric.

Content Manager Cannot Connect to the Content Store on Oracle
If you are using an Oracle database as a content store, the DPR-ERR-2058 error may be generated when logging onto the portal All tables are created on the database.

You may also receive the following error messages:

- CM-CFG-5036 Content Manager failed to connect to the content store.
ORA-01017: invalid username/password; logon denied

Setting the Oracle database server name:

The Content Manager might fail to connect to an Oracle database because of inconsistencies between the Oracle server name in IBM Cognos Configuration and the server name in the tnsnames.ora file.

Procedure
1. Start IBM Cognos Configuration.
2. In the Explorer window, click Data Access, Content Manager, Content Store.
3. Change the Oracle database server name to a fully qualified name such as host_name.companyname:1534 to match the name in the tnsnames.ora file.

DPR-ERR-2022 error displays in Web browser when starting IBM Cognos Business Intelligence

After you start the services in IBM Cognos Configuration and then try to open the portal, a message similar to the following may display:

DPR-ERR-2022 No response generated. This may be due to an incorrect configuration, a damaged installation, or the dispatcher not having finished initializing.

This problem can occur if
- You try to open the portal before IBM Cognos services are initialized.
- A system.xml file has been edited.

In this case, replace the edited system.xml file in the appropriate subdirectory in c10_location\templates\ps with a copy from backup or use an XML editor to edit it.

There are many instances of system.xml in the directories in c10_location\templates\ps. Ensure that you replace the correct file.

Corrupt characters while installing in some languages on Linux

When running the installation wizard on Linux in Korean, Chinese (simplified or traditional), or Japanese, you may see corrupted characters in the dialog boxes of the user interface or in messages that display during the installation.

To avoid the problem of corrupt characters in the user interface during installation, you can use one of the following solutions:
- Configure the Asian fonts on the Linux server:
  - Set the locale to utf8.
    - For example, ko_KR.utf8, ja_JP.utf8, zh_CN.utf8, or zh_TW.utf8
  - Ensure that Asian language Fontset *medium-r*--14* is available on X server.
- Run an unattended installation using the default response.ats file that is provided with your IBM Cognos BI product. For information about setting up an unattended installation, see the IBM Cognos Business Intelligence Installation and Configuration Guide.
Unable to download the cognos.xts file

After installing IBM Cognos BI, you are prompted to download the cognos.xts file when connecting to the IBM Cognos Business Intelligence portal. The following error message may display:

You have chosen to download a file from this location. cognos.xts from servername

This problem occurs when the permissions on the virtual directories are not set properly. You must provide the cgi-bin virtual directory in the Microsoft Internet Information Service (IIS) with execute permissions.

To resolve this problem, recreate the virtual directories in IIS with the permissions from the following table, where c10_location represents the installation location.

Table 79. Alias, path, and permissions for creating IIS virtual directories

<table>
<thead>
<tr>
<th>Alias</th>
<th>Path</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibmcognos</td>
<td>c10_location\webcontent</td>
<td>Read</td>
</tr>
<tr>
<td>ibmcognos\ cgi-bin</td>
<td>c10_location\cgi-bin</td>
<td>Read Execute</td>
</tr>
</tbody>
</table>

For example, the default installation location is C:\Program Files\IBM\Cognos\c10.

Application server startup script fails

You may have problems running the startup scripts for an application server to deploy the IBM Cognos application if IBM Cognos Business Intelligence components are installed in a directory with a name that includes spaces.

Procedure

1. Reinstall to a new directory and do not include spaces in the new name.
2. If this solution is not easily handled by the startup scripts, try adding quotation marks around the directory name that includes spaces or use the 8.3 DOS naming convention.

IBM Cognos Business Intelligence running under WebLogic Application Server on AIX fails

The IBM Cognos Business Intelligence server instance may go into a FAILED_NOT_RESTARTABLE state in the WebLogic Administration Console on AIX.

Numerous core files and Java core files are written to the IBM Cognos BI domain directory. IBM Cognos BI terminates and is not accessible via the portal. This behavior occurs only when the IBM Cognos BI Managed Node is started with the WebLogic Administration Console.

Procedure

Start the IBM Cognos BI Managed Node using the WebLogic startup scripts instead.
Deploying IBM Cognos Business Intelligence IBM WebSphere Application Server fails

Deploying IBM Cognos BI to an IBM WebSphere application server may fail.

These errors can occur because the application file that you are trying to deploy is too large. If a deployment fails, any of the following errors may occur:

- Browser timeout in administration console
- HTTP 500 Internal Error
- Return to application file selection page

Procedure

If you are using the Build Application Wizard, clear the Include static files from the Webcontent folder check box when you select the application to build. This will reduce the size of the application file. If static content is required, you can manually copy it to the deployed application location after you have successfully deployed IBM Cognos BI into the application server.

Unable to deserialize context attribute error when deploying the p2pd.war file to WebLogic

An error may occur when you deploy the p2pd.war file to WebLogic.

This error does not affect the deployment of the p2pd.war file.

Error [context]Could not deserialize context attribute

java.io.NotSerializableException: com.cognos.logserver.LogService

Procedure

To avoid this problem, add at least one language preference in Internet Explorer.

Error displays after upgrading IBM Cognos Business Intelligence on a WebLogic Application Server

You are using WebLogic and upgrade IBM Cognos BI from an earlier release.

After you deploy the p2pd.war file for the new installation, a message similar to the following may display:

<BEA-101215> <Malformed Request "null". Request parsing failed, Code: -10>

About this task

This can occur if you undeploy IBM Cognos BI from WebLogic and some files from the earlier version are not removed from the system.

To solve the problem, do the following:

Procedure

1. Use the administrative tools for your application server to ensure that IBM Cognos BI has been undeployed.
For information about undeploying applications, see your application server documentation.

2. If the directory to which IBM Cognos BI was originally deployed is not removed during the undeploy process, delete the directory. Also, remove any IBM Cognos BI.jar files that are cached in your application server environment.

3. After you remove all files from the previous installation, redeploy IBM Cognos BI.

**Chinese, Japanese, or Korean characters are different after upgrade**

If you use Chinese, Japanese, or Korean characters, you may notice differences in some characters after upgrading from ReportNet to IBM Cognos Business Intelligence.

**Examples**

- You run an existing report. When you compare the output to the same report in ReportNet, you see that some of the characters are different.
- You do a search that you did in ReportNet and get different results.

The differences occurred because the conversion tables that are used for Chinese, Japanese, and Korean were modified to meet global standards. If your report specifications or search filters contain expressions that use constant values, the results may be affected.

**Procedure**

If you want to use the same conversion table that you used in ReportNet, run the following script in the `c10_location\bin` directory:

- On UNIX, type `conv_compat.sh`
- On Linux, type `conv_compat.sh`
- On Microsoft Windows operating system, type `conv_compat.cdm`

**Accented or double-byte characters may not display correctly when installing IBM Cognos Business Intelligence on Linux**

If you are using isssetup under a UTF-8 locale, accented or double-byte characters may not display correctly.

**Procedure**

To resolve this problem when installing in German or French, use a non-UTF-8 locale and then launch isssetup to install IBM Cognos BI.
RSV-SRV-0066 A soap fault has been returned or
RQP-DEF-0114 the user cancelled the request errors display in
high user load environments

These errors may be in the IBM Cognos cogserver.log if you have a high user load
(over 165 users) and interactive reports are running continuously in a distributed
installation.

Procedure
1. Increase the async_wait_timeout_ms parameter parameter in
   webapps/p2pd/WEB-INF/services/reportservice.xml file.
   For more information, see the IBM Cognos Business Intelligence Installation and
   Configuration Guide.
2. Increase the Queue Time Limit setting to 360.
   For information, see the IBM Cognos Business Intelligence Administration and
   Security Guide.

Unable to start IBM Cognos service when upgrading
multitenant installations

When upgrading multitenant installations of IBM Cognos software, you might not
be able to start the IBM Cognos service if instances of objects that violate the
tenant consistency rules are detected in Content Manager.

About this task

The consistency rules for multitenancy require that each tenant object in the
content store must have the same tenant ID as its parent, unless the parent object is
public.

To identify and resolve the instances of tenant consistency rules violation, you
must log on to IBM Cognos BI and run the content store consistency check. To do
that, you must start the IBM Cognos service despite the configuration error. This is
possible only if you set the ignoreInvalidTenantContainmentAtStartup Content
Manager property to true.

After the instances of tenant consistency rules violation are resolved, this property
should be removed.

Procedure
1. Start IBM Cognos Configuration on the computer where your Content
   Manager is installed.
2. Under Data Access, click Content Manager.
3. For Advanced properties, click the Edit icon in the Value column.
4. Click Add.
5. In the Name column, type ignoreInvalidTenantContainmentAtStartup.
6. In the Value column, type true.
7. Click OK.
8. Start the IBM Cognos service on the computer where Content Manager is
   installed.
   Assuming that there are no other configuration errors, you should now be
   able to start the IBM Cognos service.
9. Log on to IBM Cognos BI and run a consistency check on the content store to detect and resolve the tenant-related issues.

For more information, see the topic about creating and running a content store consistency check in the chapter about multitenant environments in the *IBM Cognos Business Intelligence Administration and Security Guide*.

10. After the tenant-related issues are resolved, remove the `ignoreInvalidTenantContainmentAtStartup` property from IBM Cognos Configuration.

11. Restart the IBM Cognos service.

---

**Problems configuring IBM Cognos Business Intelligence**

After you install IBM Cognos Business Intelligence components, you may encounter problems when you save changes in IBM Cognos Configuration.

Ensure that you
- configure and start the services on the computer where Content Manager is located before you configure other components
- restart the IBM Cognos service after you make any configuration changes

**Running Database and Index Cleanup Scripts**

In some troubleshooting situations, you may be advised to start with new configuration data.

You can run SQL scripts to delete all the tables in any of the following databases that IBM Cognos BI components use:
- content store for data that IBM Cognos BI needs to operate
- delivery database for report notifications
- metric store for metric package content and Metric Studio user preferences
- database for human tasks and annotations

You can run SQL scripts to delete all the tables and indexes in the following database:
- logging database for log messages

When you delete a table, its structural definition and data are deleted permanently from the database. For the metric store, database objects may also be deleted.

When you delete the indexes from a logging database, they are deleted permanently from the database.

When you restart the IBM Cognos service, a new set of required database tables and indexes are created automatically in the location specified by your configuration settings.

**Procedure**

1. On each computer where Content Manager is located, stop the IBM Cognos service.
2. Go to the appropriate directory:
   - To delete tables and indexes from the logging database, go to `c10_location\configuration\schemas\logging`.
To delete tables from the content store, go to \C10\configuration\schemas\content.
To delete tables from the notification database, go to \C10\configuration\schemas\delivery.
To delete tables from the metric store, go to \C10\configuration\schemas\cmm.
To delete tables from the human task and annotation database, go to \C10\configuration\schemas\hts.

3. Go to the appropriate database directory.
4. Depending on the database and database type, run one of the following scripts in the appropriate database tool to delete the tables.

The following table lists the script names for the content store database.

Table 80. Database type and script name for the content store database

<table>
<thead>
<tr>
<th>Database type</th>
<th>Script name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2</td>
<td>dbClean_db2.sql</td>
</tr>
<tr>
<td>DB2 on z/OS</td>
<td>dbClean_db2zOS.sql</td>
</tr>
<tr>
<td>Derby</td>
<td>dbClean_derby.sql</td>
</tr>
<tr>
<td>Informix</td>
<td>dbClean_informix.sql</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>dbClean_mssqlserver.sql</td>
</tr>
<tr>
<td>Oracle</td>
<td>dbClean_oracle.sql</td>
</tr>
<tr>
<td>Sybase</td>
<td>dbClean_sybase.sql</td>
</tr>
</tbody>
</table>

The following table lists the script names for the notification database.

Table 81. Database types and script names for the notification database

<table>
<thead>
<tr>
<th>Database type</th>
<th>Script name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2</td>
<td>NC_DROP_DB2.sql</td>
</tr>
<tr>
<td>DB2 on z/OS</td>
<td>NC_DROP_DB2.sql</td>
</tr>
<tr>
<td>Derby</td>
<td>NC_DROP_Derby.sql</td>
</tr>
<tr>
<td>Informix</td>
<td>NC_DROP_IFX.sql</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>NC_DROP_MS.sql</td>
</tr>
<tr>
<td>Oracle</td>
<td>NC_DROP_ORA.sql</td>
</tr>
<tr>
<td>Sybase</td>
<td>NC_DROP_SYBASE.sql</td>
</tr>
</tbody>
</table>

The following table lists the script names to clean up tables and indexes for the logging database.
For Informix, the index cleanup script must be edited if you host more than one audit logging database on the Informix instance and use them at the same time. See step 5.

Table 82. Script names to cleanup tables and indexes for the logging database.

<table>
<thead>
<tr>
<th>Database type</th>
<th>Script name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2</td>
<td>LS_dbClean_db2.sql</td>
</tr>
<tr>
<td></td>
<td>LS_dbCleanIndexes_db2.sql</td>
</tr>
<tr>
<td>DB2 on z/OS</td>
<td>LS_dbClean_db2zOS.sql</td>
</tr>
<tr>
<td></td>
<td>LS_dbCleanIndexes_db2zOS.sql</td>
</tr>
<tr>
<td>Derby</td>
<td>LS_dbClean_derby.sql</td>
</tr>
<tr>
<td></td>
<td>LS_dbCleanIndexes_derby.sql</td>
</tr>
<tr>
<td>Informix</td>
<td>LS_dbClean_informix.sql</td>
</tr>
<tr>
<td></td>
<td>LS_dbCleanIndexes_informix.sql</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>LS_dbClean_mssql.sql</td>
</tr>
<tr>
<td></td>
<td>LS_dbCleanIndexes_mssql.sql</td>
</tr>
<tr>
<td>Oracle</td>
<td>LS_dbClean_oracle.sql</td>
</tr>
<tr>
<td></td>
<td>LS_dbCleanIndexes_oracle.sql</td>
</tr>
<tr>
<td>Sybase</td>
<td>LS_dbClean_sybase.sql</td>
</tr>
<tr>
<td></td>
<td>LS_dbCleanIndexes_sybase.sql</td>
</tr>
</tbody>
</table>

The following table lists the script names for the metric store database.

Table 83. Script names for the metric store database

<table>
<thead>
<tr>
<th>Database type</th>
<th>Script name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2</td>
<td>cmm_uninstall dbalias username password</td>
</tr>
<tr>
<td></td>
<td>Specify the dbalias only if a database with the same name is already cataloged.</td>
</tr>
<tr>
<td>Microsoft SQL</td>
<td>cmm_uninstall metric_store_name database_name Admin_user_name password</td>
</tr>
<tr>
<td>Oracle</td>
<td>cmm_uninstall database_name database_user_name password</td>
</tr>
<tr>
<td></td>
<td>Replace database_name with the name in the tnsnames.ora file that refers to the database SID for Metric Studio</td>
</tr>
</tbody>
</table>

The following table lists the script names for the Human Task and Annotation database.
Table 84. Script names for the Human Task and Annotation database

<table>
<thead>
<tr>
<th>Database type</th>
<th>Script name</th>
</tr>
</thead>
<tbody>
<tr>
<td>all types</td>
<td>humanTaskService-dropScript.sql</td>
</tr>
</tbody>
</table>

5. If you have more than one audit logging database on your Informix instance, do the following:
   - Go to c10_location/configuration/schemas/logging/informix and open the file LS_dbCleanIndexes_informix.sql in a text editor.
   - Replace every instance of IPFSCRIPTIDX with the value that you specified when you created the IPFSCRIPTIDX property in IBM Cognos Configuration. For more information, see the topic about specifying a log messages repository in the IBM Cognos Business Intelligence Installation and Configuration Guide.
   - Save and close the file.

6. Start the IBM Cognos service.

Error trying to encrypt information when saving your configuration

When you save your configuration using the configuration tool, you may see an error message that the cryptographic information cannot be encrypted. An error occurred when requesting a certificate from the Certificate Authority.

The cryptographic information cannot be encrypted. Do you want to save the configuration in plain text?

Before you can encrypt your configuration settings, the computer where Content Manager is installed must be configured and running. On UNIX operating systems, ensure that you copied the appropriate .jar files to the installation location of your Java Runtime Environment. In addition, ensure that your Java environment is configured correctly, the URIs are correct, and the same certificate authority password is configured for all Content Manager computers.

On Linux operating systems, ensure that you copied the appropriate .jar files to the installation location of your Java Runtime Environment.

Also, an error message similar to the following may display:


The cryptographic error usually means the Java environment is not configured correctly. Ensure that the JAVA_HOME environment variable is set correctly and the appropriate security providers are installed, such as JSSE for JRE 1.5.

Checking the URI properties and certificate authority password

To ensure that configuration settings can be encrypted, ensure that the URI properties and certificate authority password in IBM Cognos Configuration are correct.

Procedure

1. On the Content Manager computer, start IBM Cognos Configuration.
2. In the Explorer window, click Environment.
3. In the Properties window, verify these properties:
   - Under Gateway Settings > Gateway URI
   - Under Dispatcher Settings > External dispatcher URI and Internal dispatcher URI
   - Under Other URI Settings > Dispatcher URI for external applications and Content Manager URIs
4. In the Explorer window, click Security > Cryptography > Cognos.
5. In the Properties window, under Certificate Authority settings, click the value for Password.
   Ensure that the same password is used on all Content Manager computers.
6. Save the configuration and restart IBM Cognos BI.

**CAM-CRP-1315 error when saving configuration**

When you save your configuration, an error occurs when there has been a change to your environment's trust domain.

The trust domain is managed by the certificate authority associated with the content store. The following error occurs if the content store you originally used was removed or if you modified your configuration to use a Content Manager associated with a different content store after you have saved your original configuration.

*CAM-CRP-1315 Current configuration points to a different Trust Domain than originally configured.*

To resolve the problem, change your configuration to use the original content store or regenerate the cryptographic keys using the following steps.

**Procedure**

1. On the Content Manager computer, back up the existing cryptographic keys by saving the following directories to an alternate location that is secure:
   - c10_location/configuration/csk
   - c10_location/configuration/encryptkeypair
   - c10_location/configuration/signkeypair
2. Delete the csk, encryptkeypair, and signkeypair directories.
3. In IBM Cognos Configuration, save the configuration and restart the services.
4. Repeat steps 1 to 3 on all computers that have IBM Cognos BI components installed.

**CAM-CRP-0221 error when logging into the portal**

After installing IBM Cognos Business Intelligence on Microsoft Windows operating system (either a 32-bit or 64-bit system) and configuring IBM HTTP Server as the gateway, attempts to log in to the IBM Cognos BI portal result in an error message that contains the following:

*CAM-CRP-0221 Unable to load the provider 'CAM_Crypto_TOpenSSL.dll' specified in the configuration file.*

This error occurs when incompatible versions of OpenSSL libraries are loaded. To resolve the problem, load the OpenSSL libraries that are provided with IBM Cognos BI.
Procedure
1. On the gateway computer, go to IBM_HTTP_location/conf directory and open httpd.conf in a text editor.
2. Add the following lines to the file:
   ```
   LoadFile "c10_location/cgi-bin/ssleay32.dll"
   LoadFile "c10_location/cgi-bin/libeay32.dll"
   ```
   where c10_location is the path to the IBM Cognos BI installation directory.

Manually changing the installation directory name affects installations running under an application server

After installing IBM Cognos Business Intelligence using the installation wizard and later renaming the installation directory or manually copying the contents to another directory, you attempted to run IBM Cognos Business Intelligence within an application server.

One of the following problems occurs:
- IBM Cognos BI does not start.
- Log directories are empty.
- Logs contain a linkage error or unsatisfied link error.

When you manually change the installation directory, the information in the IBM Cognos BI root directory becomes invalid. To resolve the problem, you must either update the IBM Cognos BI root directory before you create the IBM Cognos BI application file to deploy to the application server or you must reinstall IBM Cognos BI in the original location. If you reinstall IBM Cognos BI, follow the process for upgrading.

Procedure
1. In the new or renamed installation directory, open c10_location/webapps/p2pd/WEB-INF/classes/cogroot.link in a text editor.
2. Replace the path with the new location of the installation directory and save the file.
3. To build the application file to be deployed to the application server, in IBM Cognos Configuration, from the Actions menu, select Build Application Files.
4. If you built and deployed an application file to the application server before updating the cogroot.link file, undo the deployment.
5. Deploy the new application file to the application server.

For more information about configuring IBM Cognos BI for another application server, see the IBM Cognos Business Intelligence Installation and Configuration Guide.

Configuration data is locked by another instance of IBM Cognos Configuration

You may get an error message that the configuration data is locked by another instance of IBM Cognos Configuration.

When you start IBM Cognos Configuration, it checks to see if the cogstartup.lock file exists in c10_location/configuration. The file may exist if a previous instance did not shut down properly or if another instance of IBM Cognos Configuration is running.
Procedure
1. If another instance of IBM Cognos Configuration is running, exit that instance. Otherwise, any changes you make to the local configuration may result in errors.
2. If no other instance of IBM Cognos Configuration is running, delete the cogstartup.lock file in c10_location/configuration.
3. If the IBM Cognos service is stopped, click Start.

Unable to exit a tab sequence when using keyboard-only navigation in IBM Cognos Configuration
If you use the Tab key to navigate in IBM Cognos Configuration, you may experience problems exiting a tab sequence. For example, in the Properties window, you can press the Tab key to move from one property to another.

However, because IBM Cognos Configuration is a Java application, when you want to close the Properties window, you must press Ctrl+Tab.

Unable to save your configuration
You may be unable to save your configuration because you are missing a resource. For example, you delete a resource such as the Cognos namespace, a cryptographic provider, or the content store. You can specify a different database type for the content store with Oracle, Microsoft SQL Server, Informix, or Sybase. You can also configure a new cryptographic provider. You cannot specify a new Cognos namespace, but you can recreate it. However, you must then recreate your Cognos groups and roles.

For more information about creating groups and roles in IBM Cognos Connection, see the IBM Cognos Business Intelligence Administration and Security Guide.

Recreating the Cognos namespace
If you deleted the Cognos namespace, you must recreate it and then recreate your Cognos groups and roles.

Procedure
1. Start IBM Cognos Configuration.
2. In the Explorer window, under Security, right-click Authentication and then click New resource > Namespace.
3. In the Name box, type a name for the resource.
4. In the Type box, click Cognos, and then click OK.
   The Cognos namespace displays in the Explorer window.
5. From the File menu, click Save.
6. Recreate the Cognos groups and roles using IBM Cognos Administration.
   For more information, see the IBM Cognos Business Intelligence Administration and Security Guide.

Java error when starting IBM Cognos Configuration
When you start IBM Cognos Configuration, you may receive an error message that the Java Runtime Environment (JRE) has changed and that the current cryptographic information is not compatible with the new JRE. You may then be prompted to regenerate the cryptographic information for the new JRE or exit to switch back to the previous JRE.
This error may occur for one of these reasons:

- Your configuration data was encrypted using a different JRE than the one IBM Cognos BI components are currently using.
- The cryptographic information may have been corrupted.

If you click **Regenerate** in the error dialog, the IBM Cognos service is stopped and the cryptographic information is regenerated.

If you click **Exit** in the error dialog, you must set the JAVA_HOME environment variable to point to the JRE that you used to save your configuration.

On Microsoft Windows operating system, if you want IBM Cognos BI components to use the JRE that is installed by default, unset JAVA_HOME or set JAVA_HOME to `c10_location/bin/jre`.

**Note:** If you want to change from one JRE to another, see the topic on changing the version of JVM that IBM Cognos BI components use. For more information, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

### Cryptographic error when starting IBM Cognos Configuration

When you start IBM Cognos Configuration, the following error message may display:

*The cryptographic information may have been corrupted or the cogstartup.xml file is invalid. You may have to fix this file or remove it from disk. For more information, see the Installation and Configuration Guide.*

This error occurs when IBM Cognos BI components detect an error in the cogstartup.xml file. This can occur when the cogstartup.xml file is manually edited and there is an error in the changed text.

To resolve the problem, replace the cogstartup.xml file with a copy from your backup location.

### Restarting the IBM Cognos service to apply configuration settings

After changing default property values or adding a resource to your installation in IBM Cognos Configuration and then saving the configuration, you may not see the changes or be able to use the resource in the run-time environment.

To apply the new settings to your computer, you must restart the IBM Cognos service.

**Procedure**

1. Start IBM Cognos Configuration.
2. From the **Actions** menu, click the appropriate command:
   - If the IBM Cognos service is currently running, click **Restart**.
     - This action starts all installed services that are not running and restarts services that are running. If you want to restart a particular service, select the service node in the **Explorer** window and then click **Restart** from the **Actions** menu.
   - If the IBM Cognos service is stopped, click **Start**.
This action starts all installed services that are not running. If you want to start a particular service, select the service node in the Explorer window and then click Start from the Actions menu.

**CM-CFG-029 error when trying to save a configuration that specifies a Microsoft SQL Server content store**

In IBM Cognos Configuration, you try to save a configuration and the following error message is in the cogserver.log file:

*CM-CFG-029 Content Manager is unable to determine whether the content store is initialized.*

*EXECUTE permission is denied on object "sp_tables", database "master", owner "dbo".*

This indicates that you do not have the correct permissions to initialize a content store or create a table in the database.

Ensure that the content store user has permissions to use the sp_tables stored procedure in the master database.

**DB2 not found error for Linux on System z**

You installed IBM Cognos Business Intelligence and after you ran the C8DB2.sh script, an error stating that DB2 cannot be found is displayed or written to the log files.

**Procedure**

1. Create a profile that sources the sqlib/db2profile from the user's home directory for the user you enter when you run the script.
   
   An example .profile would contain something like the following:
   
   ```bash
   if [-f /home/db2user/sqlib/db2profile ]; then
     /home/db2user/sqlib/db2profile
   fi
   ```

2. Run the C8DB2.sh script again.

**DPR-ERR-2079 when Content Manager configured for failover**

You configured multiple computers as standby computers to ensure failover for Content Manager.

However, the following error message displays to the user:

*DPR-ERR-2079 Firewall Security Rejection. Your request was rejected by the security firewall*

This error message can occur if you have not configured all the standby computers as valid hosts for the IBM Cognos Application Firewall.

To solve this problem, on each distributed computer, start IBM Cognos Configuration and enter the names of all the computers that you are configuring for failover.

**Procedure**

1. In the Explorer pane, click Security > IBM Cognos Application Firewall.

2. In the IBM Cognos Application Firewall - Component Properties window, click in the Value column next to Valid domains or hosts.
3. Click the edit icon.
4. Enter the names of all the computers that you are configuring for failover.
5. Save and start the configuration.

**Importing a large content store in Solaris using JRE 1.5 fails**

If you export a content store that is greater than 2 GB when exported, and then attempt to import it in Solaris using JRE 1.5, the import fails with the following error message:

```
CM-SYS-5001 A Content Manager internal error occurred.
```

This is due to a bug in JRE 1.5 on Solaris. Use JRE 1.4.2 instead.

**Importing a large deployment in Windows crashes the Java virtual machine**

The Java virtual machine under Microsoft Windows operating system may crash under the following circumstances.

- The maximum Java memory setting is 1152 MB or higher.
- You are importing a large archive from a previous release of IBM Cognos Business Intelligence.
- The archive contains large models that require upgrading.

**Procedure**
1. Start IBM Cognos Configuration.
2. In the Explorer, under Environment, IBM Cognos services, click IBM Cognos.
3. Set the Maximum memory in MB property to 768.

**DPR-ERR-2008 error when you open a report**

You run a report and get the following error message:

```
DPR-ERR-2008 The dispatcher is unable to process the request. The request is directed to an unknown service name: local.xts.run
```

This error can occur if the Presentation service is not enabled. For example, in a multi-server environment where you use routing rules to send certain reports to a set of servers which have only the Batch report service, the Report service, and Dispatcher service enabled. If the report must be upgraded before execution, and the Presentation service is not available in the set of servers, the error is displayed.

To resolve this problem, enable that the Presentation service is enabled on at least one server in the server group. Then, try running the report again.

**Cannot load TM1 Cubeviewer or WebSheet iWidget in Business Insight**

You add a TM1 Cubeviewer or WebSheet iWidget in Business Insight, and you receive the following message:

```
There was an error loading the TM1Web required to run this iWidget.
```

One possible reason why this type of error may occur is if you are running TM1Web from a different domain.
This error can occur if you are using a Microsoft Internet Explorer web browser and your TM1 Web components are installed on a different computer than your IBM Cognos BI components.

To resolve this problem, you can do any of the following options:

- Install TM1 Web on the same computer as IBM Cognos BI.
- Use Firefox as your browser.
- Change your Internet Explorer security options to add the computer on which TM1 Web is running to your web browsers Trusted Sites and then enable **Access data sources across domains** for your Trusted Sites, as described in the following steps.

**Procedure**

1. In Internet Explorer, click **Tools > Internet Options > Security**.
2. Click **Trusted Sites**, and click **Sites**.
3. Enter the URL for the TM1 Web server, and click **Add**.
4. Click **Close**.
5. Click **Custom Level**.
6. Under **Miscellaneous**, select **Enable** or **Prompt** for **Access data sources across domains**.
7. Click **OK**.

**Users are prompted for Active Directory credentials**

The single signon mechanism does not work when IBM Cognos Business Intelligence is configured as follows:

- Microsoft Internet Explorer runs on a Microsoft Windows operating system NT computer.
- The authentication namespace is configured with the Active Directory provider.

As a result, users are prompted for their Active Directory credentials.

This problem occurs because the IBM Cognos BI Active Directory provider uses ADSI protocol and Kerberos delegation for authentication in a single signon environment. When Microsoft Internet Explorer runs on Windows NT, it cannot authenticate to the IIS server using Kerberos delegation.

When your system is configured for Windows Integrated Authentication, for the single signon to work with IIS, you must

- configure IBM Cognos BI to communicate with the Active Directory server using the LDAP provider.
- configure the external identity mapping property to read the REMOTE_USER environment variable.

**Font on UNIX not found when starting IBM Cognos Configuration**

A common problem occurs on UNIX, when you start IBM Cognos Configuration.

The following error message may display:
Font specified in font.properties not found...

This error occurs if the Java Virtual Machine (JVM) is trying to use one or more fonts that are not installed on your computer. However, the JVM should use the system default, and IBM Cognos Configuration should start and run normally.

**Procedure**

Add the missing fonts to your Java Runtime Environment by editing the font.properties files.

Several font.properties files, which contain standard font environment information, are installed with your Java Software Development Kit. You can find these files in the JRE_location/lib directory.

For more information, see the Java documentation.

**ESSBASEPATH cannot be detected**

For Microsoft Windows and UNIX platforms, Oracle Essbase software uses the ESSBASEPATH environment variable to locate the Essbase 11 client software. The Oracle Hyperion Enterprise Performance Management (EPM) System Installer creates ESSBASEPATH as a user environment variable.

If the IBM Cognos service is configured to run or log on as a system account, you must manually add ESSBASEPATH as a system environment variable, if it does not exist. When IBM Cognos software cannot locate the ESSBASEPATH environment variable, you receive the following error:

DB2-ERR-0044 Essbase environment variable "ESSBASEPATH" cannot be detected. Check if Essbase client is installed.

To resolve this issue, do one of the following, and then restart the IBM Cognos service:

- Double-click IBM Cognos service, and on the Log On tab, specify a user account that has access to ESSBASEPATH.
- Add ESSBASEPATH as a system environment variable.

Note that if you are upgrading to Essbase 11 software from Essbase 9 software, you must install the appropriate client and then edit the qfs_config.xml file to change the library name.

**Changing the library name in the qfs_config.xml file**

If you are upgrading to Essbase 11 software from Essbase 9 software, then after installing the appropriate client, you must change the library name in the qfs_config.xml file.

**Procedure**

1. In the c10_location/configuration directory, open the file named qfs_config.xml.
2. Find the line of code `<provider name="DB2OlapODP" libraryName="essodp93" connectionCode="D0"/>` and change the library name from essodp93 to essodp111.
3. Save the changes.

**Query fails when using Oracle Essbase Server**

You run a query to retrieve metadata or data from an Oracle Essbase server and you receive a message similar to one of the following messages:
- The IBM Cognos gateway is unable to connect to the IBM Cognos BI server. The server may be unavailable or the gateway may not be correctly configured.
- DB2-ERR-0005 An unknown error occurred during the login. Database error code: 1,042,006.
- XQES-DS-0006 Unable to logon to the data source.

These IBM Cognos errors can result from Windows not having enough sockets or ports available on the Microsoft Windows operating system. A lack of sufficient ports can cause data retrieval from Essbase to fail because of network communication errors.

To resolve this problem, increase the number of Windows sockets or ports that are available for program use.

**Increasing the number of Windows sockets or ports**

To resolve connection errors with an Oracle Essbase Server, increase the number of sockets or ports on the Microsoft Windows operating system that are available for program use by adding two entries in Microsoft Registry Editor.

**Important:** Use Microsoft Registry Editor at your own risk. Incorrect use may cause problems that require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly.

**Procedure**

1. From the Windows **Start** menu, run the regedit application.
2. In the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters** directory, create a new **DWORD** value named **MaxUserPort**.
3. Set the properties for **MaxUserPort** to use a value of **65534** and a base of **Decimal**.
   - The range for value is from 30000 to 65534.
4. In the same directory, add another **DWORD** value named **TcpTimedWaitDelay**.
5. Set the properties for **TcpTimedWaitDelay** to use a value of **50** and a base of **Decimal**.
   - The range for value is from 30 seconds to 300 seconds, with a default value of 240 seconds (4 minutes).
6. After closing the regedit application, restart the Microsoft CRM server or restart your computer.

**Results**

For more information, visit the technet2.microsoft.com Web site and search on the terms **MaxUserPort** and **TcpTimedWaitDelay**.

**Group membership is missing from Active Directory namespace**

If an Active Directory namespace is configured for the same forest and a user is authenticated using a credential, the group membership will be missing.

The process identity of IBM Cognos Business Intelligence, when running as a local system account or a domain user, must have one of these privileges:
- impersonate a client after authentication
• act as part of the operating system
If the privilege is missing, there is no group membership for the authenticated user.

Adding group membership for an Active Directory namespace
To add group membership for an Active Directory namespace, you must add the process identity for IBM Cognos Business Intelligence to the local security policy.

Procedure
1. From the Start menu, click Settings, Control Panel.
2. Click Administrative Tools, and then double-click Local Security Policy.
3. In the console tree, click Security Settings, Local Policies.
4. Click User Rights Assignment.
5. Add the process identity of IBM Cognos BI to one of the following policies:
   • Impersonate a client after authentication
     The default is Administrators, Service.
     For more information, see the library article fe1fb475-4bc8-484b-9828-a096262b54ca1033.mspx at the Microsoft Web site.
   • Act as part of the operating system
     The default is Local system.
     For more information, see the library article ec4fd2bf-8f91-4122-8968-2213f96a95dc1033.mspx at the Microsoft Web site.
Both of these privileges give an account the ability to act as another user.
The privilege Impersonate a client after authentication is similar to the Act as part of the operating system privilege except that it will only allow a process to impersonate after authentication, whereas the privilege Act as part of the operating system allows a process to impersonate before authentication.
For more information, see the library article tkerbdel.mspx at the Microsoft Web site.

Errors displayed when deploying to Oracle 10G Application Server
You are deploying IBM Cognos Business Intelligence to an Oracle 10G Application Server.

The following error messages may occur:
CMM-APP-3254 The initialization of the metrics store failed. DIS-ERR-3115
Task execution failed
MDS-RUN-3213 Unable to locate database bulk load utility. Please install the appropriate database tool for this platform ('bcp' for SQL Server, 'sqlldr' for Oracle)

These errors occur because the bulk loading utilities (SQL Loader on Oracle) are not included in the deployment file created by IBM Cognos Configuration.

Procedure
To install the missing components, use the Oracle client software on the computer where you installed the Oracle 10G Application Server.
Ensure that you install SQL Loader.
**CGI timeout error while connected to IBM Cognos Business Intelligence through a Web browser**

When performing operations through your Web browser, you receive the following error message:

*CGI Timeout, process will be deleted from server.*

The error occurs when you use Microsoft Internet Information Services (IIS) as your Web server and the gateway is configured to use CGI. IIS has a default timeout for CGI applications.

To resolve this problem, you can configure the gateway to use ISAPI or increase the CGI timeout in IIS.

IIS does not have a default timeout for ISAPI applications. Or, if you want to keep using a CGI gateway, you can increase the CGI timeout in IIS.

**Changing the gateway to ISAPI**

To resolve a CGI timeout error in the Web browser, you can change the gateway from CGI to ISAPI.

**Procedure**

1. On the gateway computer, start IBM Cognos Configuration.
2. Under **Environment**, for the **Gateway URI** property, change the cognos.cgi portion of the URI to cognosisapi.dll
3. In your Web browser, specify the ISAPI URI:
   
   `http://computer_name/ibmcognos/isapi`

**Increasing the CGI timeout**

To resolve a CGI timeout error in the Web browser, you can increase the duration of the CGI timeout in IIS.

**Procedure**

1. In the administrative tools for Microsoft Windows operating system, open Internet Information Services.
2. Under the local computer node, right-click **Websites** and select **Properties**.
3. In the **Home Directory** tab, click **Configuration**.
4. In the **Process Options** tab, increase the CGI script timeout.

**Servlet class fails to load in WebLogic**

You may have problems when configuring a distributed server installation and using WebLogic as the application server for IBM Cognos BI.

When deploying the p2pd.war for the Application Tier Components computer, you may receive servlet exceptions and the dispatcher does not start. The cogserver.log is also not created.

The following error messages display in the WebLogic Server console:

```plaintext
<Jul 9, 2004 3:47:37 PM EDT> <Error> <HTTP><BEA-101249>
<ServletContext(id=19023494,name=p2pd,context-path=/p2pd):Servlet class
com.cognos.pogo.isolation.ServletWrapper for servletcfgss could not be loaded because the
```
requested class was not found in the classpath /host2/bea812/user_projects/domains/c10/applications/p2pd/WEB-INF/classes. java.lang.ClassNotFoundException: com.cognos.pogo.isolation.ServletWrapper.

<Jul 9, 2004 3:47:37 PM EDT> <Error> <HTTP> <BEA-101216> <Servlet: "cfgss" failed to preload on startup in Web application: "p2pd". java.servlet.ServletException: [HTTP:101249][ServletContext(id=19023494,name=p2pd,context-path=/p2pd)]: Servlet class com.cognos.pogo.isolation.ServletWrapperfor servlet cfgss could not be loaded because the requested class was not found in the classpath /host2/bea812/user_projects/domains/c10/applications/p2pd/WEB-INF/classes.java.lang.ClassNotFoundException: com.cognos.pogo.isolation.ServletWrapper. at weblogic.servlet.internal.ServletStubImpl.prepareServlet (ServletStubImpl.java:799)
at weblogic.servlet.internal.WebAppServletContext.preloadServlet(WebAppServletContext.java:3252)

To avoid this problem, do not deploy the p2pd application from the WebLogic applications directory. Create the p2pd directory in another location and deploy p2pd from there.

Deploying the p2pd application outside of the WebLogic applications directory
To resolve issues with the servlet class failing to load when deploying IBM Cognos Business Intelligence to WebLogic, deploy the p2pd application to a different directory than the WebLogic applications directory.

Procedure
1. Open IBM Cognos Configuration and configure the Application Tier Components computer.
2. Restart the Content Manager computer.
3. Create a p2pd directory in a location that is accessible by the WebLogic server but is not in the WebLogic applications directory.
   For example, create a directory named p2pd in the following location:
   WebLogic_location/user_projects/domain_name
4. Create the p2pd.war file.
5. In the p2pd directory, extract the p2pd.war file to the WebLogic installation using the following command:
   %JAVA_HOME%/bin/jar xvfm "c10_location/p2pd.war
7. In the WebLogic Server Console, deploy the p2pd application.

Desktop icons or IBM Cognos Configuration window flicker on Windows
When you run IBM Cognos Configuration on Microsoft Windows operating system, you may notice that the desktop icons or the IBM Cognos Configuration window flickers.

Procedure
Start IBM Cognos Configuration using the -nodraw command line option.
Migration Does Not Work

After installing and configuring IBM Cognos PowerPlay, you either cannot find the Migration Assistant or you run a migration and nothing happens.

Procedure

To resolve the problem, check the following:

- The components PowerPlay Server and PowerPlay Administration are installed on the IBM Cognos PowerPlay server.
- If you install IBM Cognos PowerPlay with IBM Cognos Business Intelligence, install the IBM Cognos PowerPlay Content Manager component on the same computer as the IBM Cognos BI Content Manager component.
- On the computer where Content Manager is installed, in IBM Cognos Configuration, under Environment, IBM Cognos BI service, ensure the Migration service enabled property is set to True.
- IBM Cognos Series 7 Migration Components are installed on your IBM Cognos Series 7 PowerPlay Server computer.
- The IBM Cognos Series 7 migration service is started on the IBM Cognos Series 7 PowerPlay Server computer.
- Users are enabled to run a migration task. For more information, see the IBM Cognos PowerPlay Migration and Administration Guide.

Additionally, ensure that the users who will be running migration tasks have the appropriate permissions to create a migration task. In IBM Cognos Administration,

- Click Configuration, Content Administration.
- Click the Set Properties - Administration icon.
- Click the Permissions tab
- Ensure that the users who run migration tasks have Read, Write, Execute, and Traverse permissions.

Missing translations for object names in some locales

After you upgrade IBM Cognos Business Intelligence or import an archive, some object names might not be localized for certain locales. For example, Public Folders, My Folders, or group names display in English, and not in the specified language.

This problem might occur in the following situations:

- Cognos BI was upgraded to a newer version, but an older content store version was configured as the active Content Manager.
- An archive that was created with an older version of Cognos BI was imported into a newer version of Cognos BI.

For example, you might encounter untranslated object names in the Catalan, Croatian, Danish, Greek, Kazakh, Norwegian, Slovak, Slovenian, or Thai locale if your Cognos BI 10.2 installation is configured with the 10.1 version of Content Manager. Support for the above-mentioned locales was added in Cognos BI versions 10.1.1 and 10.2 so your 10.1 version of Content Manager does not have these translations.

To add the translations into the Cognos BI environment, perform the following procedure.
**Procedure**

1. Start IBM Cognos Configuration on the computer where the active Content Manager service is installed.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Confirm that the required locales are listed on the **Content Locales** and **Product Locales** tabs. If the locales are missing, add them and save your changes.
4. Go to `c10_location/webapps/p2pd/WEB-INF/classes` directory, and confirm that a `cmmsgsRL.locale.properties` message file exists for each required locale. For example, for Slovenian this message file is the `cmmsgsRL_sl.properties` file.
5. In the `c10_location/configuration` directory, copy the `updateInitialContentNames.xml.sample` file and save it as `updateInitialContentNames.xml`.
6. Edit the `updateInitialContentNames.xml` file:
   a. Specify the locales that you want to add. For example, modify the file in the following way to display Croatian and Slovenian object names:
   ```xml
   <updateInitialContentNames>
   <locales>
   <locale>hr</locale>
   <locale>sl</locale>
   </locales>
   </updateInitialContentNames>
   ```
   b. Remove or comment out any other locales that are not affected by the localization issue.
   c. Save your changes.
7. Start the IBM Cognos service.
8. To add another locale later, repeat these steps.

**Results**

The localized object names are added during the IBM Cognos service startup process. You can view the results of the operation in the `cogserver.log` file. The `updateInitialContentNames.xml` file is deleted in the process to prevent unnecessary updates on each restart.
Notices

This information was developed for products and services offered worldwide.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service. This document may describe products, services, or features that are not included in the Program or license entitlement that you have purchased.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Software Group
Attention: Licensing
3755 Riverside Dr
Ottawa, ON K1V 1B7
Canada

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.
Trademarks

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

The following terms are trademarks or registered trademarks of other companies:
- Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Glossary

This glossary includes terms and definitions for IBM Cognos Business Intelligence.

The following cross-references are used in this glossary:

- See refers you from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- See also refers you to a related or contrasting term.

To view glossaries for other IBM products, go to [www.ibm.com/software/globalization/terminology](http://www.ibm.com/software/globalization/terminology) (opens in new window).

**A**

access permission
A privilege that permits the access or use of an object.

accountability scorecard
A scorecard that Metric Studio automatically builds for each user which contains the metrics and projects they own.

agent
A process that performs an action on behalf of a user or other program without user intervention or on a regular schedule, and reports the results back to the user or program.

alias
An alternative name used instead of a primary name.

anonymous access
A type of access that allows users and servers to access a server without first authenticating with it.

application tier component
For installation, the set of processors that access the query databases to gather information and then render the results as PDF and HTML reports and metrics. Application tier components also pass requests to Content Manager and render the results that Content Manager retrieves from the content store.

attribute
In BI Modeling, a characteristic of an entity which is descriptive rather than a unique identifier or an aggregative measure.

authentication
The process of validating the identity of a user or server.

authentication provider
The communication mechanism to an external authentication source. Functionalities, such as user authentication, group membership, and namespace searches, are made available through authentication providers.

B

burst
To create several report results by running a single report once. For example, the user can create a report that shows sales for each employee, and run it once, sending different results to regional managers by bursting on region.

burst key
The dimension or level of a query in the report specification that is used to create, or burst, a set of report results.

C

CA
See certificate authority.

calculated member
A member of a dimension whose measure values are not stored but are calculated at run time using an expression.

canvas
An area within a dashboard or workspace that users interact with to create, view, and manipulate content and data.

capability
A group of functions and features that
can be hidden or revealed to simplify the user interface. Capabilities can be enabled or disabled by changing preference settings, or they can be controlled through an administration interface.

cardinality
1. For relational data sources, a numerical indication of the relationship between two query subjects, query items, or other model objects.
2. For OLAP data sources, the number of members in a hierarchy. The cardinality property for a hierarchy is used to assign solve orders to expressions.

cascading prompt
A prompt that uses values from a previous prompt to filter the values in the current prompt or pick list.

certificate
In computer security, a digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also [certificate authority].

certificate authority (CA)
A component that issues certificates to each computer on which components are installed.

class style
A combination of formatting characteristics, such as font, font size, and border, that the user names and stores as a set.

custom set
In Analysis Studio, a named object which can include filter rules, calculations, and sort rules. Custom sets can define a set of members that is different from any set originally defined in the cube model. See also [predefined set].

cryptosystem
The combination of authentication, key exchange algorithm, and the Secure Sockets Layer (SSL) cipher specification used for the secure exchange of data.

cube
A multidimensional representation of data needed for online analytical processing, multidimensional reporting, or multidimensional planning applications.

credential
A set of information that grants a user or process certain access rights.

customer
A named email address to which reports and agent e-mails can be sent. Contacts are never authenticated.

decryption
The step in which a message encoded as a cipher text is decoded back into plain text.

decryption key
A key that decrypts a cipher text that has been encrypted with a corresponding encryption key.

dependent set
A set whose members are included within the members of another set.

dependent variable
A variable in a function whose value depends on the value of another variable.

descriptor (meta data)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.

descriptor (metadata)
A data type that can be used to define attributes of other data types.
**dashboard**
A web page that can contain one or more widgets that graphically represent business data.

**data source**
The source of data itself, such as a database or XML file, and the connection information necessary for accessing the data.

**data source connection**
The named information that defines the type of data source, its physical location, and any sign-on requirements. A data source can have more than one connection.

**data tree**
Within a studio, a structure that contains objects such as query subjects, query items, dimensions, levels, and members. A data tree is used as a palette of the available data that can be inserted into calculations, filters, display areas, and other authoring gestures.

**deployment**
The process of moving an application (such as a report or model) to a different instance. For example, reports are often created in a test environment and then deployed to production. When an application is deployed, it is exported, transferred, and imported.

**deployment archive**
A file used for deployment. A deployment archive contains the data from the content store that is being moved.

**deployment specification**
A definition of what packages to move (deploy) between source and target environments, the deployment preferences, and the archive name. Deployment specifications are used for import and export.

**derived index**
A calculated metric that provides a status and a score based on other metrics.

**details-based set**
A set based on an item and its immediate details. See also set.

**dimension**
A broad grouping of descriptive data about a major aspect of a business, such as products, dates, or locations. Each dimension includes different levels of members in one or more hierarchies and an optional set of calculated members or special categories.

**dimensional data source**
A data source containing data modeled using OLAP concepts, including dimensions, hierarchies, and measures.

**drill down**
In a multidimensional representation of data, to access information by starting with a general category and moving downwards through the hierarchy of information, for example from Years to Quarters to Months.

**event**
A change to a state, such as the completion or failure of an operation, business process, or human task, that can trigger a subsequent action, such as persisting the event data to a data repository or invoking another business process.

**event key**
A combination of data items that uniquely defines an event instance. Identifying an event instance enables the agent to determine if it is new, ongoing or stopped.

**event list**
The set of detected event instances evaluated by the task execution rules to determine which agent tasks should be performed.

**fact**
See measure.

**gateway**
An extension of a web server program that transfers information from the web server to another server. Gateways are
often CGI programs, but may follow other standards such as ISAPI and Apache modules.

glyph The actual shape (bit pattern, outline) of a character image. For example, italic A and roman A are two different glyphs representing the same underlying character. Strictly speaking, any two images which differ in shape constitute different glyphs. In this usage, glyph is a synonym for character image, or simply image (The Unicode Standard – Version 1.0).

group A collection of users who can share access authorities for protected resources.

grouping In reporting, the process of organizing common values of query items together and only displaying the value once.

H

hierarchy The organization of a set of entities into a tree structure, with each entity (except the root) having one or more parent entities and an arbitrary number of child entities.

I

information card A display of high-level information about dashboard, workspace, or report content, such as owner, contact information, date modified, and an optional thumbnail view of the dashboard, workspace, or report.

information pane In Analysis Studio, a pane that helps the user to confirm their selection in the data tree by displaying related information, such as the level and attributes.

initiative A task developed to achieve objectives or close the gap between performance and targets. Initiatives are associated with individual objectives and often known as projects, actions, or activities.

item See member

J

job A group of runnable objects, such as reports, agents, and other jobs that the user runs and schedules as a batch.

job step The smallest part of a job that can be run separately. A job step can be a report or it can be another job.

L

layout The arrangement of printed matter on a screen or page, including margins, line spacing, type specification, header and footer information, indents, and more.

level A set of entities or members that form one section of a hierarchy in a dimension and represent the same type of object. For example, a geographical dimension might contain levels for region, state, and city.

locale A setting that identifies language or geography and determines formatting conventions such as collation, case conversion, character classification, the language of messages, date and time representation, and numeric representation.

M

MDX See Multidimensional Expression Language

measure A performance indicator that is quantifiable and used to determine how well a business is operating. For example, measures can be Revenue, Revenue/Employee, and Profit Margin percent.

member A unique item within a hierarchy. For example, Camping Equipment and 4 Man tent are members of the Products hierarchy.

metric A measure to assess performance in a key area of a business.

metric extract A set of mappings between an existing Cognos data source and a Metric Studio object or value. For example, a cube
measure named Revenue is mapped to a Metric Studio metric named Revenue Actual Value.

**metric package**
In Cognos Connection, a representation of a Metric Studio application. A metric package contains connection information, reports, and metric management tasks for that application. See also **package**.

**metric store**
A database that contains content for metric packages. A metric store also contains Metric Studio settings, such as user preferences.

**metric type**
A category of metrics that defines the business rules such as performance pattern, units, and meaning of a group of metrics. For example, Revenue can be a metric type, and European Revenue and North American Revenue would be metrics of this type.

**model**
A physical or business representation of the structure of the data from one or more data sources. A model describes data objects, structure, and grouping, as well as relationships and security. In Cognos BI, a model is created and maintained in Framework Manager. The model or a subset of the model must be published to the Cognos server as a package for users to create and run reports.

**multidimensional data source**
See **dimensional data source**.

**Multidimensional Expression Language (MDX)**
The multidimensional equivalent of Structured Query Language (SQL).

**N**

**named set**
See **predefined set**.

**namespace**
A part of the model in which the names may be defined and used. Within a namespace, each name has a unique meaning.

**news item**
A single entry in a Really Simple Syndication (RSS) compatible format. It can include a headline, text, and a link to more information. A news item task in an agent can be used to create news items for display in a Cognos Connection portlet.

**O**

**object**
In Report Studio, an empty information container that can be dragged to a report from the Toolbox tab and then filled with data. Reports are made up of objects, which include crosstabs, text items, calculations, graphics, and tables.

**object extract**
An extract that defines the metadata for a Metric Studio object, such as a user defined column, a scorecard, or a data source.

**P**

**package**
A subset of a model, which can be the whole model, to be made available to the Cognos server. See also **metric package**.

**page set**
In Report Studio, a set of one or more designed pages which repeat in the report output for each instance of a chosen query item. See also **set**.

**passport**
Session-based information, stored and encrypted in Content Manager memory, regarding authenticated users. A passport is created the first time a user accesses Cognos 8, and it is retained until a session ends, either when the user logs off or after a specified period of inactivity.

**portlet**
A reusable component that is part of a web application that provides specific information or services to be presented in the context of a portal.

**predefined set**
A set of members defined inside an OLAP data source as a list or by an expression. Predefined sets can be used in analysis and report authoring. See also **custom set**.

**product locale**
The code or setting that specifies which language, regional settings, or both to use for parts of the product interface, such as menu commands.
project

1. In Metric Studio, a task or set of tasks undertaken by a team and monitored on a scorecard. A project tracks dates, resources, and status.

2. In Metric Designer, a group of extracts. Each extract contains the metadata that is used to populate the Metric Studio data store or to create applications.

prompt

A report element that asks for parameter values before the report is run.

properties pane

Within a studio, a pane that provides an overview of the properties for selected data. The properties pane can also be used to make several changes and apply them at the same time, instead of repeating several different commands.

publish

In Cognos BI, to expose all or part of a Framework Manager model or Transformer PowerCube, through a package, to the Cognos server, so that the data can be used to create reports and other content.

query

The simple report specifications created and edited by Query Studio.

query item

A representation of a column of data in a data source. Query items may appear in a model or in a report and contain a reference to a database column, a reference to another query item, or a calculation.

query subject

A named collection of query items that are closely functionally related. Query subjects are defined using Framework Manager to represent relational data and form the set of available data for authoring reports in Query Studio and Report Studio. A query subject is similar to a relational view in that it can be treated as a table but does not necessarily reflect the data storage.

R

Really Simple Syndication (RSS)

An XML file format for syndicated web content that is based on the Really Simple Syndication specification (RSS 2.0). The RSS XML file formats are used by Internet users to subscribe to websites that have provided RSS feeds. See also Rich Site Summary.

repeater

In Report Studio, a cell container that repeats values within itself with no predefined internal structure.

repeater table

In Report Studio, a table-like container that repeats cells across and down the page or row in the associated query.

report

A set of data deliberately laid out to communicate business information.

report output

The output produced as a result of executing a report specification against a data set.

report specification

An executable definition of a report, including query and layout rules, which can be combined with data to produce a report output.

report view

A reference to another report that has its own properties, such as prompt values, schedules, and results. Report views can be used to share a report specification instead of making copies of it.

response file

An ASCII file that can be customized with the setup and configuration data that automates an installation. During an interactive installation, the setup and configuration data must be entered, but with a response file, the installation can proceed without any intervention.

Rich Site Summary (RSS)

An XML-based format for syndicated web content that is based on the RSS 0.91 specification. The RSS XML file formats are used by Internet users to subscribe to websites that have provided RSS feeds. See also Really Simple Syndication.
see Really Simple Syndication.
2. See Rich Site Summary.

**S**

**score** A number or ranking that expresses applicability in relation to a standard.

**scorecard** A collection of metrics representing the performance of one unit or aspect of an organization.

**scorecard structure** The hierarchy of scorecards that reflects how an enterprise organizes its metrics.

**security provider** See authentication provider.

**selection-based set** A collection of individual items that the user has explicitly selected. The items or members may be selected from one or more levels of the same hierarchy. See also set.

**session** The time during which an authenticated user is logged on.

**set** A collection of related items or members. Members in a set may be specifically chosen, or selected by one or more filter rules. See also custom set, details-based set, page set, predefined set, selection-based set, stacked set.

**stacked set** Two or more sets arranged one above another in rows or side-by-side in columns. See also set.

**strategy** The overall plan of action (such as for a brand unit, business unit, channel, or company) to achieve a stated goal. Strategies normally cover a period of more than one year.

**strategy map** In Metric Studio, a visual representation of the strategy and the objectives of that strategy for an organization. For example, a strategy map may show employees how their jobs are aligned to the overall objectives of the organization.

**summary** In reporting and analysis, an aggregate value that is calculated for all the values of a particular level or dimension. Examples of summaries include total, minimum, maximum, average, and count.

**T**

**task** An action performed by an agent if the event status meets the task execution rules. For example, an agent can send an email, publish a news item, or run a report.

**task execution rule** A user-specified option within an agent that determines which statuses and values cause a task to be run. It determines which tasks to execute for each event instance.

**template** In report authoring, a reusable report layout or style that can be used to set the presentation of a query or report.

**thumbnail** An icon-sized rendering of a larger graphic image that permits a user to preview the image without opening a view or graphical editor.

**tuple** An ordered collection of two or more members from different dimensions. For example, the tuple (2007, Camping Equipment, Japan) returns the value for the intersection of the three members: 2007, Camping Equipment, and Japan. Tuples can be used to filter and sort data, and to create calculations.

**U**

**union set** See stacked set.

**user** Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

**user-defined column** In metric management, a column used to represent a value other than the actual or target. It may be an industry benchmark or any other useful additional numerical information for a period, including a calculation based on the other values of the metric. User-defined columns may be different for each metric type.
watch list
A list of metrics that each user has chosen to monitor closely. If notification is enabled in Metric Studio, the user will receive email notification of changes to these metrics. Users can also choose to display their watch list as a portlet within Cognos Connection.

watch rule
A user-defined condition that determines whether a report is delivered to the user. When the rule is run, the output is evaluated and, if it satisfies the condition or rule, the report is delivered by email or news item. Watch rules limit report delivery to those reports containing data of significance to the user.

Web Services for Remote Portlets
A standard for creating presentation-oriented web services so that they can be easily integrated within other applications, such as web portals.

widget
A portable, reusable application or piece of dynamic content that can be placed into a web page, receive input, and communicate with an application or with another widget.

work area
The area within a studio that contains the report, analysis, query, or agent currently being used.

workspace
See dashboard
Index

Special characters

- .ats file using to remove components 270

Numerics

1024-bit certificates 204
32-bit installation requirement for 32-bit library files 28
64-bit application server problem connecting to IBM Cognos BI portal 328
64-bit installation requirement for 64-bit library files 28
64-bit installations 13
64-bit operating system memory 24

A

accented characters not displayed properly 321
access
- configuring secure access to the portal 71, 109
accessibility features 291
active Content Manager 92
Active Directory Server
- advanced properties 146
- authenticating in multiple domains 146
- enabling single signon 148
- enabling SSL 146
- Kerberos authentication 243
- missing group membership 335
- using for authentication 143
- with an LDAP namespace 160
active scripting
- enabling in Web browsers 34
agent service 272
AIX
- environment variables to install IBM Cognos BI 55, 93, 112, 119
- error connecting to DB2 database 312
- support for RACF namespace 173
aliases
- configuring on Web servers 73, 125
Analysis Studio
- component description 7
- annotation service 272
anonymous access
- disabling 71, 109
anonymous logon
- disabling 142
Apache modules 73, 126
Apache Tomcat
- tuning for 64-bit installations 276
Apache Web servers
- configuring aliases 73, 125
application pools 73, 125
- application servers changing from the default 247
- configuring 256
application servers (continued)
- JVM options 248
- problems running IBM Cognos BI 328
- servlet class fails to load in WebLogic 337
- servlet gateways 77, 130
- startup script fails 319
- startup scripts 255
- upgrading IBM Cognos BI 263
application tier components
- configuration requirements 12
- installing on separate computer 12
Application Tier Components
- installing 53
- log server 215
Architect models
- migration to IBM Cognos BI 15
archiving
- report output 199
ASCII
- requirements for installation directory 314
Asynchronous timeout 278
audience of document xi
audit
- logs 215
- audit logs
  See also log messages
  See also troubleshooting
- log destinations 215
authentication
- Active Directory Server 143
- CA SiteMinder 170
- configuring IBM Cognos Series 7 namespace 152
- custom authentication providers 156
- custom properties for Active Directory Server 145
- custom user properties for LDAP 167
- deleting namespaces 177
- disabling anonymous logon 142
- domain trees for Active Directory Server 146
- LDAP 157, 158
- LDAP using Active Directory Server 160
- LDAP using IBM Directory Server 162
- LDAP using Novell Directory Server 163
- LDAP using Oracle Directory Server 165
- requirements for single signon with Microsoft Analysis Server or Microsoft SQL Server 144
- SaferAPIGetTrustedSignon function 154
- SAP 175
- single signon using Active Directory Server 148
- single signon using IBM Cognos Series 7 namespace 153
- single signon using LDAP 169
- single signon using RACF 174
- single signon using SAP 176
- Siteminder provider 172
- SSL using LDAP 168
- trusted signon plug-ins for IBM Cognos Series 7 154
- using namespaces 141
authentication provider
- configuring IBM Cognos BI to use security 67, 109
backing up
  IBM Cognos BI information 180, 249
basic installations
  multiple locations 90
batch report service 273
Batch report service
  list of embedded fonts for PDF reports 197
Bind user DN and password property
  special characters for LDAP namespace 157
bookmark conversion utility 8
Build Application Wizard 253
builds
  running in IBM Cognos Connection by using Data Movement service 18

c8db2.sh script
  error 331
CA certificates 204
CA SiteMinder 170
configuring namespaces 172
  cross-script checking in IBM Cognos Application Firewall 190
CA,
  See certification authority
CAM-CRP-1157 error 308
certificate authority
  configuring 205
  certification authority
    configuring the service 205
CGI gateway
  Apache server 78, 131
  IBM HTTP Server 78, 131
CGI timeout errors 337
changing
  configuration template 275
  default configuration settings 182
  email encoding 228
  Java versions 180
  URLs 184
characters
  encoding not supported 308
  characters improperly displayed 321
Chinese
  characters display incorrectly after upgrade 321
  corrupt characters during installation on Linux 318
chunking patches
  application servers 248
cipher suites
  setting a priority for SSL connections 214
client component 8
client setup
  DB2 databases 60, 97
CM-SYS-5001 A Content Manager internal error occurred 332
CM-SYS-5007 error 313
cogconfig.sh
  command line options 293
Cognos Content Database
  changing users and passwords 183
  component description 7
  improving performance 276
Cognos namespace
  recreating 329
Cognos service
  starting from the command line 284
Cognos Viewer
  component description 6
Cognos Workspace approved domains 190
cogroot.link file 328
cogstartup.lock file 302
cogstartup.xml file 280, 284
  changing properties manually 281
  invalid file 330
collation sequences
  case-sensitive 308
command line options 293
common symmetric key 186
compatible query mode
  memory 24
components 5
  Analysis Studio 7
  application tier components 12
  bookmark conversion utility 8
Cognos Content Database 7
Cognos Viewer 6
Content Manager 7, 12, 53
data store 9
data sources 9
gateways 6, 11, 53
IBM Cognos Administration 6
IBM Cognos BI samples 7
IBM Cognos Configuration 6
IBM Cognos Connection 6
IBM Cognos Workspace 7
installation requirements for 64-bit systems 13
installing 53
installing on one computer 10
Migration Assistant 8
Migration Service 8
  optional 7
other 5
report server 53
Confidentiality algorithm 188
configuration
  adding resources 280
  automating 265
  backing up 180, 249
  changing defaults settings 182
  changing the template 275
Content Manager 12
cryptographic information cannot be encrypted 326
data locked 329
default settings 182
error when encrypting information 326
global settings 223
issues 323
lock file 302
multiple versions of IBM Cognos BI 43
requirements for single signon with Microsoft Analysis Server or Microsoft SQL Server 144
running from command line 284
settings for IBM Cognos BI 25, 182
settings not applied 330
testing 83
Tomcat settings 25
unable to open IBM Cognos Configuration 302
unable to save 329
unattended 265, 269
configuration files
  applications.xml for Portal Services 236
coglocale.xml 282
cogstartup.xml 280
exporting 269
configuring 293
  Active Directory namespace 144
  application server properties 256
certificate authority service 205
custom authentication providers 156
default time zone 228
destination for log messages 215
environment properties for application tier
  components 117
fonts 194
gateways 124
IBM Cognos BI 33
IBM Cognos service 275
LDAP namespace 158
LDAP namespace for Active Directory Server 160
LDAP namespace for IBM Directory Server 162
mail server 108
mail server accounts 70
notification databases 203
Portal Services 235
properties in an unattended configuration 281
RACF namespace 173
SAP namespace 176
shared trust with other servers 212
SiteMinder provider 172
SSL protocol 210
standby Content Manager 106
temporary file location 192
transfer specification files (.ats) 265
unattended 269
Web browsers 34
Web server 73, 125
connections
  data source 139
content expiry
  images directory 73, 125
content locales
  customizing 225
displaying supported locales 225
mapping to user locale 225
Content Manager
  active and standby 92
  attempt to register the dispatcher 313
  changing time zones 228
  component 12
  component description 7
  configuration 12
  configuring on multiple computers 106
  error messages 331
  failover protection 12
  fails to start 313
  installation options 12
  installing 53
  log server 215
requirements for changing application server 248
requirements if using IBM Cognos Transformer with Series 7 namespace 53, 152
saving report output externally 200
setting up a content store 203
standby 12
Content Manager service 273
Content Manager URLs 106, 117

content store
  and other locations to store report output 197
  backing up 180, 249
compatibility versions of DB2 and Java 308
component description 9
connection management 67, 103
creating 53, 203
creating on Oracle 30
creating tablespaces 62, 98
deleting tables from the database 323
invalid settings 308
multiple versions of IBM Cognos BI 43
requirements for changing application server 248
upgrading 312
context attribute cannot be deserialized 320
cross-script checking
  configuring in IBM Cognos Application Firewall 190
cryptographic error 330
cogstartup.xml file invalid 330
JRE error 330
cryptographic information cannot be encrypted 326
cryptographic keys
  backing up and deleting 180, 249
  regenerating 327
cubes
  cannot open 314
customizing
  custom user properties
    Active Directory Server 145
    LDAP 167
customization support 224
custom user properties
  Active Directory Server 145
  LDAP 167
dashboards
  application 3
data
  locked by IBM Cognos Configuration 329
  sharing data locations in a network 234
Data files location
  configuring for Windows Vista 234
Data integration service 273
Data Manager
  using in IBM Cognos BI 18
Data Movement service
  using in IBM Cognos Connection 18
data source connections
  setting 67, 103
data sources
  component description 9
  samples connections 139
  setting up Kerberos-enabled 243
database cleanup scripts 323
database client
  setting up for a logging database 216
database connection strings
  IBM DB2 67, 103
  Microsoft SQL Server 67, 103
  Oracle 67, 103
database connections 103
database drivers
  DB2 60, 97
  Informix 65, 102, 217
  Oracle 65, 102
  Sybase 65, 102
databases
  bulk load utility missing 336
  content store 203
deleting tables 323
  logging 218
  logging database client 216
  notification 108
DB2
  client setup 60, 97
database drivers 60, 97
  specifying as a log messages repository 219
supported Java versions 308
DB2 content store 275
derror when running C8DB2.sh script 331
script 61, 98
DB2-ERR-0005 335
default connection pool time-out
  conflicts between IBM Cognos BI and some application servers 251
deleting dispatchers 48
delivery
  decreasing the time to open reports 277
delivery service 273
deploying
  configuration objects 50
deploying IBM Cognos BI 256
  deployment archives
    importing 50
    moving 50
Deployment files location
  configuring for Windows Vista 232
Derby
  page cache size 276
description of product xi
diagnostics
  See troubleshooting
differences
  between IBM Cognos Series 7 PowerPlay and IBM Cognos PowerPlay xi
directory not found error 316
disabling
  anonymous access 71, 109
  dispatcher unregistering 262
dispatchers
  Application Tier Components computer 337
deleting 48
  importing 50
  system metrics 271
  displayLog
    new feature description for version 10.2 2
displayLog option 268
distributed installations
  scenarios 9
documentation
  Software Development Kit 3
domains
  Active Directory Server domain trees 146
  approved for Cognos Workspace 190
setting for cookies 229
double-byte characters
  improperly displayed 321
download of resource fails 312
DPR-CMI-4006 error 313
DPR-DPR-1035 error 308
DuseCMLargeResultSet parameter 313
dynamic query mode
  memory 24
E
EAR files,
  See Enterprise archive files
e-mail
  configuring mail server accounts 70
e-mail messages
    changing the encoding 228
    embedded fonts 197
  enabling
    IBM Cognos Application Firewall 190
    services 193
    SSL for an application server 261
Encrypt temporary files property 192
encryption
  changing settings in unattended configuration 281
  configuration errors 326
Enterprise archive files
  deploying IBM Cognos BI 285
environment properties 66
environment variables
  configuring for application tier components 117
  requirements on Windows Vista 232
  setting for application servers 250
  to install IBM Cognos BI on UNIX or Linux 55, 93, 112, 119
error messages
  CAM-CRP-1064 311
  CAM-CRP-1315 Current configuration points to a different trust domain 327
  CFG-ERR-0106 Cognos Configuration received no response 305
  CGI timeout 337
  CM-CFG-029 Content Manager is unable to determine 331
  CMM-APP-3254 The initialization of the metrics store failed 336
corrupt cryptographic information 330
could not deserialize context attribute 320
cryptographic information cannot be encrypted 326
DIS-ERR-3115 Task execution failed 336
download of specified resource fails 312
DPR-ERR-2014 314
DPR-ERR-2022 No response generated 318
DPR-ERR-2058 313, 316
DPR-ERR-2079 331
HTTP Error 404 316
Java Runtime Environment 330
malformed request 320
MDS-RUN-3213 Unable to locate database bulk load utility 336
page not found 316
PRS-CSE-1255 311
RQP-DEF-0114 322
RSV-SRV-0066 322
error messages (continued)
servlet class fails to load on WebLogic 337
SoapSocketException 313
SQL1224N 312
Unable to load balance the request 314
you have chosen to download a file 319
ers
ESSBASEPATH 334
ESSBASEPATH
adding 334
event logs 218
event management service 273
exporting
configuration files 269
external identity mapping property
editing for an LDAP namespace 169
External identity mapping property
special characters for LDAP namespace 157
external object store
for report output 200
testing connection 201

F
failover protection 12
features
new features in version 10.2.1 1
file locations
requirements on Windows Vista 232
file system
to save copies of report output 197
files
not found 316
Firefox
browser settings 34
fix pack
installing 58, 96, 115, 122
fix packs
installing on UNIX or Linux computers 59, 97, 116, 123
installing on Windows computers 59, 96, 115, 123
flcker 338
font embedding lists 197
fonts
changing for PDF reports 196
changing the default 196
configuring 194
list of embedded fonts for PDF reports 197
not found when starting IBM Cognos Configuration on UNIX 334
Framework Manager
cryptographic error 307
uninstalling 290

G
gateway
connection issues 328
gateways
adding in a network to decrease delivery times 277
component description 6
configuration requirements 11
configuring 124
configuring to use a namespace 193
installing 53
installing on separate computer 11
log file 303

gateways (continued)
recommended settings for Microsoft IIS 337
when to use ISAPI 337
GB18030 194, 196
glossary 345
Google Chrome
browser settings 34
graphics service 273
groups
missing membership in Active Directory Server 335

H
HP-UX
environment variables to install IBM Cognos BI 55, 93, 112, 119
HTML cookies,
See cookies
HTTP Error 404 316
human task service 273

I
IBM Cognos
maintenance package installation 58, 96, 115, 122
updater 58, 96, 115, 122
IBM Cognos Administration
component description 6
IBM Cognos Application Firewall
configuring 190
IBM Cognos BI
changing application servers 247
components 5
configuring 33
default settings 53
deploying 256
dispatchers 274
does not start on an application server 328
installation options 9
installing 53
installing migration tool on Windows 84, 136
logging in 67, 109
maintenance package installation 58, 96, 115, 122
service does not start 308
services 274
system requirements 22
troubleshooting installations 295
uninstalling 289
updater 58, 96, 115, 122
with Kerberos authentication 241
IBM Cognos BI portal
problem connecting on 64-bit WebSphere Application Server 328
IBM Cognos BI samples 7
IBM Cognos BI server
fails to start 308
IBM Cognos Configuration
command line options 293
component description 6
font not found error on UNIX 334
invalid settings 308
problems opening 302
problems saving a configuration 323
problems with keyboard navigation 329
unable to start 329
unattended mode 269
Java Management Extensions
- configuring JMX properties for remote monitoring of system metrics 271
- with user logs 222
Java scripts
- enabling in Web browsers 34
Java Software Development Kit from IBM 271
Java virtual machine
- crashes when importing deployment 332
JAVA_HOME
- setting 330
java.lang.NoClassDefFoundError 307
JDBC drivers
- setting up Oracle databases 217
job service 273
JobStreams
- running in IBM Cognos Connection by using Data Movement service 18
JREs
- updating 24, 181
JVM
- changing 180, 249
- copying security provider files 181
- memory settings for Cognos Content Database 276
JVM options 248

K
Kerberos authentication 149
- Active Directory Server namespace 243
- constrained delegation 150
- creating a data source 243
- enabling single signon 241
keyboard
- navigation problems 329
keyboard shortcuts 291
Korean characters
- corrupt during installation on Linux 318
- display incorrectly after upgrade 321

L
language
- customizing for user interface 223
- customizing locale content support 225
languages
- conversion tables 321
- incompatibility after upgrade 321
latency
- improving 277
LDAP
- Active Directory Server 160
- configuring a namespace 158
- custom properties 167
- editing the External identity mapping property 169
- enabling single signon 169
- enabling SSL 168
- IBM Directory Server 162
- Novell Directory Server 163
- Oracle Directory Server 165
- using for authentication 157
LDAP templates
- new feature description version 10.2 2
library files
- for 32-bit versus 64-bit installation 28
libXm.so.4
- error running issetup 304
Lifecycle Manager 52
Linux
- characters not displayed properly 321
- corrupt characters during installation 318
- environment variables for IBM Cognos BI 55, 93, 112, 119
- log messages 218
- starting and stopping the Cognos service 284
- system requirements 53
Linux on System z
- C8DB2.sh script error 331
Linux on System Z
- support for RACF namespace 173
load balancing
- configuring mail server settings 108
- enabling and disabling services 193
- setting 12
locales
- displaying supported content locales 225
- displaying supported product locales 223
- missing translations of object names 340
localhost
- requirement to change to host name or IP address 66
log database
- deleting tables 323
log destinations
- types of 215
log files 301
- gateway errors 303
- locale configuration 303
- run-time 303
- silent mode 304
- startup configuration 302
- transfer 302
- transfer summary 302
- uninstallation 303
log messages
- See also audit logs
- See also troubleshooting
- enabling for IBM Cognos Application Firewall 190
log database
- configuring 219
- database 218
- database client 216
- remote log servers 218
- using files 218
logging database
- creating using DB2 28
- creating using Informix Dynamic Server database 32
- creating using Microsoft SQL Server 31
- creating using Oracle 30
- creating using Sybase 33
- guidelines for creating 216
logging in
- configuring security 67, 109
- hiding namespaces during 157
logs
- message processing 215
- service 274

M
macro
- converting ppr reports to ppx reports 8
namespaces (continued)
    requirements for Content Manager if using Transformer with Series 7 namespace 53, 152
network access
    sharing data locations 234
network outage
    services fail to start 311
    NIST SP800-131a 204
    no response generated 318
    nomsgboxes option 268
    notification database
        configuring 203
        creating 202
        creating tables 62, 98
delleting tables 323
Novell Directory Server
    with an LDAP namespace 163

O
OLAP data sources 314
members missing or inaccessible 335
operating systems
    supported versions 21
Oracle
    creating connections strings 67, 103
    database drivers 65, 102
    database JDBC drivers 217
    deployment errors 336
    specifying as a log messages repository 219
Oracle application server 247
Oracle Directory Server
    with an LDAP namespace 165
Oracle Essbase
    query fails 335
Oracle Java SE Development Kit 222, 271
Oracle WebCenter Interaction Portal
    configuring 235
Oracle WebLogic 247
other components 9
OutOfMemoryError 313

P
p2pd.war file for WebLogic 320
page cache size
    Derby 276
page not found error
    starting IBM Cognos BI in Windows 2003 316
    passwords
        changing for Cognos Content Database 183
        changing in unattended configuration 281
paths
    setting for cookies 229
PDF fonts
    mapping to built-in PDF fonts for faster report printing 195
performance
    improving for Apache Tomcat on 64-bit 276
permissions
    for the user account that is used for the IBM Cognos service 66, 103, 116, 123, 179
portal
    configuring secure access for users 71, 109
delleting errors in starting 316, 318


N
namespace
    RACF 173
namespaces
    Active Directory Server missing group membership 335
    authentication 141
cannot log on 311
    configuring custom authentication providers 156
    configuring for a gateway 193
    deleting 177
    hiding during login 157
    IBM Cognos Series 7 71
    Kerberos authentication 243
    recreating 329
portal problems
unable to open 316
Portal Services 235
specifying the applications.xml file 236
ports
changing 184
default configuration settings 25
multiple versions of IBM Cognos BI 43
ports already in use 307
PowerCubes
access in IBM Cognos BI 17
cannot open 314
requirements for successful language conversion 17
PowerPlay Administration 339
PowerPlay Client component 8
PowerPlay Server 339
presentation service 274
Presentation service
requirements 272
printing reports
customizing for UNIX and Linux print servers 201
problem determination
exchanging information with IBM Support 299
processing log messages 215
product codes
in transfer specification files 270
product locales
displaying supported locales 223
mapping for user interface 227
product versions 58, 96, 115, 122
products
supported versions 21
properties
changing in unattended configuration 281
configuring for application server 256
temporary file location 192
protocol
IP address 230
purpose of document xi

Q
quality of protection in SSL connections 214
query databases 9
query service 274

R
RACF
authentication settings for IBM Cognos BI
administrators 173
connectivity 173
enabling single signon 174
RACF account properties
mapping to RACF namespace 173
RACF authentication provider configuration
changed feature in version 10.1.0 3
RACF namespace 173
recreating the Cognos namespace 329
relational data sources
members missing or inaccessible 335
release notes
reviewing before you install 21
remote log servers 218
configuring 219
removing components from multiple servers 270
report conversion
from ppr to ppx format 8
report data service 274
report distribution
on a network 277
report output
reusing 199
saving to a file system 197
sharing with users outside IBM Cognos BI 198
Report service
list of embedded fonts for PDF reports 197
requirements 272
report services 275
report specifications
upgrading 51
Report Studio
loading images 73, 125
reports
changing default font 196
customizing language support 225
decreasing delivery time 277
repository services 275
requirements
installation directory 314
Resource Access Control Facility
See also RACF 173
resources
adding 280
response.ats file 265, 266
reviewing the release notes before you install 21
root directory
for saving report output outside IBM Cognos BI 198
RSS feeds
troubleshooting 300

S
Safari 5
browser settings 34
SaferAPIGetTrustedSignon function
using for authentication 154
sAMAccountName
using Kerberos authentication 150
Sample Outdoors Company samples
installing 139
samples 7
data source connections 139
importing 140
installing 139
testing a report 140
SAP
enabling single signon 176
using for authentication 175
SAP BW
authorization settings for IBM Cognos BI
administrators 176
authorization settings for IBM Cognos BI users 175
connectivity 176
SAP Enterprise Portal
configuring 235
screen flicker 338
scripts
creating a content store in DB2 61, 98
to delete tables from databases 323
to improve metric store performance 277
secure flag
setting for cookies 229
secure LDAP communication 168
Secure Sockets Layer,
See SSL protocol
security
configuring secure access to the portal 71, 109
enabling 67, 109
issues with Integrated Windows Authentication 333
settings for Web browsers 22
security provider files
copying to application server JVM 181
Series 7 PowerCubes
requirements for successful language conversion 17
server components 5
installation sequence 89
server time zones
changing 228
servers
system metrics 271
service
graphics 273
human task 273
index data 273
index search 273
index update 273
service pack
installing 58, 96, 115, 122
services
adjusting to improve performance 272
agent 272
annotation 272
batch report 273
Content Manager 273
data integration 273
delivery 273
enabling and disabling 193
event management 273
fail to start after network outage 311
IBM Cognos BI 274
job 273
log 274
Metadata 274
Metrics Manager 274
Migration 274
migration service not working 339
monitor 274
presentation 272, 274
query 274
report 275
Report 272
report data 274
repository 275
setting the user account for shared network access 234
starting from the command line 284
stopping from the command line 284
system metrics 271
unable to start 307
uninstalling 289
servlet gateway
configuring 77, 130
SHA1 certificates 204
shared trust
setting up between IBM Cognos BI and other servers 212
SharePoint Portal
configuring 235
using Kerberos authentication 241
shortcut keys 291
silent installation
-startupfile path/filename.xml
new feature description for version 10.2 2
display status on screen 268
modifying a response file 267
option to bypass status messages 268
option to display status on screen 2
starting 268
startup file 2
silent installations 265
silent mode 265
silent uninstallation 270
Simplified Chinese
configuring fonts 194, 196
single signon
Active Directory namespace 148
issues with Integrated Windows Authentication 333
LDAP namespace 169
RACF namespace 174
SAP namespace 176
using IBM Cognos Series 7 namespace 153
using Kerberos authentication 241
Software Development Kit
documentation 3
software requirements
supported product versions 21
Solaris
environment variables to install IBM Cognos BI 55, 93,
112, 119
JRE 1.5 332
special characters
in LDAP namespace properties 157
SQL scripts
to delete databases 323
SSL
Active Directory Server 146
enabling for an application server 261
enabling on Web servers 214
LDAP namespace 168
quality of protection 214
setting up shared trust with other servers 212
using IBM Cognos Series 7 namespace 153
SSL protocol
configuring 210
standby Content Manager 12, 92
configuring 106
starting
the IBM Cognos service from IBM Cognos
Configuration 72
starting the Cognos service
from the command line 284
startup
collection lock file 302
DB2 returns SQ1TV1224N error when connecting from
AIX 312
download of resource fails 312
failure without error 308
IBM Cognos service 330
page not found 316
problems 304
script fails 319
unable to download cognos.xts 319
unable to open IBM Cognos Connection 316
unable to start service 307
startup options 293
startup scripts,
See application servers
Index 363

T

Tab key

problems in IBM Cognos Configuration 329

tables
deleting from a database 323
tablespace 275
content store scripts 62, 98
template
changing the size of template 275
temporary file location 192
configuring 192
Temporary files location
configuring for Windows Vista 232
testing
configuration 83
installation 83
testing the installation 111, 118, 135
Thai email encoding
JRE requirements 228
The Sample Outdoors Company 7
time zones
changing 228
Tomcat
64-bit installations 276
default configuration settings 25
transfer specification file
using to remove components 270
transfer specification files (.ats)
configuration 265
Transformer
data access in IBM Cognos BI 17
requirements for Content Manager if using Series 7
namespace 53, 152
uninstalling 290
troubleshooting 295
contacting IBM Support 298
Content Manager fails to start 313
exchanging information with IBM Support 299
fixes
getting 298
for a specific user 222
getting fixes 298
identifying problems 295
knowledge bases
searching for troubleshooting solutions 297
logging 215
troubleshooting (continued)
searching knowledge bases 297
subscribing to support 300
trust domain error
when saving the configuration 327
tuning
Apache Tomcat settings on 64-bit installations 276
DB2 content store 275

U

unable to open IBM Cognos Configuration 302
unattended configuration
changing properties 281
setting up 265
unattended installation
modifying a response file 267
setting up 265
starting 268
unattended mode 265
unattended uninstallation 270
uninstall command 270
uninstalling
Framework Manager 290
IBM Cognos BI 289, 290
Transformer 290
uninst command 270
UNIX
environment variables for IBM Cognos BI 55, 93, 112, 119
font not found error 334
log messages 218
starting and stopping the Cognos service 284
system requirements 53
UNIX AIX
support for RACF namespace 173
unregistering
dispatchers 48
unregistering dispatchers 262
unsupported characters 308
updater
installing 58, 96, 115, 122
updating
java environment 24, 181
upgrading 39
affect on Chinese, Japanese, or Korean characters 321
comparing reports from different versions 52
content store 47, 312
from other IBM Cognos products to IBM Cognos BI 14
IBM Cognos BI on an application server 263
missing translations of object names 340
moving content 46
process 39
report specifications 51
resources 41
tasks 43
viewing content from a previous version 43
upgrading a logging database on IBM DB2 on z/OS 48
URI
changing 184
default configuration settings 25
URI properties
requirement to change localhost to host name or IP
address 66
User account
requirements to run the IBM Cognos service 66, 103, 116, 123, 179
user credentials
  changing in unattended configuration 281
user interface
  customizing language support 223
mapping for product locale 227
user locale
  mapping to content locale 225
user logs
  configuring secure access to the portal 71, 109
User lookup property
  special characters for LDAP namespace 157
users
  changing for Cognos Content Database 183
UTF-8
  encoding for email messages 228

V
virtual directories
  IBM Cognos BI 73, 125
virtualization
  supported environments 21

W
WAR files, See Web archive files
web alias
  changed feature in version 10.1.0 3
Web aliases
  IBM Cognos BI 73, 125
Web archive files
  deploying IBM Cognos BI 285
Web browsers
  configuring 34
  errors in starting the Web portal 318
  errors when starting the web portal 316
  security settings 22
  using Kerberos authentication 241
Web Distributed Authoring and Versioning
  See WebDAV

Web servers
  configuring 73, 125
  enabling SSL 214
  servlet gateways 77, 130
  setting Report Studio load time 73, 125
  single signon using Active Directory and IIS Web server 148
WebDAV
  configuring to view images 81, 134
WebLogic
  application server 258, 260
  could not deserialize context attribute 320
  deploying p2pd.war file 320
  servlet class fails to load 337
  startup script 255
  startup script fails 319
WebLogic Application Server
  IBM Cognos BI fails 319
WebSphere 247
  application server 256
  WebSphere Application Server
    IBM Cognos BI deployment failure 320
    install Cognos BI 253
    problem connecting to IBM Cognos BI portal 328
    startup script fails 319
Windows
  installing IBM Cognos migration tool 84, 136
  system requirements 53
Windows authentication 148
Windows event log
  destination for log messages 218
Windows IIS
  recommended gateway settings 337
Windows Vista
  requirements for file locations 232

X
XQE-DS-0006 335