# Table of Contents

**Introduction** 13

**Part 1: IBM Cognos 8 PowerPlay**

**Chapter 1: What's New?** 15

- New Features in Version 10.1.0 15
  - Access to Software Development Kit Installation and Configuration Guide 15
- Changed Features in Version 10.1.0 15
  - Default Installation Location and Web Alias 15
  - PowerPlay Batch Administration 16
  - IBM Cognos Go! Dashboard is Merged with Features from IBM Cognos Viewer into One User Interface 16
  - Enhanced Support for Authentication Using a RACF Provider 16
  - Secure Access When Monitoring System Metrics Externally 16
- Removed Features in Version 10.1.0 16
  - Managing Memory for the IBM Cognos Service 16
- New Features in Version 8.4 17
  - Additional Language Support 17
  - Support for DB2 Universal Driver for Content Store, Notification, and Logging Databases 17
  - DB2 on z/OS as Content Store, Logging, or Notification Database 18
  - Support for IPv6 IP Addresses 18
  - Support for 64-bit Application Servers 18
  - Hide the Namespace from Users During Login 18
- Changed Features in Version 8.4 18
  - Installing Supplementary Languages Documentation Required for Translated Product Documentation 19
  - Default Connection to an IBM DB2 Content Store Replaces Microsoft SQL Server 19
  - IBM Java Runtime Environment (JRE) Replaces Sun Java Runtime Environment 19
- Deprecated Features in Version 8.4 19
  - Support for DB2 JDBC Type 2 Driver for the Content Store, Notification, and Logging Databases on Linux, UNIX and Windows (db2java.zip) 19
- Removed Features in Version 8.4 20
  - Text-based User Interface for Installing and Uninstalling on UNIX and Linux 20
  - Language Support for IBM Cognos 8 User Interface Text and Messages Moved from Supplementary Languages to IBM Cognos 8 Server Installation 20

**Chapter 2: Components Used by IBM Cognos PowerPlay** 21

- Server Components 21
  - Web communication - gateway 21
  - Application Tier Components 21
  - Managing Application Data - Content Manager 22
  - Optional Server Components 22
- Migration Components 23
- Client Components 24
Other Components 24

Part 2: Planning Your Installation

Chapter 3: Distribution Options for IBM Cognos PowerPlay 25

Distributing IBM Cognos PowerPlay Server Components 25
  All Components on One Computer 26
  Gateways on Separate Computers 26
  Application Tier Components and Content Managers on Separate Computers 27
  Installing IBM Cognos PowerPlay with Other IBM Cognos BI Components in a 64-bit System 29
  Accessing Product Documentation in an Integrated Environment 30
IBM Cognos PowerPlay with Other IBM Cognos Products 30
  IBM Cognos Series 7 Products That Can Be Migrated to IBM Cognos PowerPlay 30
  IBM Cognos Products That Interoperate with IBM Cognos PowerPlay 31
  IBM Cognos Series 7 Content That Can Be Recreated in IBM Cognos BI 34

Chapter 4: Preparing to Install 37

Review the Release Notes Before You Install 37
Review Supported Environments 37
Verify System Requirements 38
Review the Default Port Settings for IBM Cognos Business Intelligence 40
Guidelines for Creating the Content Store 41
  Suggested Settings for Creating the Content Store in DB2 on Linux, Windows and UNIX 42
  Suggested Settings for Creating the Content Store in DB2 on z/OS 45
  Suggested Settings for Creating the Content Store in Oracle 45
  Suggested Settings for Creating the Content Store in Microsoft SQL Server 46
  Suggested Settings for Creating the Content Store in the IBM Informix Dynamic Server Database 47
  Suggested Settings for Creating the Content Store in Sybase 48
Configure a User Account or Network Service Account for IBM Cognos Business Intelligence 49
Configure Web Browsers 49

Part 3: Installation and Configuration

Chapter 5: Upgrading to IBM Cognos PowerPlay 53

Planning the Upgrade 54
  Review the Documentation 55
  Recommendation - Assess Applications in the Source Environment 56
  Recommendation - Perform a Trial Upgrade 58
  Create the Test Environment 58
  Plan Your Deployment 59
  Create an Export Deployment Specification 61
  Copy the Deployment Specification to the Test Environment 63
  Include Configuration Objects in Import of Entire Content Store 63
  Import to the Test Environment 64
  Test the Deployed Content 65
  Recommendation - Test the Upgraded Content 65
  Moving to the Production Environment 66
Upgrading from an Earlier Version of IBM Cognos PowerPlay 67
  Upgrade IBM Cognos PowerPlay 69
Chapter 6: Installing and Configuring IBM Cognos PowerPlay on One Computer 79

Install IBM Cognos PowerPlay 80
Installing Fix Packs 84
Create a Database for a DB2 Content Store on Linux Using a Script 87
Create Tablespaces for a DB2 Content Store on z/OS 88
JDBC Driver Options for Using DB2 Database as a Content Store 90
Set Up Database Connectivity for the Content Store Database 91
Update the Java Environment 92
Configure IBM Cognos PowerPlay 93
  Configure Environment Properties in IBM Cognos Configuration 94
  Enable Security 94
  Set Database Connection Properties for the Content Store 95
  Specify a Connection to a Mail Server Account 98
  Configure an IBM Cognos Series 7 Namespace in IBM Cognos BI 99
Configure the Web Server 101
Start the IBM Cognos services 103
Test the Installation and Configuration 104
Installing and Configuring Migration on IBM Cognos Series 7 Computers 105
  Install IBM Cognos Series 7 Migration Components 105
  Configure the IBM Cognos Series 7 Migration Service for Migrations from Upfront in Distributed IBM Cognos Series 7 Installations 106
  Start the IBM Cognos Series 7 Migration Service 107
Uninstalling IBM Cognos BI 108
  Uninstall IBM Cognos Business Intelligence on UNIX or Linux 108
  Uninstall IBM Cognos Business Intelligence on Windows 109
  Uninstall Cognos Content Database 109
  Uninstall the Migration Components 111

Chapter 7: Installing and Configuring IBM Cognos PowerPlay Server Components on Different Computers 113

Installation Sequence for Server Components 115
Recommendation - Install and Configure the Basic Installation for Distributed Installations 115
Installing and Configuring Content Manager 116
  Active and Standby Content Manager Components 117
  Install the Content Manager Components 118
  Install Cognos Content Database on a Separate Server 122
  Installing Fix Packs 122
  Create a Database for a DB2 Content Store on Linux Using a Script 125
  Create Tablespaces for a DB2 Content Store on z/OS 126
  Update the Java Environment 128
  Set Up Database Connectivity for the Content Store Database 129
  Start IBM Cognos Configuration 130
  Set Database Connection Properties for the Content Store 131
  Configure Environment Properties for Content Manager Computers 135
  Specify a Connection to a Mail Server Account 137
Enable Security 138
Configure an IBM Cognos Series 7 Namespace in IBM Cognos BI 139
Start Content Manager 140
Test the Content Manager Installation 141
Installing and Configuring Application Tier Components 141
Install the Application Tier Components 142
Installing Fix Packs 145
Start IBM Cognos Configuration 148
Configure Environment Properties for Application Tier Components Computers 149
Start the Application Tier Components 150
Test the Application Tier Components 151
Test IBM Cognos BI Migration Service 151
Installing and Configuring the Gateway Component 152
Install the Gateway Components 152
Installing Fix Packs 155
Start IBM Cognos Configuration 158
Configure Environment and Security Properties for Gateway Computers 159
Configure the Web Server 160
Test the Gateway 163
Installing and Configuring Migration on IBM Cognos Series 7 Computers 163
Install IBM Cognos Series 7 Migration Components 163
Configure the IBM Cognos Series 7 Migration Service for Migrations from Upfront in Distributed IBM Cognos Series 7 Installations 165
Start the IBM Cognos Series 7 Migration Service 166
Uninstalling IBM Cognos BI 166
Uninstall IBM Cognos BI on UNIX or Linux 166
Uninstall IBM Cognos BI on Windows 167
Uninstall Cognos Content Database 168
Chapter 8: Install and Configure Optional Components 171
PowerPlay Samples 171
Install the IBM Cognos BI Samples 172
Setting Up the IBM Cognos PowerPlay Samples 173
Install Translated Product Documentation 177
Install and Configure Additional Language Fonts 178
Configure Support for Japanese Yen and Korean Won Characters 179
Part 4: Customizing IBM Cognos PowerPlay in Your Environment
Chapter 9: Configuring IBM Cognos Components to Use an Authentication Provider 181
Disable Anonymous Access 182
Restrict User Access to the Cognos Namespace 183
Configuring IBM Cognos Components to Use Active Directory Server 183
Configure an Active Directory Namespace 184
Make Custom User Properties for Active Directory Available to IBM Cognos Components 185
Enabling Secure Communication to the Active Directory Server 186
Include or Exclude Domains Using Advanced Properties 186
Enabling Single Signon Between Active Directory Server and IBM Cognos Components 187
Configuring IBM Cognos to Use IBM Cognos Series 7 Namespace 188
Configure an IBM Cognos Series 7 Namespace 189
Enabling Secure Communication to the Directory Server Used by the IBM Cognos Series 7 Namespace 190
Enabling Single Signon Between IBM Cognos Series 7 and IBM Cognos 190
IBM Cognos Series 7 Namespaces and the IBM Cognos Series 7 Trusted Signon Plug-in 191
Configuring IBM Cognos to Use a Custom Authentication Provider 193
Configure a Custom Authentication Namespace 194
Hide the Namespace from Users During Login 194
Configuring IBM Cognos Components to Use LDAP 195
LDAP Mapping 195
Configure an LDAP Namespace 196
Configure an LDAP Namespace for Active Directory Server 197
Configure an LDAP Namespace for IBM Directory Server 200
Configure an LDAP Namespace for Novell Directory Server 202
Configure an LDAP Namespace for Sun Java System Directory Server 204
Make Custom User Properties for LDAP Available to IBM Cognos Components 206
Enable Secure Communication to the LDAP Server 207
Enabling Single Signon Between LDAP and IBM Cognos Components 209
Replace Operation 209
Configuring IBM Cognos Components to Use eTrust SiteMinder 210
Configure a Netegrity SiteMinder Namespace 211
Enabling Secure Communication to the eTrust SiteMinder User Directory 212
Enable Single Signon Between eTrust SiteMinder and IBM Cognos 212
Protecting the IBM Cognos Web Alias 213
Hide the Namespace from Users During Login 213
Configuring IBM Cognos Components to Use an NTLM Namespace 213
Configure an NTLM Namespace 214
Enable Single Signon Between NTLM and IBM Cognos Components 214
Configuring IBM Cognos to Use a RACF Provider for Authentication 215
Configuring a RACF Namespace 215
Enabling Single Signon Between RACF and IBM Cognos 216
Delete an Authentication Provider 217

Chapter 10: Configuration Options 219
Start IBM Cognos Configuration 220
Changing Default Configuration Settings 220
Change Default User and Password for Cognos Content Database 221
Change a Port or URI Setting 223
Configuring Cryptographic Settings 225
Configure IBM Cognos Components to Use IBM Cognos Application Firewall 230
Encrypt Temporary File Properties 231
Configure the Gateway to Use a Namespace 232
Enable and Disable Services 232
Configuring Fonts 233
Considerations to Support Simplified Chinese 235
Update the Registry Entries for Windows Font Links 236
Change the Default Font for PDF Reports 236
Configure Embedded Fonts for PDF Reports 237
Saved Report Output 238
Table of Contents

Changing the Location of Temporary Report Output 239
Change the Notification Database 240
  Suggested Settings for Creating a DB2 Notification Database on z/OS 240
  Create Tablespaces for the DB2 Notification Database on z/OS 241
  Change the Connection Properties for the Notification Database 242
Create a New Content Store Using Cognos Content Database 242
Configuring the SSL Protocol 243
  Configure SSL for IBM Cognos Components 243
  Set Up Shared Trust Between IBM Cognos Servers and Other Servers 246
  Select and Rank Cipher Suites for SSL 247
  Enable SSL on the Web Server 248
Configuring a Repository for Log Messages 249
  Guidelines for Creating a Logging Database 250
  Create Tablespaces for DB2 Logging Database on z/OS 250
  Set Up the Database Connectivity for the Logging Database 252
  Log Message Repositories 254
  Specify the Log Messages Repository 255
  Enabling User-specific Logging 260
Changing Global Settings 261
  Customize Language Support to the User Interface 262
  Customizing Currency Support 263
  Customize Content Locale Support 263
  Map Content Locales 264
  Map Product Locales 266
  Customize the Server Time Zone 267
  Change Encoding for Email Messages 267
  Customize Cookie Settings 269
Changing the Gateway 270
  Configure the Gateway for IBM Cognos Apache Web Server Module 271
  Configure the Servlet Gateway 276
Change the IP Address Version 277
Configure the Router to Test Dispatcher Availability 279
Update File Location Properties on Windows Vista 279
Change Configuration Settings for the IBM Cognos Series 7 Migration Service 280
Assign a User Account to the PowerPlay and Migration Services for Migration 281

Chapter 11: Configuring Portal Services 283
  Specify the Location of the Applications.xml File 283
Configuring Security for Portal Services 284
  Disable Anonymous Access to IBM Cognos Components 284
  Enable Single Signon Using Shared Secret 285
  Enable Single Signon for WebSphere Portal Using the Application Server 289
  Enable Single Signon for Oracle WebCenter Interaction Portal Using Basic Authentication 289
  Enable Single Signon for Oracle WebCenter Interaction Portal Using SiteMinder 290

Chapter 12: Configuring IBM Cognos BI for an Application Server other than Tomcat 291
  Create a Separate JVM Instance 292
  Create Additional Profiles to Distribute IBM Cognos BI Components for Linux on System z 293
  Check the Setup of IBM Cognos Components 293
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back Up Existing IBM Cognos Information</td>
<td>294</td>
</tr>
<tr>
<td>Set Environment Variables</td>
<td>296</td>
</tr>
<tr>
<td>Adjust the Default Connection Time-out for IBM Cognos BI</td>
<td>297</td>
</tr>
<tr>
<td>Configure IBM Cognos Components to Run Within the Application Server</td>
<td>297</td>
</tr>
<tr>
<td>Identifying the JDK for WebLogic 9 on AIX</td>
<td>299</td>
</tr>
<tr>
<td>Change the Application Server Startup Script</td>
<td>300</td>
</tr>
<tr>
<td>Configure Application Server Properties and Deploy IBM Cognos Components</td>
<td>302</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>307</td>
</tr>
<tr>
<td>Configuring Web Communication</td>
<td>308</td>
</tr>
<tr>
<td>Configure the Web Server</td>
<td>308</td>
</tr>
<tr>
<td>Configure a Virtual Directory for SAP NetWeaver on Windows</td>
<td>310</td>
</tr>
<tr>
<td>Unregister Dispatchers</td>
<td>311</td>
</tr>
<tr>
<td>Import Content Store Data</td>
<td>311</td>
</tr>
<tr>
<td>Upgrade to IBM Cognos BI in an Application Server Environment</td>
<td>312</td>
</tr>
</tbody>
</table>

Chapter 13: Advanced Configuration Options 313

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changing the Version of Java Runtime Environment Used by IBM Cognos BI Components</td>
<td>313</td>
</tr>
<tr>
<td>Back Up Existing IBM Cognos Information</td>
<td>313</td>
</tr>
<tr>
<td>Update the Java Environment</td>
<td>315</td>
</tr>
<tr>
<td>Import Content Store Data</td>
<td>316</td>
</tr>
<tr>
<td>Configuring IBM Cognos BI Components to Use a Another Certificate Authority</td>
<td>316</td>
</tr>
<tr>
<td>Generate Keys and Certificate Signing Requests</td>
<td>317</td>
</tr>
<tr>
<td>Configure IBM Cognos BI Components to Run Within Another Certificate Authority</td>
<td>320</td>
</tr>
</tbody>
</table>

Chapter 14: Setting Up an Unattended Installation and Configuration 323

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Up an Unattended Installation</td>
<td>323</td>
</tr>
<tr>
<td>Set Up an Unattended Configuration</td>
<td>326</td>
</tr>
<tr>
<td>Set Up an Unattended Uninstallation</td>
<td>327</td>
</tr>
</tbody>
</table>

Part 5: Maintenance

Chapter 15: Performance Maintenance 329

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Performance Metrics</td>
<td>329</td>
</tr>
<tr>
<td>Monitoring System Metrics Externally</td>
<td>329</td>
</tr>
<tr>
<td>Enabling Only Services That are Required</td>
<td>330</td>
</tr>
<tr>
<td>Tuning a DB2 Content Store</td>
<td>333</td>
</tr>
<tr>
<td>Adjusting the Memory Resources for the IBM Cognos Service</td>
<td>334</td>
</tr>
<tr>
<td>Tune Apache Tomcat Settings</td>
<td>334</td>
</tr>
<tr>
<td>Increase the Request-handling Capacity for Cognos Content Database</td>
<td>335</td>
</tr>
<tr>
<td>Improve Metric Store Database Performance</td>
<td>335</td>
</tr>
<tr>
<td>Reduce Delivery Time for Reports in a Network</td>
<td>336</td>
</tr>
<tr>
<td>Increase Asynchronous Timeout in High User Load Environments</td>
<td>336</td>
</tr>
</tbody>
</table>

Part 6: Appendices

Appendix A: Manually Configuring IBM Cognos BI 339

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually Configuring IBM Cognos BI on UNIX and Linux</td>
<td>339</td>
</tr>
<tr>
<td>Manually Change Default Configuration Settings on UNIX and Linux Computers</td>
<td>340</td>
</tr>
<tr>
<td>Manually Change the Global Settings on UNIX and Linux Computers</td>
<td>343</td>
</tr>
<tr>
<td>Starting and Stopping IBM Cognos BI in Silent Mode on UNIX and Linux Computers</td>
<td>344</td>
</tr>
<tr>
<td>Manually Create an IBM Cognos Application File</td>
<td>345</td>
</tr>
</tbody>
</table>
Appendix B: Troubleshooting 349

Log Files 349

Problems Starting IBM Cognos Business Intelligence 351

CFG-ERR-0106 Error When Starting the IBM Cognos service in IBM Cognos Configuration 352

Cryptographic Error When Starting IBM Cognos BI 353

Unable to Start the IBM Cognos service Because the Port is Used by Another Process 354

IBM Cognos service Does Not Start or Fails After Starting 354

IBM Cognos BI Server Fails to Start and Gives No Error Message 355

IBM Cognos BI Server Not Available When Starting IBM Cognos BI 355

Cannot Log On to a Namespace When Using IBM Cognos Connection 359

IBM Cognos services Fail to Restart After a Network Outage 359

No Warning That Installing a Later Version of IBM Cognos BI Will Automatically Update the Earlier Version of the Content Store 360

Download of Resource Fails 360

DB2 Returns SQL1224N Error When Connecting from AIX 360

Content Manager Error When Starting IBM Cognos BI 360

Content Manager Fails to Start or Takes a Long Time to Start 361

DPR-ERR-2014 Error Displays in Log File on Content Manager Computer 362

Non-ASCII Characters in Installation Directory Cause Run-time Errors 362

Cannot Open an MS Cube or PowerCube 362

The Page Cannot Be Found When Starting IBM Cognos BI in Windows 2003 363

The Page Is Not Shown When Opening a Portal After Installing IBM Cognos BI 363

DPR-ERR-2058 Error Displays in Web Browser When Starting IBM Cognos BI 363

DPR-ERR-2022 Error Displays in Web Browser When Starting IBM Cognos BI 365

Corrupt Characters While Installing in Some Languages on Linux 366

Unable to Download the cognos.xts File 366

Application Server Startup Script Fails 367

IBM Cognos BI Running under WebLogic Application Server on AIX Fails 367

Deploying IBM Cognos BI to an Oracle Application Server or IBM WebSphere Application Server Fails 367

Unable to Deserialize Context Attribute Error When Deploying the p2pd.war File to WebLogic 368

Error Displays After Upgrading IBM Cognos BI on a WebLogic Application Server 368

Chinese, Japanese, or Korean Characters Are Different After Upgrade 368

Accented or Double-Byte Characters May Not Display Correctly When Installing IBM Cognos BI on Linux 369

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 369

Problems Configuring IBM Cognos Business Intelligence 369

Configuration Tool cogconfig.sh Return Values Are Not Compliant with Conventional UNIX Return Values 369

Run Database and Index Cleanup Scripts 370

Error Trying to Encrypt Information When Saving Your Configuration 373

Problems Generating Cryptographic Keys in IBM Cognos Configuration 374

CAM-CRP-1315 Error When Saving Configuration 374

CAM-CRP-0221 Error When Logging Into the Portal 374

Manually Changing the Installation Directory Name Affects Installations Running Under an Application Server 375
Configuration Data is Locked by Another Instance of IBM Cognos Configuration 376
Unable to Exit a Tab Sequence When Using Keyboard-only Navigation in IBM Cognos Configuration 376
Unable to Save Your Configuration 376
Java Error When Starting IBM Cognos Configuration 377
Cryptographic Error When Starting IBM Cognos Configuration 377
Current Configuration Settings Are Not Applied to Your Computer 377
CM-CFG-029 Error When Trying to Save a Configuration That Specifies a Microsoft SQL Server Content Store 378
DB2 Not Found Error for Linux on System z 378
DPR-ERR-2079 When Content Manager Configured For Failover 378
Importing a Large Content Store in Solaris using JRE 1.5 Fails 379
Importing a Large Deployment in Windows Crashes the Java Virtual Machine 379
Users are Prompted for Active Directory Credentials 379
Font on UNIX Not Found When Starting IBM Cognos Configuration 380
ESSBASEPATH Cannot Be Detected 380
Query Fails When Using Oracle Essbase Server 381
Group Membership is Missing From Active Directory Namespace 381
Errors Displayed Deploying to Oracle 10G Application Server 382
CGI Timeout Error While Connected to IBM Cognos BI Components Through a Web Browser 383
Servlet Class Fails to Load in WebLogic 383
Desktop Icons or IBM Cognos Configuration Window Flicker on Windows 384
Migration Does Not Work 384

Appendix C: Keyboard Shortcuts for the Installation Wizard 387

Glossary 389

Index 393
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 PowerPlay Migration and Administration Guide.

Audience
To use this guide, you should be familiar with

- IBM Cognos Series 7 PowerPlay
- installing software on Microsoft® Windows® and UNIX® computers
- 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 at http://publib.boulder.ibm.com/infocenter/cogic/v1r0m0/index.jsp. Updates to Release Notes are published directly to Information Centers.

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

Using quick tours
Quick tours are short online tutorials that illustrate key features in IBM Cognos product components. To view a quick tour, start IBM Cognos Connection and click the Quick Tour link in the lower-right corner of the Welcome page. Quick Tours are also available in IBM Cognos Information Centers.

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" (p. 387).

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 Great Outdoors Company, GO Sales, any variation of the Great Outdoors name, 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.

For changes to previous versions, see:

- New Features in Version 8.4
- Changed Features in Version 8.4
- Deprecated Features in Version 8.4
- Removed Features in Version 8.4

To review an up-to-date list of environments supported by IBM® Cognos® Business Intelligence products, such as operating systems, patches, browsers, web servers, directory servers, database servers, and application servers, visit the IBM Cognos Customer Center (http://www.ibm.com/software/data/support/cognos_crc.html).

New Features in Version 10.1.0

Listed below 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, at http://publib.boulder.ibm.com/infocenter/chi/v10r1m0/.

Changed Features in Version 10.1.0

Listed below 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® BI 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 BI server, Version 10.1.0, you can configure a RACF namespace directly in IBM Cognos Configuration on UNIX® AIX® or on Linux® for System Z operating systems. For more information, see "Configuring IBM Cognos to Use a RACF Provider for Authentication" (p. 215).

**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 BI 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. For more information, see "Monitoring System Metrics Externally" (p. 329).

**Removed Features in Version 10.1.0**

Listed below 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 value for the Maximum memory in MB property 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 value for the Maximum memory in MB property. For more information, see "Adjusting the Memory Resources for the IBM Cognos Service" (p. 334)

New Features in Version 8.4

Listed below are new features introduced in the previous release. Links to directly-related topics are included.

Additional Language Support

In addition to Japanese, German, and French, the installation documentation and the user interface for the installation program and IBM® Cognos® Configuration are available in the following languages:

- Chinese (simplified)
- Chinese (traditional)
- Korean
- Italian
- Spanish
- Portuguese (Brazilian)

During the installation you can select the language to use from the first page of the installation wizard. This determines the language of the user interfaces of the installation wizard and IBM Cognos Configuration.

However, you must configure IBM Cognos 8 to use the additional languages. For more information, see "Customize Language Support to the User Interface" (p. 262).

Support for DB2 Universal Driver for Content Store, Notification, and Logging Databases

DB2 introduced a universal JDBC driver that contains both type 2 and type 4 JDBC driver support. IBM Cognos 8 can connect to a DB2 content store, notification database, or logging database using either type of JDBC connectivity, but you must first copy two JAR files to the IBM Cognos 8 installation directory. If you are upgrading, you can continue to use type 2 JDBC connectivity without changing the connection properties for the DB2 content store.

For more information about connection properties for the content store, see "Set Database Connection Properties for the Content Store" (p. 95).

The two JAR files that you must copy to your IBM Cognos 8 installation directory are as follows:

- a license file, for example db2jcc_license_cisuz.jar or db2jcc_license_cu.jar
- a driver file, db2jcc.jar
For information about copying these files, see "Set Up Database Connectivity for the Content Store Database" (p. 91).

**DB2 on z/OS as Content Store, Logging, or Notification Database**

You can use DB2 on z/OS as your content store, logging, or notification database. Connection settings to DB2 on z/OS are similar to those for DB2 on Linux®, UNIX®, and Microsoft® Windows®. However, additional advanced settings must be configured.

For information about the configuration settings, see "Suggested Settings for Creating the Content Store in DB2 on z/OS" (p. 45), "Suggested Settings for Creating a DB2 Notification Database on z/OS" (p. 240), and "Suggested Settings for Creating the DB2 Logging Database on z/OS" (p. 250).

You must run scripts to create tablespaces for storing Large Objects (LOBs). For more information, see "Create Tablespaces for a DB2 Content Store on z/OS" (p. 88), "Create Tablespaces for DB2 Logging Database on z/OS" (p. 250), and "Create Tablespaces for the DB2 Notification Database on z/OS" (p. 241).

**Support for IPv6 IP Addresses**


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 Microsoft® Windows®, you can set the option permanently by adding the option to the Start menu shortcut.

For more information, see "Change the IP Address Version" (p. 277).

**Support for 64-bit Application Servers**

IBM Cognos 8 Business Intelligence products are now available with support for 64-bit application servers.

For information about supported application servers, visit the IBM Cognos Customer Center (http://www.ibm.com/software/data/support/cognos_crc.html).

For information about configuration, see the IBM Cognos 8 Installation and Configuration Guide.

**Hide the Namespace from Users During Login**

You can now hide namespaces from users during login. This lets you have trusted signon namespaces without showing them on the namespace selection list that is presented when users log in. For more information, see "Hide the Namespace from Users During Login" (p. 194).

**Changed Features in Version 8.4**

Listed below are changes to features introduced in the previous release. Links to directly-related topics are included.
Installing Supplementary Languages Documentation Required for Translated Product Documentation

You must install the Supplementary Languages Documentation to access product documentation in languages other than English. For more information, see "Install Translated Product Documentation" (p. 177).

By default, when you install the IBM® Cognos® 8 gateway component, the installation documentation, which includes the Installation and Configuration Guide, the Quick Start Installation and Configuration Guide and the Release Notes, is installed in all supported languages. The product documentation, such as the Administration and Security Guide, is installed in English.

Default Connection to an IBM DB2 Content Store Replaces Microsoft SQL Server

When you start IBM® Cognos® Configuration for the first time, the connection to IBM DB2 replaces Microsoft® SQL Server for the default content store.

If you did not install IBM Cognos Content Database, and want to use another database server for the content store, you must delete the default content store. After you uninstall, if you install into the same location as a previous release, your configuration is preserved and the existing content store is used.

For more information, see "Set Database Connection Properties for the Content Store" (p. 95).

IBM Java Runtime Environment (JRE) Replaces Sun Java Runtime Environment

IBM Cognos 8 now contains the IBM version of the JRE as part of Microsoft® Windows® installations. This replaces the Sun JRE for 32-bit Windows platforms.

The installation location remains the same. Any content encrypted with Sun JRE can be decrypted with the IBM JRE.

Deprecated Features in Version 8.4

A deprecated feature is one that is being replaced by a newer version or a better implementation. The intention is to discontinue the use of the feature and provide recommendations for adapting to this change over multiple releases.

Listed below are deprecated features from the previous release, including links to related topics.

Support for DB2 JDBC Type 2 Driver for the Content Store, Notification, and Logging Databases on Linux, UNIX and Windows (db2java.zip)

DB2 introduced a universal JDBC driver that contains both type 2 and type 4 JDBC driver support. This new universal driver replaces the deprecated type 2 driver, db2java.zip.

You can continue to use type 2 connectivity with no configuration changes required. If you choose to use type 4 connectivity, a configuration change is required.

For more information, see "Set Database Connection Properties for the Content Store" (p. 95).
Removed Features in Version 8.4

Listed below are features that were removed in the previous release. Links to directly-related topics are included.

Text-based User Interface for Installing and Uninstalling on UNIX and Linux

In earlier versions of IBM® Cognos® 8 BI products, you could run a text-based, or console-mode, installation or uninstallation program on systems that did not have XWindows. In the current release, the text-based installation and uninstallation programs are not available. Users who install on UNIX® and Linux® without XWindows must run an unattended installation or uninstallation (p. 323).

Language Support for IBM Cognos 8 User Interface Text and Messages Moved from Supplementary Languages to IBM Cognos 8 Server Installation

IBM Cognos 8 comes with a set of user interface text and messages in several more languages than in the previous release. You are no longer required to install supplementary languages from a separate installation program to show the user interface in one of the supported languages. The required files are automatically installed when you install the IBM Cognos 8 server.

However, you must use Supplementary Languages Documentation to install the Andale WT fonts for Japan and Korea. These fonts map the U+005C value as a yen or won character. For more information, see "Install and Configure Additional Language Fonts" (p. 178).
Chapter 2: Components Used by IBM Cognos PowerPlay

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

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 PowerPlay uses Tomcat as an application server. You can configure IBM Cognos Business Intelligence products to run on supported application servers that you currently use in your environment.

Server Components

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

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

Some server components are provided with all IBM® Cognos® Business Intelligence products. Common server components include the following tools:

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 BI, 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 URLs 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 and IBM Cognos PowerPlay®. It provides easy access to the overall management of the IBM Cognos BI 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
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.

Facilitating decision-making - IBM Cognos Business Insight
In IBM Cognos Business Insight, you can create sophisticated interactive dashboards 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 dashboards and reports, manipulate the content in the dashboards, and email your dashboards. You can also use comments and activities for collaborative decision making.

Managing Application Data - Content Manager
Content Manager is the IBM® Cognos® BI 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 it in the same location as Content Manager, Cognos Content Database is configured as the default content store for IBM Cognos Business Intelligence.

Use Cognos Content Database in a test or proof-of-concept environment only.

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, Great Outdoors. 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. They are also used to migrate PowerPlay® Studio reports to Analysis Studio and Report Studio.

For more information about the migration components, see the 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.

Migration to Analysis Studio and Report Studio
Analysis Studio and Report Studio are server components that are available in IBM Cognos BI. Users can open PowerPlay reports and migrate them to Analysis Studio or Report Studio by using the Open with Analysis Studio or Open with Report Studio functionality. This functionality, which the PowerPlay administrator can disable, uses the IBM Cognos BI migration service to migrate the reports.
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.

Other Components

In addition to the tools provided with IBM® Cognos® PowerPlay®, other components are required.

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 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
PowerPlay supports PowerCube data sources. Other IBM Cognos Business Intelligence components support other types of data sources. For more information, see the IBM Cognos BI Administration and Security Guide.
Chapter 3: Distribution Options for IBM Cognos PowerPlay

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 requirements, resources, and preferences. Configuration requirements differ depending on whether you install all components on one computer or more than one computer.

PowerPlay is compatible with other IBM Cognos Business Intelligence products of the same version. If your environment includes other IBM Cognos products, you must consider how 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 PowerPlay Migration and Administration Guide.

Distributing IBM Cognos PowerPlay Server Components

When you install IBM® Cognos® PowerPlay® server components, you specify where to place the gateway, 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 Business Intelligence 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 IBM Cognos Content Database, you can install it on the same computer as Content Manager or on another computer. If you install it on the same computer and in the same location, IBM Cognos Content Database is automatically configured for use as your content store. If you install it on another computer, ensure that you set the connection properties for IBM Cognos Content Database on your Content Manager computer.

- Install IBM Cognos PowerPlay server components on the same computer as other IBM Cognos BI products of the same version.
IBM Cognos BI products are designed to share components, including the gateway, Content Manager, content store, IBM Cognos Connection, and IBM Cognos Configuration. If you install more than one IBM Cognos BI product on the same computer, install them in the same installation location. The installation program checks to determine whether other IBM Cognos BI components exist in the installation location. If a component exists and can be shared, it is not reinstalled.

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 can choose to 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 modeling components in separate locations. For more information about installing Framework Manager or Transformer, see the IBM Cognos BI Installation and Configuration Guide.

**All Components on One Computer**

You can install all the IBM® Cognos® PowerPlay® 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 Windows-based PowerPlay Client on a separate computer that runs on Microsoft® Windows®.

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

**Configuration Requirements**

If you install all server components for PowerPlay on the same computer, you must then

- configure your web server to view IBM Cognos content
- specify connection information to the content store
- specify a mail server and 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 IBM Cognos BI 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 web servers with gateways and Application Tier Components](image)

**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 view 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.

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 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 PowerPlay components you must

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

**More Than One Content Manager**

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

Content Manager stores data that IBM Cognos Business Intelligence 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 BI 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 the application 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.

In the following diagram, a request directed to the default Content Manager fails. The request is redirected to the standby Content Manager computer, which became active when the default Content Manager computer failed.

![Diagram showing distribution options for IBM Cognos PowerPlay](image_url)
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
- specify the Dispatcher URI for external applications
- set up a connection to an email account for notifications (if you want to email reports)

Installing IBM Cognos PowerPlay with Other IBM Cognos BI Components in a 64-bit System

Some IBM® Cognos® Business Intelligence components are available for 64-bit operating systems. 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. 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. For 32-bit installations, the default installation directory is C:\Program Files\IBM\Cognos\c10 (Microsoft® Windows® operating systems) or /usr/IBM/cognos/c10 (UNIX® and Linux® operating systems). For 64-bit installations, the default installation directory is C:\Program Files\IBM\Cognos\c10_64 (Windows) or /usr/IBM/cognos/c10_64 (UNIX or Linux).

Server Components That Must Be Installed in the 64-bit 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)
  
  If using a web server that cannot load a 32-bit compiled library in a 64-bit compiled server, such as Apache Web Server, install the 32-bit version of the Gateway component on a 32-bit web server.

- 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)

Server Components That Must Be Installed in the 32-bit Directory
The following components can be installed together on the 64-bit server, but in a separate directory from the 64-bit components. They can also be installed on a separate 32-bit system:
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 can 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 will be 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 you 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 migration 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 PowerPlay Migration and Administration Guide.

**IBM 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 install the 32-bit IBM Cognos BI server. You must also ensure that both products are the same version.

For more information, see the Analyst User Guide.
IBM 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 install the 32-bit IBM Cognos BI server. You must also ensure that both products are the same version.

For more information, see the Contributor Administration Guide.

IBM 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.

IBM 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 install the 32-bit IBM Cognos BI server. You must also ensure that both products are the same version.

IBM 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 (p. 188) 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 BI 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.

**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.

**IBM Cognos Mobile**

With IBM Cognos Mobile you can access reports authored with Analysis Studio, Report Studio, and Query Studio on a mobile device (such as a BlackBerry). To download, view, and interact with reports, IBM Cognos Mobile requires the installation of a rich client on the mobile device, 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.

**IBM Cognos Series 7 Content That Can Be Recreated in IBM Cognos BI**

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

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

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

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

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

**IBM Cognos Portal Services**
You can duplicate most IBM Cognos Portal Services functionality using IBM Cognos Connection.
Chapter 4: 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 and configure web browsers. You can also create a user or service 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. 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 the supported environments.
- Ensure that your computer meets the software and hardware requirements.
- Review the default port settings.
- Create the database for the content store.
- Configure a user or network service account for IBM Cognos BI, if required.
- Configure web browsers.

After you complete these tasks, continue with "Installing and Configuring IBM Cognos PowerPlay on One Computer" (p. 79) or "Installing and Configuring IBM Cognos PowerPlay Server Components on Different Computers" (p. 113).

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 disk. Release Notes updates are also available on the IBM Cognos Customer Center (www.ibm.com/software/data/cognos/customercenter/).

Review Supported Environments

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.
To review an up-to-date list of environments supported by IBM Cognos products, such as operating systems, patches, browsers, Web servers, directory servers, database servers, and application servers, visit the IBM Cognos Customer Center (www.ibm.com/software/data/cognos/customercenter/).

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.

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.

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 under Linux.</td>
</tr>
<tr>
<td>RAM</td>
<td>Minimum: 2 GB</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 2.5 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>
<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

<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.</td>
</tr>
<tr>
<td></td>
<td>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>
<tr>
<td>Database</td>
<td>Cognos Content Database can be installed and configured as the default content store database in a test or proof-of-concept system.</td>
</tr>
<tr>
<td></td>
<td>You must have one of the following databases available to store IBM Cognos data in a production environment:</td>
</tr>
<tr>
<td></td>
<td>● Oracle</td>
</tr>
<tr>
<td></td>
<td>● DB2®</td>
</tr>
<tr>
<td></td>
<td>● Microsoft® SQL Server</td>
</tr>
<tr>
<td></td>
<td>● Sybase</td>
</tr>
<tr>
<td></td>
<td>● Informix</td>
</tr>
<tr>
<td></td>
<td>TCP/IP connectivity is required for all database types.</td>
</tr>
<tr>
<td>Web browser</td>
<td>For all Web browsers, the following must be enabled:</td>
</tr>
<tr>
<td></td>
<td>● cookies</td>
</tr>
<tr>
<td></td>
<td>● JavaScript</td>
</tr>
<tr>
<td></td>
<td>For Microsoft Internet Explorer only, the following must be enabled:</td>
</tr>
<tr>
<td></td>
<td>● Run ActiveX controls and plug-ins</td>
</tr>
<tr>
<td></td>
<td>● Script ActiveX controls marked safe for scripting</td>
</tr>
<tr>
<td></td>
<td>● Active scripting</td>
</tr>
<tr>
<td></td>
<td>● Allow META REFRESH</td>
</tr>
<tr>
<td>Other</td>
<td>On Windows, Microsoft Data Access Component (MDAC) for use with product samples</td>
</tr>
</tbody>
</table>
**Review the Default Port Settings for IBM Cognos Business Intelligence**

The following table lists the default ports and URI 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 in the `c10_location/configuration` directory.

### Default Port Settings for IBM Cognos BI Components

<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>
<tr>
<td>Dispatcher URI (Internal, 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>Dispatcher URI for external applications</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>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 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>

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.

### 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 Connector</td>
<td>9300</td>
<td>The port Tomcat uses to pass requests from the Web server to IBM Cognos BI</td>
</tr>
</tbody>
</table>
The port Tomcat uses to listen for secure connections
SSL Coyote HTTP/1.1 connector 9334

The port Tomcat uses to listen for a shutdown command
Shutdown port 9399

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

### 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 Number</td>
<td>21567</td>
<td>The port used for communications between IBM Cognos Series 7 migration 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.

### Database Properties

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

### Character Encoding and Protocol Used by Database s

<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>
</tbody>
</table>
If you plan to use the Cognos Content Database as your content store, a database is created and pre configured when the installation is complete.

**Collation Sequence**

Note that 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 database documentation.

### Suggested Settings for Creating the Content Store in DB2 on Linux, Windows and UNIX

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 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 of library files are needed must be listed first.

### Guidelines for Creating the Content Store in DB2 on Linux, UNIX, or Windows

If you create your own content store, use the following checklist to help you set up the content store on DB2.

- If you use type 2 JDBC connectivity, set the appropriate environment variables for DB2, which are as shown in the following table.
### Environment variable Description

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2DIR</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. For example (replace ## with 32 or 64 as appropriate), LD_LIBRARY_PATH= $DB2_location/sqllib/lib##: $LD_LIBRARY_PATH Examples (replace ## with 32 or 64 as appropriate): For Solaris and Linux: LD_LIBRARY_PATH= $DB2DIR/lib##: $LD_LIBRARY_PATH For AIX®: LIBPATH=$DB2DIR/lib##:$LIBPATH For HP-UX: SHLIB_PATH=$DB2DIR/lib##:$SHLIB_PATH</td>
</tr>
<tr>
<td>DB2INSTANCE</td>
<td>The default database server connection.</td>
</tr>
<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 if your database has the correct code set, using the command line interface, type the following at the command prompt:

```bash
db2 get database configuration for database_name
```

The code set value should be UTF-8 and the code page value should be 1208.

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application heap size (applheapsz)</td>
<td>1024 KB If the application heap size value is too small, out of memory errors may occur when there are many users.</td>
</tr>
</tbody>
</table>
SettingProperty

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<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 (DB2_INLIST_TO_NLJN)</td>
<td>YES</td>
</tr>
<tr>
<td></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 4 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 4 KB buffer pool you created. Global temporary tables will be created in the user temporary tablespace.
- Create a regular user tablespace using the 4 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 will 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 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 sqlib/db2profile from the DB2 user’s home directory. For example, the content of your .profile will be similar to the following:

```bash
if [ -f /home/db2user/sqlib/db2profile ]; then
  ./home/db2user/sqlib/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.

Guidelines for Creating the Content Store in DB2 on z/OS

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 administrator privileges in DB2 (DBADM authority) in z/OS.

- Create a database instance, storage group, and a user account for the content store.
  A user must have permissions to create and delete tables in the database.
  IBM® Cognos® Business Intelligence uses the credentials of the user account to communicate with the database server.

- Ensure 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 tablespaces to hold Large Objects and other data for the content store and grant user rights to the tablespaces. For information about running the script, see "Create Tablespaces for a DB2 Content Store on z/OS" (p. 88).

- 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 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.

Guidelines for Creating the Content Store in Oracle

Use the following checklist 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:

  ```sql
  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 will be used 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.

**Suggested Settings for Microsoft SQL Server**

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 the IBM Informix Dynamic Server Database

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.

### Suggested Settings for the Informix Dynamic Server Database

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 two sbspaces named CMDATASPACE and CMOBJPROPS7SPACE, with the logging turned on.

❑ 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.

Suggested Settings for Sybase

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 ibmcognos. This group must contain the user that owns the IBM Cognos files. Change the group ownership of the IBM Cognos files to the ibmcognos 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 topic about configuring the Web server.

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 topic about configuring the Web server. 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.

The following table shows the settings that must be enabled.
Browser Settings Required 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>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>
</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 "Configure IBM Cognos Components to Use IBM Cognos Application Firewall" (p. 230)

For more information, see the topic about configuring IBM Cognos Application Firewall in the Installation and Configuration Guide.

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

Cookies Used by IBM Cognos BI Components

<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><strong>Cookie</strong></td>
<td><strong>Type</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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</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 &quot;view members folder&quot; 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>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>Footer</td>
<td></td>
<td>These cookies store the preferences for export to PDF.</td>
</tr>
</tbody>
</table>

| **FrameBorder**  | Session temporary     | These cookies store the preferences for export to PDF.                                                                                     |
| **PageOrientation** |                    |                                                                                                                                          |
| **PageSize**     |                       |                                                                                                                                          |
| **PDFLayerDimension** |                |                                                                                                                                          |
| **PDFOPTS**      |                       |                                                                                                                                          |
### Purpose

<table>
<thead>
<tr>
<th>Cookie</th>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<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 5: Upgrading to IBM Cognos PowerPlay

New versions of IBM® Cognos® PowerPlay® provide enhancements that may affect many components, such as product features and functionality, performance and scalability, and usability. Because of these improvements, upgrading may not be simple, and should be considered a process that you perform in stages.

If you are upgrading both PowerPlay and other IBM Cognos Business Intelligence components, see the IBM Cognos BI Installation and Configuration Guide for upgrade information for IBM Cognos BI components such as Framework Manager.

You should treat upgrading as an IT project that requires careful planning, adequate time, and resources.

When you upgrade, you perform two distinct activities:
1. Install the new version of the product.
2. Move applications to the new version of the product.

Install the New Version of the Product
You can install the new version of the product in the same location as the existing version after you uninstall, or you can install into a new location.

First install into a new location, such as a test environment. This allows you to test your applications in both the old and new environment to ensure that they work as expected when you upgrade. You can compare the appearance and functionality of the reports in both environments to ensure equivalency.

Move Content to the New Environment
As part of the upgrade process, ensure that your applications work as expected in the new version. Sometimes, changes may introduce unexpected results. It is important to test your applications before you move them.

In IBM Cognos BI, when you move content from one environment to another, you do a deployment. Different groups are commonly involved in each of these activities. As part of the project, you should assess both your current IT environment and your existing applications separately, to ensure that the infrastructure can support your business objectives.

If you have IBM Cognos Series 7 content, you can move some of that content to IBM Cognos BI using migration tools that are available in a separate installation.

If you are using previous versions of ReportNet®, Metrics Manager, IBM Cognos for Microsoft® Office, or Transformer, you can upgrade your content to IBM Cognos BI. You can also upgrade from previous versions of IBM Cognos BI, including full and maintenance (MR) releases.
Upgrade Process

The following diagram shows the approach to upgrade. The diagram shows the stages in the upgrade process. Before you start, you plan the upgrade, assess the applications that you want to upgrade and create a test environment. You should iteratively deploy and test content in both the source and target environments before you to move successfully upgraded applications to a production environment.

In some upgrade situations, other tasks may be required. For example, if you use Software Development Kit applications that depend on the report specifications, you must upgrade your Software Development Kit applications before upgrading the report specifications. If you are upgrading from ReportNet 1.1 MR3 or MR4 or from any previous version of IBM Cognos BI, you can use Lifecycle Manager to automate some tasks in the trial upgrade stage.

See the following topics for information about upgrading:

- Planning the Upgrade
- Upgrading from an Earlier Version of IBM Cognos PowerPlay

Planning the Upgrade

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.

The following diagram shows a high level view of the phases in an upgrade project.
When planning your upgrade, ensure that you

- 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 reports run as expected

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

Do not change security providers, such as changing from an IBM® Cognos® Series 7 namespace to Active Directory as part of the upgrade process. You should treat that as a separate project.

Ensure that you have the skills available, either internal or using external resources. Also consider the hardware that you will need before you begin.

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

- Review the documentation.
- Assess applications in the source environment.
- Perform a trial upgrade, which includes the following tasks:
  - Create the test environment.
  - Plan the deployment of content from the source environment to the test environment.
  - Create an export deployment specification.
  - Copy the deployment specification to the test environment.
  - Include configuration objects for import, if required.
  - Import the deployment specification to Cognos BI in the test environment.
  - Test the upgraded content.
- Move to the production environment.

**Review the Documentation**

Documentation is provided from a variety of sources to help you achieve a successful upgrade. All the documentation is available online at the IBM® Cognos® Customer Service Center (http://www.ibm.com/software/data/support/cognos_crc.html).

**Steps**

1. Read the "What's New" section in this guide (p. 15).
   
   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. Read the topic about IBM Cognos BI with other IBM Cognos products (p. 30).

It contains information about other IBM Cognos products that you may have in your environment and that must be considered in the upgrade.

4. From the Documentation link on the IBM Cognos Customer Service Center (http://www.ibm.com/software/data/support/cognos_crc.html), download and review the latest versions of the documentation listed in the following table:

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Cognos PowerPlay Release Notes</td>
<td>Recent issues that may affect an upgrade</td>
</tr>
<tr>
<td>IBM Cognos Business Intelligence New Features</td>
<td>New features that may affect the behavior of existing content</td>
</tr>
<tr>
<td>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 metadata, Impromptu catalogs and reports, PowerPlay® reports, and Upfront content from IBM Cognos Series 7 to IBM Cognos BI</td>
</tr>
<tr>
<td>IBM Cognos Lifecycle Manager User Guide</td>
<td>Using Lifecycle Manager to audit trial upgrades from ReportNet® 1.1 MR3 or MR4 to IBM Cognos BI, Version 8.2 or later</td>
</tr>
<tr>
<td>IBM Cognos Software Development Kit Developer Guide</td>
<td>Upgrading Software Development Kit applications</td>
</tr>
</tbody>
</table>

**Recommendation - Assess Applications in the Source Environment**

Preventing to upgrade provides an opportunity to review your current BI investment, and clean up your source environment. Inventory your BI applications to understand the strengths, weaknesses, and areas for improvement in your environment.

For example, you may have a hundreds of reports, packages, public folders and applications in your environment. However, it is not uncommon to find that a number of applications are not used, or no longer meet the company’s requirements, or do not work in the source environments.

Conduct an audit of your applications to determine which applications should be upgraded. Assessing and reducing the number of reports is a useful exercise. Do not rely only on user feedback to determine which content is used.
An audit of your existing applications may include the following:

- **Do a site survey.**
  
  A survey will help you to assess the current production environment and identify areas that require attention during an upgrade. The site survey should include information about the infrastructure, applications, users, and configuration settings for your IBM® Cognos® BI products.

- **Assess the software that you use in your reporting application.**
  
  List software, such as operating systems, Web servers, security, databases, and so on. Compare the list to the supported versions for your target upgrade version, available from the Production Information, Software Environments links at the IBM Cognos Customer Service Center (http://www.ibm.com/software/data/support/cognos_crc.html). Determine whether any components require updating.

- **List your BI applications, including the following:**
  
  - Framework Manager models
  - published packages
  - reports
  - Transformer models
  - Software Development Kit applications and their dependencies

- **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 may have an impact on the time required to complete the upgrade.

- **List all the reports contained in your application and do the following:**
  
  - Interview the team members to see which cubes, views, or reports are needed and used, which ones can be consolidated, and which ones can be eliminated. Use audit report data to determine report usage.
    
    Upgrade only the reports that work and that users need and use. This reduces the number of applications that you must upgrade.

    For more information about audit reports, see the *Administration and Security Guide*.
  
  - Look at the purpose of each report and assign a priority.
  
    This identifies business-critical applications and the functionality that is required in the new environment.
  
  - Flag reports that fail to run or validate in the current environment.
  
    They are unlikely to upgrade successfully. Repair these reports so that they upgrade.
  
  - Consider retiring unused or little-used reports.
  
  - Group the reports into categories, such as upgrade, eliminate, no longer used, and do not upgrade,
Chapter 5: Upgrading to IBM Cognos PowerPlay

- List the following information about your configuration:
  - configuration settings that you enabled using IBM Cognos Configuration
    These settings are preserved through the upgrade. They are stored in two files. For ReportNet® v1.1, the files are crnstartup.xml and crnlocale.xml. For IBM Cognos BI, the files are cogstartup.xml and coglocale.xml.
  - changes to other configuration files
    Changes to other files must be made manually during the upgrade. If you changed other configuration files, you must assess the changes that you want to preserve in the upgraded environment. This may include .xml, .txt, and .css files in the configuration, templates, webapps, and webcontent directories of the installation location.
    Note that changes to .ini files are not supported. If you changed .ini files, please contact Customer Support.

- Back up all reports, models, and configuration data and files.
- Create an upgrade plan.

Recommendation - Perform a Trial Upgrade

Pilot upgrade projects are valuable and practical exercises because they ensure that the upgrade produce the expected and required outcome. In addition, an evaluation of the pilot project ensures that the upgrade is successful. If unexpected results occur, you can determine whether the differences are enhancements for your situation or whether you should take action to mitigate the differences.

When you upgrade, applications usually work in the new environment, with little or no intervention. By running an pilot upgrade you can validate selected reports to see if the expected results are produced.

Perform a trial upgrade several weeks before upgrading your production system. The trial upgrade identifies components that will upgrade with minimal effort, and components that may require additional actions before or after the upgrade.

Commonly, you upgrade a sample set of reports in an isolated environment, and you compare the appearance and behavior of the reports before and after the upgrade.

Ensure skilled resources are available to perform migration work, especially for mission-critical applications. Also, test and debug all applications prior to deployment.

If you are upgrading from ReportNet® 1.1 MR3 or MR4, you can use Lifecycle Manager to automate some tasks in the trial upgrade stage.

Create the Test Environment

Create a test environment for the new software in preparation for your trial upgrades.

Initially, the new environment does not need to be large, or be the same as your production environment. For example, if it is acceptable, you may use hardware from existing environments, such as development servers.
The environment can be scaled up and out in a phased way after the basic new environment is up and running.

Alternatively, existing environments can remain untouched. If you want the test environment to become the new production environment, configure the test system to match your production environment.

**Steps**

1. Ensure the infrastructure is in place.
2. Review the supported environments.
3. Install the new software in the test environment.

Having the new version of software in a different location than the earlier version ensures that you run both versions at the same time and confirm that your applications work properly in both environments.

After you have installed the software, use the deployment process to upgrade the content. For more information, see the online help in the IBM Cognos Administration console.

**Plan Your Deployment**

Deployment involves moving applications from one installation to another. In IBM® Cognos® BI, you deploy packages, top-level folders, or the entire content store from a source environment to a target environment.

When you deploy, you must consider how to handle security and whether to deploy the entire content store or to deploy selected packages, folders, and directory content. Other considerations relate to the database you use for the content store, bursting reports, and ownership of entries.

For more information about planning the deployment of content to a new environment, see the online help for the Administration console.

The following diagram summarizes the deployment process.

**Security**

Before you deploy, you must consider access permissions and security of deployment archives.

To deploy IBM Cognos Connection entries, you must have the following permissions:

- Execute permissions for the **Administration tasks** secured feature.
- Traverse permissions for the **Administration** secured function.
You must also belong to the System Administrators group, and have read and write access to the Cognos namespace, so that you can deploy the System Administrators group.

For information about deploying IBM Cognos groups and roles, see the online help in the IBM Cognos Administration console.

References to Namespaces
Some entries, such as groups, roles, distribution lists, contacts, data source signons, and some report properties, such as email recipients and report contacts, can refer to entities in namespaces, or authentication providers. When you deploy public folders and directory content, you can deploy these entries with or without the third-party references.

Deploying the Entire Content Store
Deploying the entire content store ensures that all packages, folders, and directory content are copied to a new location. For example, if you are changing the computer where IBM Cognos BI is installed, you can move the entire content store from the old environment to the new environment and keep all the reports and other entries created by administrators and users.

When you import an entire content store, configuration data is included in the export, but excluded from the import by default. Do not change this setting. However, if you must import configuration settings (p. 63), you can change the default in the Advanced Settings.

Deploying Selected Public Folders and Directory Content
You can choose to do a partial deployment, deploying only selected public folders and directory content.

You can choose the packages and folders that you want to deploy by browsing the Public Folders hierarchy and select a package or folder. Once you select a package or folder, its contents are deployed. You cannot select specific entries in the packages or folders. During export, the parent packages and folders are not exported and Content Manager does not create placeholder locations for them in the target environment. During both export and import, you can specify a new target location in the Content Manager hierarchy for each deployed package and folder.

When you do a partial export of public folders and directory content, you must have the following permissions:
- Read and traverse permissions for the entries that you export.
- Write permissions because you create a deployment specification and deployment history when you export.
- Write and set policy permissions for the entries that you import.

Deploying Packages
A package is an entry that contains published reports and metadata. Packages are stored in the content store and appear as entries in IBM Cognos Connection.

During a partial deployment, you can deploy one or more packages at a time. A package can reference objects that are outside the package, such as security objects, data sources, and distribution lists. However, referenced objects are not deployed with the package.
Create an Export Deployment Specification

After planning your deployment, the first step in moving content from the one installation to another is to export the content store or the entries that you want to keep in your new environment. To do this, you create an export deployment specification in your source environment.

The entries are exported to an export deployment archive in the source environment. Later, you import the archive entries into the target environment. You can update the entries in the target environment using the entries from the deployment archive.

Stop the IBM® Cognos® BI service in IBM Cognos Administration before you export and import. For more information, see the Administration and Security Guide.

Steps to Create a New Export Deployment Specification for the Content Store

1. In IBM Cognos Administration, on the Configuration tab, click Content Administration.

2. On the toolbar, click the new export button and follow the instructions in the New Export wizard.

3. To export the entire content store, click Select the entire content store and select whether to include user account information.

4. Click Next.

5. If you want to secure the archive, under Encryption, click Set the encryption password, type a password, and then click OK, and then click Next.

   The summary information appears.

6. Review the summary information and click Next.

   Tip: If you want to change information, click Back and follow the instructions.

7. Determine how you want to run the export by selecting the action you want.

After you run the export, you can move the deployment archive. You can also see the export run history.

Steps to Create a New Export Deployment Specification for Partial Deployments

1. In IBM Cognos Administration, on the Configuration tab, click Content Administration.

2. On the toolbar, click the new export button and follow the instructions in the New Export wizard.

3. To export specific folders and directory content, click Select public folders and directory content, and then click Next.

4. In the Select the Public folders content page, click Add.

5. In the Select entries page, 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 you want. Click the right arrow button to move the selected items to the Selected entries box, and click OK.

6. For each package and folder that you export, do one of the following:
   - If you want to make any changes to the package or folder in the target environment, click the edit button 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.

7. Under Options, select whether you want to include the report output versions, run history, and schedules and what to do with entries in case of a conflict, and then click Next.

8. In the Select the directory content page, select whether you want to export IBM Cognos groups and roles, distribution lists and contacts, and data sources and connections and what to do with the entries in case of a conflict, and then click Next.

9. In the Specify the general options page, select whether to include access permissions and who should own the entries after they are imported in the target environment.

10. Specify the Recording Level for the deployment history, and then click Next.

11. In the Specify a deployment archive page, under Deployment archive, select an existing deployment archive from the list, or type a new name to 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.

12. If you want to secure the archive, under Encryption, click Set the encryption password, type a password, and then click OK.

13. Click Next.

    The summary information appears.

14. Review the summary information and click Next.

    Tip: If you want to change information, click Back and follow the instructions.

15. Determine how you want to run the export by selecting the action you want.

After you run the export, you can move the deployment archive. You can also see the export run history.

**Steps to Run an Export**

1. In the Actions column, click the run with options button.

2. Click Now to run the export immediately, or click Later, and enter the time that you want the export to run.
You can also schedule a task to run on a recurring basis, and view a list of scheduled tasks using the Schedule Management tool.

You can now move the deployment archive.

**Copy the Deployment Specification to the Test Environment**

Move the deployment archive that you created in the source environment to the test environment. Later, you use the deployment archive to import entries into the target environment.

If the source and test environments use the same content store, you can import without moving the deployment archive.

The default location is `c10_location\deployment`.

If you plan to move the deployment archive to a location on a LAN, ensure that there is enough disk space. If you did not encrypt the deployment archive, copy it to a secure location.

**Steps to Copy the Deployment Specification**

1. In the source environment, copy the deployment specification from the deployment files location specified in the configuration tool to a common shared location or shareable media.
   
   In IBM® Cognos® Configuration, the **Deployment files location** property is under **Environment**. If you change this property, the new location must be accessible to the active Content Manager service.

2. In the test environment, copy the deployment specification from the common shared location or shareable media to the deployment files location specified in the configuration tool.

You can now include configuration objects if you’re importing an entire content store or import to the target environment.

**Include Configuration Objects in Import of Entire Content Store**

You can include configuration objects when importing an entire content store. For example, you may 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.

**Steps**

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 button.

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 that appears, type the following in uppercase:
   
   **CM.DEPLOYMENTINCLUDECONFIGURATION**

8. In the **Value** column, type **true**

9. Click **OK** to finish.

**Import to the Test Environment**

You import entries from the deployment archive into the target environment. 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 only 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 already exist in the target environment and the date and time 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.

**Steps to Import Deployment Specification**

1. In the target environment, in **IBM Cognos Administration**, on the **Configuration** tab, click **Content Administration**.

2. On the toolbar, click the new import button 🔄. The **New Import** wizard appears.

3. In the **Deployment archive** box, click the deployment archive that you want to import.

4. If the deployment archive is encrypted, type the password, and then click **OK**.

5. Click **Next**.

6. Type a unique name and an optional description and screen tip for the deployment specification, select the folder where you want to save it, and then click **Next**.

7. Select the content that you want to include in the import.

   **Tip:** To ensure that the required target package or folder exists in the target content store, click the edit button 📋 next to the package, and check the location. If you want, you can change the target location now.

8. Select the options you want, along with your conflict resolution choice for the options that you select.

9. In the **Specify the general options** page, select whether to include access permissions and who should own the entries after they are imported in the target environment.
10. Specify the **Recording Level** for the deployment history.

   The default level, **Basic**, saves the deployment progress and summary information. If you want just the summary information, select **Minimal**. If you want all deployment details, select **Trace**.

11. Click **Next**.

   The summary information appears.

12. Review the summary information, and click **Next**.

13. Determine how you want to run the import by selecting the action you want.

   After you run the import, you can **test the deployment**.

**Steps to Run an Import**

1. In the **Actions** column, click the run with options button.

2. Click **Now** to run the import immediately, or click **Later**, and enter the time that you want the import to run.

3. If you want to upgrade the report specifications, click **Upgrade all report specifications to the latest version**.

   You can also use the Schedule Management tool to schedule a task to run on a recurring basis, and view a list of scheduled tasks.

   You can now **test the deployment**.

**Test the Deployed Content**

After you import the packages from the deployment archive, you can check that all the entries were deployed successfully in the target environment.

You can test your deployment by doing the following:

- Review the run history for a deployment.
- Ensure that the correct packages and folders were imported, along with their contents.
- Run imported reports and report views.

For more information, see the online help in the IBM Cognos Administration console.

**Recommendation - Test the Upgraded Content**

After you import the packages from the deployment archive, you can check that all the entries were deployed successfully in the target environment.

Test your upgraded content by doing the following:

- Test your reports, as follows:
  - In Report Studio, validate each report and note whether the validation was successful.
  - In Report Studio, Query Studio, and Analysis Studio, run the applicable reports and note whether each report ran successfully.
You can download Lifecycle Manager from the IBM Cognos Customer Center (http://www.ibm.com/software/data/cognos/customercenter/) to help you test. Lifecycle Manager is a verification tool that checks that your reports run and produce the same results in the new environment.

- Test models and PowerCubes in IBM Cognos Transformer, if required:
  - Open models with the appropriate security options and save them.
  - Test PowerCubes.

- Test models in Framework Manager.
  You can use the same models and projects in Framework Manager for IBM Cognos BI that you used with the earlier version. When upgrading models, the validation process produces errors for every model. To upgrade a project, open and save it in the new version of Framework Manager. For more information, see the Framework Manager User Guide.

- Repair or exclude reports and models that do not operate correctly.

- Test the repaired reports and models by running them again on the test system.
  Troubleshoot any issues, and contact Cognos Software Services about unresolved upgrade issues.

- Revise the upgrade plan to include adaptations that you made during the trial upgrade.
  For more information, see the online help in the IBM Cognos Administration console.

## Moving to the Production Environment

When all issues that you discovered during the trial upgrade are resolved, you are ready to begin the full upgrade in your production environment. Your upgrade plan will provide the details for each step of the full upgrade.

The following diagram shows the high level steps in the process of moving upgraded applications to a production environment. After preparing the production environment and backing up data and configuration files, you can uninstall the older version of the software, and install the new version in the same location. Then, you can deploy the content from your test environment.

If you want to leverage your existing resources and upgrade in the same directory, you must first back up your configuration data, ensure that Framework Manager models are backed up and checked into a source control system (if applicable), and uninstall the older version of IBM Cognos BI.

Use the following checklist to guide you through the process of moving to a production environment:

1. Prepare the production environment.
• Back up files and data.

You may have modified files other than those in the configuration folder. Back up the entire installation directory.

When you back up the configuration data, store it in a secure directory. You must protect the directory from unauthorized or inappropriate access.

• Install your new release system in the production environment.

If you install the new software from the test environment to the same location as the existing software, you must first uninstall the existing software.

• Configure the system.

❑ Manually configure customization.

• If you manually edited any configuration files, the changes will be overwritten during the upgrade. You must reapply the changes. You should keep a record of any customizations to ensure that they can be reapplied after upgrading. You should also back up these files so that you can restore the original version 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. The system.xml files are overwritten during the installation of IBM Cognos BI. Therefore, you must back up the customized versions of these files and then copy them to the directory after upgrading IBM Cognos BI. The automatic upgrade will be applied when you start the IBM Cognos service.

• The system.xml files for which automatic upgrade is supported are in the following directories:

  c10_location/templates/ps

  c10_location/templates/ps/portal

  c10_location/templates/ps/qs

• **Note:** To upgrade customized files, manually reapply changes after the new software is installed. Use automatic upgrade of system.xml files only when you have made a large number of customizations to these files.

❑ Deploy the application on the production system.

When upgrading, you can export the entire content store to a deployment archive and then import the deployment archive into IBM Cognos BI after upgrading the software.

❑ Deploy the reports and models from the test system to the production system.

---

**Upgrading from an Earlier Version of IBM Cognos PowerPlay**

You must upgrade the software to move from an earlier version of IBM® Cognos® PowerPlay® to a new version of PowerPlay. You must upgrade all components. Components from different versions
are not compatible. If you are using IBM Cognos Series 7 PowerCubes as a data source, it is not necessary to upgrade Transformer unless you want to use the features of the new version of Transformer. PowerCubes that are built using IBM Cognos Series 7 Transformer version 7.3 or later and IBM Cognos Transformer version 8.3 or later are both supported with IBM Cognos Business Intelligence reporting and metrics.

You can run different versions of the software on your computer at the same time, provided that you install them in different directories and configure each to use a different content store and a different set of ports and URLs for each version.

Before you begin upgrading, plan your upgrade strategy (p. 54). The strategy you use depends on the data that you want to use and any customization that you have done with your existing configuration.

After upgrading to IBM Cognos BI using existing data, additional configuration may be required if you want to use new features. For information about new features in IBM Cognos BI, see IBM Cognos BI New Features.

**Content Manager**

When you start the service after upgrading, Content Manager automatically upgrades the schema and contents in the content store if you use the same content store database as the previous version. Upgraded content store databases are not backward compatible and thus cannot be used by previous versions of IBM Cognos BI. To protect your original content store data, you must configure IBM Cognos BI to use a copy of the content store. You create a copy by backing up the original content store and restoring the data into a new content store.

**Content Store**

If you saved reports from IBM Cognos Series 7 PowerPlay® or scorecards from IBM Cognos Metrics Manager 2.x in ReportNet, the content store upgrade carries the saved reports and scorecards forward into IBM Cognos BI.

**Framework Manager**

You can use the same models and projects in Framework Manager for IBM Cognos BI that you used with the earlier version. When upgrading models, the validation process produces errors for every model. To upgrade a project, you open and save it in the new version of Framework Manager. For more information, see the Framework Manager User Guide.

If you have Software Development Kit applications that rely on an earlier version of the report specifications, you cannot use Framework Manager to publish your model without losing backward compatibility.

**Security**

When you upgrade from ReportNet or an earlier version of IBM Cognos BI, security may be affected. For example, new roles may exist that were not in earlier releases and some roles may have new capabilities. As a result, the security of your upgraded system may not be at the desired level. To confirm the security level after upgrading, see the Administration and Security Guide.
Operating Systems

As you upgrade your IBM Cognos BI products, you may choose to install some components on new operating systems. You must consider how these operating systems might affect the installation and configuration of IBM Cognos BI.

If your upgrade includes installing IBM Cognos BI client components on Microsoft Windows® Vista operating system, you must consider the following:

- **roaming profiles**
  
  Profiles of users are stored in a different location than in earlier Windows operating systems. The Documents and Settings directory is replaced by the Users directory. The All Users directory is replaced by the Public directory.

- **environment variables**
  
  The default paths that are associated with environment variables are changed. If you use scripts or applications that reference the paths in the environment variables, you may need to update the scripts and applications.

  In addition, you may want to reconfigure the default file locations in IBM Cognos Configuration so that a single file location can be used across operating systems in your IBM Cognos BI environment. For more information, see the topic about updating file location properties in the configuration chapter (p. 279).

Upgrade IBM Cognos PowerPlay

You can upgrade IBM® Cognos® Business Intelligence in the same directory as an earlier version or in a different directory, depending on where you are in the process. For example, if you are setting up your test environment, you install in a new directory. If you have finished testing your applications and want to upgrade the software in your production environment, you can install in the same directory after uninstalling the earlier version.

If you want to upgrade IBM Cognos BI in the same directory, you must first back up your configuration data, ensure that Framework Manager models are backed up and checked into a source control system (if applicable), and uninstall the older version of IBM Cognos BI. For complete instructions, see the steps to install in the same directory.

If you are installing on a new computer, see the steps to install in a new directory.

When you back up the configuration data, you store it in a secure directory. The directory must be protected from unauthorized or inappropriate access.

An alternative method of upgrading includes exporting the entire content store to a deployment archive and then importing the deployment archive into IBM Cognos BI after the upgrade. For more information about deployment, see the IBM Cognos BI Administration and Security Guide. A deployment upgrade is required if you want to change the type of database that you use for the content store. If you use the deployment upgrade method, only the steps for exporting and restoring the configuration data are different. All other steps are the same as documented in this section.

IBM Cognos BI installs and uses Tomcat as its application server by default. If you do not want to use Tomcat, you must follow a different set of steps to upgrade. For more information, see "Upgrade to IBM Cognos BI in an Application Server Environment " (p. 312).
After the IBM Cognos BI content is upgraded, the report administrator will no longer have access to the Content Administration tool and will not be able to create deployment definitions.

**Customized IBM Cognos BI Files**

If you manually edited any configuration files, the changes will be overwritten during the upgrade. You must reapply the changes. You should keep a record of any customizations to ensure that they can be reapplied after upgrading. You should also back up these files so that the original version can be restored if necessary.

You may have modified files other than those in the configuration folder. Back up the entire installation directory.

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. The system.xml files are overwritten during the installation of IBM Cognos BI. Therefore, you must back up the customized versions of these files and then copy them to the directory after upgrading IBM Cognos BI. The automatic upgrade will be applied when you start the IBM Cognos BI service.

The system.xml files for which automatic upgrade is supported are in the following directories:

- `c10_location/templates/ps`
- `c10_location/templates/ps/portal`
- `c10_location/templates/ps/qs`

**Note:** To upgrade customized files, manually reapply changes after the new software is installed. Automatic upgrade of system.xml files is to be used only when you have made a large number of customizations to these files.

**Steps to Install in the Same Directory**

1. Using your database tools, back up your existing content store database.
   
   For information on how to do this, see the documentation for your database.

2. Back up the following files to a secure location:
   
   - cogstartup.xml and coglocale.xml in the `c8_location/configuration` directory
   - server.xml in the `c8_location/tomcat4.1.27/conf` directory
   - system.xml in the appropriate directory, if required

   Ensure that you note the original directory path for each backed up file. For example, `c8_location/templates/ps`

3. In IBM Cognos Configuration, export the configuration data to the same secure location.
   
   To make the configuration data usable for upgrading, name the file cogstartup.xml.

   **Important:** Because the exported cogstartup.xml file contains unencrypted passwords, ensure that the location is secure.
4. Back up any manually edited files in the `c8_location/configuration` and other directories to a secure location.

5. If you use a source control system such as Concurrent Versions System (CVS), ensure that all Framework Manager models are backed up and checked in before upgrading.

6. Stop all IBM Cognos services and any Web servers hosting IBM Cognos BI content.

7. Prepare Transformer models, if required.

8. Upgrade or install other products.

9. Uninstall IBM Cognos BI from every IBM Cognos BI computer.

10. Install the newer version of IBM Cognos BI in the same directory that you used for IBM Cognos BI on every computer.

11. For files that were manually edited in earlier versions of IBM Cognos BI, edit the same files in the `c10_location` directory and reapply the changes that were made to the original customized files.

    Do not copy the customized files from the backup location to the `c10_location` directories. The earlier versions of these files may not be compatible.

12. If you use Oracle for a notification database, logging database, or the content store database, delete the classes12.jar file or ojdbc14.jar file from the `c10_location\webapps\p2pd\WEB-INF\lib` directory.

    Older versions of ReportNet and IBM Cognos BI used these files, which conflict with the ojdbc5.jar file that is used in the new version.

13. If you use a DB2 content store on a System z operating system, edit and run the script to upgrade the DB2 content store.

    You must have permission to create tablespaces to run the script.

    The script creates new tablespaces and grants Content Manager rights to use the tablespaces.

14. In IBM Cognos Configuration, review the configuration, and then save it.

    When you save the configuration, an upgrade dialog box appears and asks if you want to upgrade your report specifications. The default setting is to not upgrade report specifications.

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

15. Start IBM Cognos BI.

    IBM Cognos BI automatically upgrades the content store. System.xml files are upgraded, if required, to an IBM Cognos BI compatible version.

16. Install and configure Framework Manager.
Chapter 5: Upgrading to IBM Cognos PowerPlay

17. Upgrade your Framework Manager projects and reports as required. For instructions, see the Framework Manager User Guide.

Report Studio users must clear their Web browser cache to get the latest images.

18. Install and configure Transformer, if required.

19. Upgrade Transformer models and PowerCubes, if required.

**Steps to Install in a New Directory**

1. Using your database tools, copy your existing content store database into a new content store database.

   For information on how to do this, see the documentation for your database.

2. Back up the following files to a secure location:
   - coglocale.xml in the \c8\_location\configuration directory
   - server.xml in the \c8\_location\tomcat4.1.27\conf directory
   - system.xml in the appropriate directory, if required
     
     Ensure that you note the original directory path of the backed up files. For example, \c8\_location\templates\ps
   - any manually edited files in the \c8\_location\configuration and other directories

3. In IBM Cognos Configuration, export the configuration data to the same secure location.

   To make the configuration data usable for upgrading, name the file cogstartup.xml.

   **Important:** Because the exported cogstartup.xml file contains unencrypted passwords, ensure that the location is secure.

4. Prepare Transformer models, if required.

5. Upgrade or install other products.

6. Install IBM Cognos BI in a new directory.

7. Copy the .xml files from the secure backup location to the following directory:
   - Copy cogstartup.xml and coglocale.xml to \c10\_location\configuration.
   - Copy server.xml to \c10\_location\tomcat4.1.27\conf.
   - Copy system.xml to the same directory in the new location as it was in the earlier version, if required.
     
     For example,
     
     \c10\_location\templates\ps

   If you are prompted to overwrite existing files, click Yes.

8. For files that were manually edited, edit the same files in the \c10\_location directory and reapply the changes that were made to the original customized files.
Do not copy the customized files from the backup location to the `c10_location` directories. The earlier versions of these files may not be compatible with the new version of IBM Cognos BI.


10. If you use a DB2 content store on a System z operating system, edit and run the script to upgrade the DB2 content store.
    
    You must have permission to create tablespaces to run the script.
    
    The script creates new tablespaces and grants Content Manager rights to use the tablespaces.

11. In IBM Cognos Configuration, configure IBM Cognos BI to point to the new content store, configure new ports and URLs, use a different cookie path, and then save the configuration.
    
    Ensure that the port numbers and service name for this installation are different from those used for earlier versions so that there are no conflicts.
    
    Ensure that security authentication settings are not changed. For example, the namespaces must be the same for policies, users, roles, and groups to work correctly.
    
    When you save the configuration, an upgrade dialog box appears and asks if you want to upgrade your report specifications. The default setting is to not upgrade report specifications.
    
    **Important:** Do not upgrade your report specifications if you have SDK applications that create, modify, or save report specifications. You must first update your SDK applications to comply with the IBM Cognos BI report specifications schema. Otherwise, your SDK applications may not be able to access the upgraded report specifications. In addition, do not save your reports until the SDK applications have been updated. For information about upgrading report specifications, see the IBM Cognos Software Development Kit *Developer Guide*.

12. Start IBM Cognos BI.
    
    IBM Cognos BI automatically upgrades the new content store. System.xml files are upgraded, if required, to an IBM Cognos BI compatible version.

13. Install and configure Framework Manager, if required.

14. Upgrade your Framework Manager projects and reports, if required. For instructions, see the Framework Manager *User Guide*.

15. Open the Administration portal, and unregister the dispatchers that are used with earlier versions of IBM Cognos BI.
    
    When you open the Administration portal in IBM Cognos BI, you may see the dispatchers that are registered for both versions.
    
    For more information, see the *Administration and Security Guide*.

16. Install and configure Transformer, if required.

17. Upgrade Transformer models and PowerCubes, if required.

18. When you are ready to uninstall the previous version of IBM Cognos BI, do the following:
    
    - Stop the IBM Cognos BI service and any Web servers hosting IBM Cognos BI content.
Uninstall IBM Cognos BI from all computers.

When you complete the upgrade tasks, IBM Cognos BI is fully configured except for new properties and features.

If you use Chinese, Japanese, or Korean characters, you may notice differences in some characters after upgrading from IBM ReportNet to IBM Cognos BI. For more information, see the Troubleshooting section of the Administration and Security Guide.

If you use a DB2 database for the content store, you can tune the database to take advantage of DB2 features. For more information, see the Architecture and Deployment Guide.

To ensure the security and integrity of IBM Cognos BI, it is important to protect the installation directory from unauthorized or inappropriate access.

Upgrading a DB2 Content Store on a System z Operating System

If you use a DB2 content store on a System z operating system, you must run a script that creates new tablespaces and grants Content Manager rights to use the tablespaces before you save the configuration for the upgraded IBM Cognos BI product.

You must have permission to create tablespaces to run the script. You must run the script after you install the new version of IBM Cognos BI and before you save the configuration for the new version.

Steps

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 DB2 database.

For the placeholders listed in the following table, ensure that you use the same values when you configure the connection to the content store in IBM Cognos Configuration:

<table>
<thead>
<tr>
<th>Placeholder</th>
<th>Property in IBM Cognos Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMSCRIPT_DATABASE</td>
<td>Resource name that appears under Data Access &gt; Content Manager in the Explorer window</td>
</tr>
<tr>
<td>CMSCRIPT_USERNAME</td>
<td>The user ID portion of User ID and password in the Properties window</td>
</tr>
</tbody>
</table>

3. Save and run the file.

You can now continue the upgrade process by opening IBM Cognos Configuration to configure properties and start the IBM Cognos service.
Install or Upgrade Other Products

When you upgrade IBM® Cognos® PowerPlay®, you may need to upgrade to new versions of other products, update some components of other products, or install additional other products to support new features in IBM Cognos Business Intelligence.

To view a list of other products that are used by IBM Cognos BI, see "Verify System Requirements" (p. 38).

To review an up-to-date list of environments supported by IBM Cognos products, such as operating systems, patches, browsers, web servers, directory servers, database servers, and application servers, visit the IBM Cognos Customer Center (http://www.ibm.com/software/data/support/cognos_crc.html).

Step

- If you do not have the supported version of a required product, install or upgrade the product. For information, see "Preparing to Install" (p. 37).
  - setting up a database client
  - updating the Java™ environment
  - configuring a web server
  - configuring a web browser
  - changing the version of Java Runtime Environment used in IBM Cognos BI

For instructions to install or upgrade other products, see the instructions provided with each product.

Run Multiple Versions or Instances of IBM Cognos BI at the Same Time

You must change the ports and the Web server alias in IBM® Cognos® BI if you want to run IBM Cognos BI and ReportNet®, or two instances of IBM Cognos BI, on the same computer and at the same time.

In ReportNet, there is no default cookie path, which means the cookie is sent to all URLs on the Web server. If IBM Cognos BI uses the same Web server, IBM Cognos BI will then receive two cam_passport cookies. To prevent this conflict, you must set a cookie path in ReportNet.

Other configuration changes may be required depending on your environment. If you use Portal Services, you must specify the location of the applications.xml file. If you use an ISAPI gateway on an IIS Web server, you must isolate the IBM Cognos BI gateway to prevent a conflict with the ReportNet gateway. For IIS 5, you isolate the gateway by setting the application protection for the Web site and virtual directories to High. For IIS 6 and 7, you must create an application pool for each version of the IBM Cognos BI product and associate the aliases to it.
If you are using the same type of database for the content store with multiple instances or versions of an IBM Cognos BI product, then to avoid conflicts between the database instances, you must change the content store port in IBM Cognos Configuration.

**Steps for the New Instance or Version of IBM Cognos BI**

1. In IBM Cognos BI, start IBM Cognos Configuration.

2. In the Explorer window, click Environment.

3. In the Properties window, under Dispatcher Settings, click the value for Internal dispatcher URI.

4. Select the port number and then type the new port number.

5. If required, change the port number for the following URIs to match the new port number that you entered for Internal dispatcher URI.
   - Under Dispatcher Settings, change the port for External dispatcher URI.
   - Under Other URI Settings, change the port for Dispatcher URI for external applications and Content Manager URIs.

   Content Manager URIs does not appear on a gateway computer.

6. Under Gateway Settings, click the value for Gateway URI and ensure that the URI contains the correct Web server alias for IBM Cognos BI. For example, replace crn with ibmcognos.

7. If you are using Portal Services, update the applications.xml file:
   - In the Explorer window, click Environment > Portal Services.
   - In the Properties window, ensure that the port number for Location of Applications.xml matches the port for the other URI properties.

8. In the Explorer window, click Data Access > Content Manager > Content Store.

9. In the Properties window, configure IBM Cognos BI to use the new content store:
   - For Database name, specify the name of the new content store.
   - To avoid conflicts with other instances of content store databases, for the Database server and port number property, specify the server name and a different port number.
   - If you are using Cognos Content Database as the content store, and another instance of Cognos Content Database is running on the computer, then you must also specify a different listening port number:
     In the Explorer window, expand Environment > IBM Cognos content database.
     In the Properties window, for Listening port number, type the port number.

**Important:** When you install the IBM Cognos BI product, you must select Cognos Content Database in the installation wizard. Cognos Content Database is not for use in a production environment.
For **User ID and password**, click the edit button and specify the userid and password to access the new content store.

10. If you are running two instances of IBM Cognos BI, change the cookie path for the new version of IBM Cognos BI:

   - From the **Actions** menu, click **Edit Global Configuration**.
   - In the **Global Configuration** window, click **Cookie Settings**.
   - Go to a different path from the one that is used by the older version of IBM Cognos BI.
   - Click **OK**.

11. Save the configuration and start IBM Cognos BI.

**Steps for ReportNet or the Older Version or Instance of IBM Cognos BI Product**

1. In ReportNet or the older version or instance of IBM Cognos BI product, start IBM Cognos Configuration.

2. Change the cookie path:

   - From the **Actions** menu, click **Edit Global Configuration**.
   - In the **Global Configuration** window, click **Cookie Settings**.
   - Set the path to the installation directory (for example, /crn).
   - Click **OK**.

3. Save the configuration.

You can now run ReportNet and IBM Cognos BI, or two instances of IBM Cognos BI, at the same time.

**Note:** When you change from the default ports in the URI properties on a Microsoft® Windows® operating system, the port number is automatically appended to the service name. The service name in IBM Cognos Configuration does not show the port number. You can view the service name and port number under **Services** in your Windows administrative tools.
You can install IBM® Cognos® PowerPlay® 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 PowerPlay on different computers. For more information, see "Installing and Configuring IBM Cognos PowerPlay Server Components on Different Computers" (p. 113).

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.

Use the following checklist to guide you through the installation tasks:

- If you want to use Report Studio, Analysis Studio, or Query Studio, install IBM Cognos Business Intelligence Server before you install IBM Cognos PowerPlay.
  
  For instructions, see the IBM Cognos BI Installation and Configuration Guide.

- Install IBM Cognos PowerPlay

- Install the fix pack, if available.

- Create a database for a DB2 content store on Linux using a script

- Create tablespaces for a DB2 content store on z/OS

- Update the Java environment

- Set JDBC driver options for using DB2 as a content store

- Set up database connectivity for the content store database

- Configure IBM Cognos PowerPlay

- Configure the web server

- Start the services

- Test the installation

- Install and configure migration components on IBM Series 7 computers

You can customize the components for use in your environment by changing other settings in IBM Cognos Configuration (p. 219).
Install IBM Cognos PowerPlay

Use the installation wizard to select the components that you want to install and the location on your computer where you want to install them. 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 PowerPlay with IBM Cognos Business Intelligence Server, install and configure IBM Cognos BI Server first. Both products must be the same version. For more information, see "IBM Cognos Products That Interoperate with IBM Cognos PowerPlay" (p. 31).

If you are upgrading from a previous release of PowerPlay, you must use the upgrading steps. For information, see "Upgrading to IBM Cognos PowerPlay" (p. 53).

Upgrading your Installation

If you are upgrading from a previous release of IBM Cognos products, you must use the upgrading steps (p. 53).

If you are upgrading from ReportNet or 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® 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® 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 one Cognos Content Database. If you install Cognos Content Database on the same computer as Content Manager, and you later decide to use another database for your content store, you must uninstall Cognos Content Database.

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.

Steps to Install for UNIX and Linux

1. If you are installing to a directory with other IBM Cognos BI components, stop the IBM Cognos BI 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 IBM Java, to run on Linux®.

   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 on the CD or in the directory where the installation files were downloaded and extracted, 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 *(p. 323)*.

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

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

   If you want to use the content store database that is provided with IBM Cognos BI, select Cognos Content Database from the components list. If you later decide to use another database for your content store, you must uninstall Cognos Content Database.

   If you are installing in a directory that contains other IBM Cognos BI components, you are prompted to create backup copies of the files that will be replaced.

   Install IBM Cognos PowerPlay 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.

   - Ensure that the IBM Cognos Configuration check box is clear. Do not configure IBM Cognos BI immediately because you must do other tasks first to ensure that your environment is properly set up.
You can later configure IBM Cognos BI using IBM Cognos Configuration by typing cog-config.sh in the \c10_location/bin directory, or by running a silent configuration or editing cogstartup.xml in the \c10_location/configuration directory.

- Click Finish.

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

11. On Linux, set the PRINTER environment variable to the name of your printer.

To ensure the security and integrity of IBM Cognos BI, it is important to protect the installation directory from unauthorized or inappropriate access.

If you want users to see product documentation in a language other than English, you must install the Supplementary Languages Documentation component in the location where you installed the gateway component. For more information, see "Install Translated Product Documentation" (p. 177).

**Steps to Install for Windows**

1. If you are installing to a directory with other IBM Cognos BI components, stop the IBM Cognos BI 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 for the installation program. You can change the language of the user interface for the product to any of the installed languages after installation.

4. Follow the directions in the installation wizard to copy the required files to your computer.
   If you want to use the content store database that is provided with IBM Cognos BI, select Cognos Content Database from the components list. If you later decide to use another database for your content store, you must uninstall Cognos Content Database.

   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.

   If you are installing in a directory that contains other IBM Cognos BI components, you are prompted to create backup copies of the files that will be replaced.
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**.
   - Ensure that the IBM Cognos Configuration check box is clear. Do not configure IBM Cognos BI immediately because you must do other tasks first to ensure that your environment is properly set up.
     
     You can later configure IBM Cognos BI using the Windows **Start** menu to start IBM Cognos **Configuration** from the shortcut folder.
   - Click **Finish**.

To ensure the security and integrity of IBM Cognos BI, it is important to protect the installation directory from unauthorized or inappropriate access.

If you want users to see product documentation in a language other than English, you must install the Supplementary Languages Documentation. For more information, see "Install Translated Product Documentation" (p. 177).

If you want to use the samples, you must install them from the IBM Cognos Business Intelligence Samples CD. For more information, see "Install the IBM Cognos BI Samples" (p. 172).

### 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 Business Intelligence components.

If a fix pack becomes available after your IBM Cognos product has been deployed, you must stop the service, install the fix pack in the same location as the IBM Cognos BI components, and then start the service.


**IMPORTANT:** Fix packs are not standalone installations. You must install them on computers that have IBM Cognos BI server components installed. Install the fix pack or 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 `C8BISRVR_version=`.

Before you install the fix pack, create a backup of the content store database. In addition, back up any customized files from the current installation.

**Steps for the Microsoft Windows Operating System**

1. If your IBM Cognos BI product is running, open IBM Cognos Configuration and stop the IBM Cognos service.
2. Back up the content store database.
3. If your IBM Cognos BI environment is customized, back up the entire IBM Cognos BI location.
4. Insert the disk for the Microsoft® Windows® operating system fix pack or go to the location where you downloaded and extracted the files. If more than one fix pack is available, install the fix pack with the lowest version number first.

5. On the disk or in the download location, go to the win32 directory and double-click the issetup.exe file.

6. Follow the directions in the installation wizard, installing in the same location as your existing IBM Cognos BI server components. The issetup program prompts you to allow the fix pack to create a backup copy in the installation folder before copying new files.

7. If an updater is available, do the following:
   - To install from a disk, insert the updater disk for the Windows operating system.
   - To install from a download, follow the instructions on the support site and then go to the location where you downloaded and extracted the files.
   - Within the updater directory on the disk or download location, go to the win32 directory and double-click the issetup.exe file.
   - Follow the directions in the installation wizard.

8. To return a deployed IBM Cognos BI product to service, open IBM Cognos Configuration, save the configuration, and then start the IBM Cognos service.

9. If you have a distributed environment, repeat these steps for all remaining IBM Cognos BI servers.

10. If you are running the IBM Cognos BI product on an application server other than the default, Tomcat, redeploy the IBM Cognos BI product to the application server. For instructions, see "Configure Application Server Properties and Deploy IBM Cognos Components" (p. 302).

**Steps for the UNIX and Linux Operating Systems**

1. If your IBM Cognos BI product is running, open IBM Cognos Configuration and stop the IBM Cognos service.

2. Back up the content store database.

3. If your IBM Cognos BI environment is customized, back up the entire IBM Cognos BI location.

4. If using a disk, mount the fix pack disk that is appropriate for your UNIX® or Linux® operating system, using Rock Ridge file extensions.

   **Important:** To mount the IBM Cognos 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 rrrip <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.

5. If using a download, go to the location where you downloaded and extracted the fix pack files. If more than one fix pack is available, install the fix pack with the lowest version number first.

6. To start the installation wizard, type

   `/issetup`

   If you do not use XWindows, run an unattended installation (p. 323).

7. Follow the directions in the installation wizard to install to the same location as your existing IBM Cognos BI server components.

   The issetup program prompts you to allow the fix pack to create a backup copy in the installation folder before copying new files.

8. If an updater is available, do the following:

   - To install from a disk, mount the updater disk that is appropriate for your operating system, using Rock Ridge file extensions.

     **Important:** To mount the disk on HP-UX, follow the bulleted instructions in step 4.

   - To install from a download, go to the location where you downloaded and extracted the updater files.

   - To start the installation wizard, type

     `/issetup`

     If you do not use XWindows, run an unattended installation (p. 323).

   - Follow the directions in the installation wizard to install to the same location as your existing IBM Cognos BI server components.

9. To return a deployed IBM Cognos BI product to service, open IBM Cognos Configuration, save the configuration, and then start the IBM Cognos service.

10. If you have a distributed environment, repeat these steps for all remaining IBM Cognos BI servers.
Create a Database for a DB2 Content Store on Linux Using a Script

A script named C8DB2.sh is provided to allow you to create a content store database in DB2 on Linux operating systems. The script is located in the c10_location/C8SE directory after you install IBM Cognos Business Intelligence.

DB2 must be installed and configured before you run the script. The script creates and configures a database that you can use as your content store. For more information about the minimum settings for a DB2 content store, see "Suggested Settings for Creating the Content Store in DB2 on Linux, Windows and UNIX" (p. 42).

Permissions

To run the script you must be a member DB2 group named dasadm1. When you run the script you are prompted for a user account that will be given the required privileges to access and write to the database. When you configure the content store connection information for IBM Cognos BI, use the user account that you enter when you run the script, not the user account you use to run the script.

The script creates the database in the first DB2 instance in your path. If you have more than one DB2 instance, ensure that the DB2 instance in which you want to create the content store appears first in your path.

Steps

1. From the c10_location/C8SE directory where you installed IBM Cognos BI, copy the C8DB2.sh script to your database server.

2. On your database server computer, change to a user who is a member of the DB2 group named dasadm1.

3. Run the script using the following command:

   ./C8DB2.sh

   You are prompted for the following information:

   • a name for the content store database
   • a user who will be granted the required privileges to access and write to the content store database

   When you set the database connection properties for the content store, you must enter this user in the User ID and password property.
When the script has finished, a database will be created in DB2 that you can use as your content store database.

Create Tablespaces for a DB2 Content Store on z/OS

A database administrator must run a script to create a set of tablespaces required for the content store database. The script must be modified to replace the placeholder parameters with ones that are appropriate for your environment.

If you are using the same DB2® database on z/OS® for both the content store and notification (the default setup), then you must run scripts to create the notification tablespaces at the same time that you create the content store tablespaces.

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. For more information, see the IBM® DB2 Information Center.

Steps

1. Connect to the database as a user with 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. Open the tablespace_db2zOS.sql script file and 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 may be added in the future.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMSCRIPT_CREATE_IN</td>
<td>Specifies the base tables location</td>
</tr>
<tr>
<td></td>
<td>For example, databaseName.baseTablespaceName</td>
</tr>
<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 instance identification for the content store database.</td>
</tr>
<tr>
<td></td>
<td>The ID must not be longer than two characters.</td>
</tr>
<tr>
<td>CMSCRIPT_TABLESPACE</td>
<td>Specifies the name of the tablespace that will contain all of the base tables in the content store.</td>
</tr>
<tr>
<td></td>
<td>Auxiliary tables are not included.</td>
</tr>
<tr>
<td></td>
<td>The name cannot be longer than six characters.</td>
</tr>
</tbody>
</table>
### Parameter Name | Description
---|---
CMSCRIPT_LARGE_BP | Specifies the name of the large buffer pool allocated for especially large objects.
CMSCRIPT_REGULAR_BP | Specifies the name of the regular size buffer pool allocated for regular and large objects.
CMSCRIPT_USERNAME | Specifies the user account that accesses the content store database.

4. Save and run the script.

5. Grant the IBM Cognos® user rights to the tablespaces that were created when you ran the `tablespace_db2zOS.sql` file script:
   - In the remote access tool, open the `rightsGrant_db2zOS.sql` script file and replace the placeholder parameters with values that are appropriate for your environment.
     **Tip:** Ensure that you use the same values that you used when you allocated resources to the buffer pools and user account.
   - Save and run the file.

6. Replace placeholder parameters in the following scripts and run them:
   - `dbInitTest_db2zOS.sql`
   - `dbInitMeta_db2zOS.sql`
   - `dbInitScript_db2zOS.sql`
   - `dbInitLock_db2zOS.sql`

7. If you are using the same database for notification that you use for the content store (the default setup), perform the remaining steps.

8. Open the `NC_TABLESPACES.sql` script file and use the following table to help you to replace the placeholder parameters with ones that are appropriate for your environment.

For parameters that are not in the script, add them.

### Parameter Name | Description
---|---
NCCOG | Specifies the name of the content store database.
DSN8G810 | Specifies the name of the storage group used for the content store database.
BP32K | Specifies the name of the buffer pool used for the tablespaces.
9. Save and run the script.

10. Open the NC_CREATE.sql script file and replace the NCCOG placeholder parameter with the name of the content store database.

11. Save the script.

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

The content store database is created. You can now configure a database connection.

### JDBC Driver Options for Using DB2 Database as a Content Store

IBM® Cognos® Business Intelligence uses Java™ Database Connectivity (JDBC) to access the database used for the content store.

If you use DB2® on a Microsoft® Windows®, Linux®, or UNIX® operating system as your content store you must choose whether to use the type 2 or type 4 JDBC driver depending on how you want to connect to the content store.

If you are using a DB2 database on z/OS® for the content store, you must use a type 4 JDBC connection.

You specify the driver type to use in IBM Cognos Configuration.

#### Configuration Options for the Universal Driver

DB2 introduced a universal JDBC driver that contains both type 2 and type 4 JDBC driver support. The universal driver, db2jcc.jar, replaces the deprecated type 2 JDBC driver, db2java.zip.

If you are upgrading, you can continue to use a type 2 JDBC connection with no configuration change required. If you want to use a type 4 JDBC connection, you must change your configuration to include the host name and port number of the database server.

For information about configuration requirements, "Set Database Connection Properties for the Content Store" (p. 95).

For both a type 2 and type 4 JDBC connection, however, you must copy the new universal driver, db2jcc.jar, and the accompanying license file, db2jcc_license_*.*, to your IBM Cognos BI installation location.

For more information, see "Set Up Database Connectivity for the Content Store Database" (p. 91).

#### Using the Type 2 JDBC Driver

Type 2 JDBC drivers are comprised of a native-API component and a Java™ component.

The connection to the DB2 database occurs through the DB2 CLI libraries, which comprise the native component that communicates with the database server.

Because type 2 JDBC drivers require common client code and rely on the native code of the product, a DB2 client must be installed to use this driver. For example, a DB2 client must be installed on the computer where you have Content Manager installed.
Using the Type 4 JDBC Driver

Type 4 JDBC drivers are pure Java drivers which provide direct access to DB2 database features through network communication.

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

Set Up Database Connectivity for the Content Store Database

If you are using a database other than Cognos® Content Database 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.

Steps for DB2

1. If you are using a type 2 JDBC connection, install the DB2® client software on the Content Manager computers.
   
   If you are using a type 4 JDBC connection for DB2, you are not required to install the DB2 client software where Content Manager is installed. If you use a DB2 database on z/OS® for the content store, you must use a type 4 JDBC connection.
   
   For more information about the differences between type 2 and type 4 drivers, see "JDBC Driver Options for Using DB2 Database as a Content Store" (p. 90).

2. If you are using a type 2 JDBC connection, and the content store is on a different computer than Content Manager, configure a database alias to the content store.
   
   On Microsoft® Windows® operating systems, run the DB2 Client Configuration Assistant.
   
   On UNIX® or Linux® operating systems, use the DB2 command line interface.
   
   If the content store database and Content Manager are on the same computer, the content store name automatically becomes the alias.
   
   When you configure the Content Manager computers, ensure that they are all configured to use the same content store.

3. On Windows, stop the DB2 services and the HTML Search Server.

4. Copy the following files from DB2_installation/sqlib/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, db2jcc_license_cu.jar
     for DB2 on z/OS, 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.DB2Jjcc -version
```

5. On Windows, restart the DB2 services and the HTML Search Server.

6. On UNIX, if you are using a type 2 JDBC connection, ensure that the 32-bit DB2 libraries are in the library search path, which is usually the $DB2DIR/lib directory or the $DB2DIR/lib32 directory.

7. Repeat this entire procedure on the IBM Cognos BI computers where Content Manager is installed or where notification is sent to a DB2 database.

You can tune the database to take advantage of DB2 features. For more information, see the "Tuning a DB2 Content Store" (p. 333).

Steps for Oracle

1. On the computer where the Oracle client is installed, go to the ORACLE_HOME/jdbc/lib directory.

2. Copy the ojdbc5.jar file to the c10_location/webapps/p2pd/WEB-INF/lib directory on computers where Content Manager is installed and where notification is sent to an Oracle database.

   If the directory contains the classes12.jar file or ojdbc14.jar file, delete it before installing the ojdbc5.jar file.

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

Steps for Informix

1. On the computer where Informix® is installed, go to the Informix_location/sqllib/jaav 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

Steps for Sybase

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.

Update the Java Environment

You can use an existing Java™ Runtime Environment (JRE) or the JRE that is provided with IBM® Cognos® Business Intelligence. To support the cryptographic services in IBM Cognos BI, you may
be required to update or set a JAVA_HOME environment variable. Depending on your security policy, you may also have to install the unrestricted Java Cryptography Extension (JCE) policy file.

**JAVA_HOME**

If you want to use your own JRE and have JAVA_HOME set to that location on Microsoft® Windows® or if you are installing on UNIX® or Linux®, you must update JAVA_HOME for the cryptographic services.

On Windows, you can set JAVA_HOME as a system variable or a user variable. If you set it as a system variable, it may be necessary to restart your computer for it to take effect. If you set it as a user variable, set it so that the environment in which Tomcat is running can access it.

If you do not have a JAVA_HOME variable already set on Windows, the JRE files provided with the installation will be used, and you do not have to update any files in your environment. If JAVA_HOME points to a Java version that is not valid for IBM Cognos BI, you must update JAVA_HOME with the path to a valid Java version.

**Unrestricted JCE Policy File**

Whether you use the default Windows JRE or download a JRE for UNIX or Linux, the JRE includes a restricted policy file that limits you to certain cryptographic algorithms and cipher suites. If your security policy requires 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.

**Steps**

1. Ensure that the JAVA_HOME environment variable is set to the JRE location.
   
   For example, to set JAVA_HOME to a JRE that you are already using, the path is `Java_location/bin/jre/version`.

2. If your security policy requires it, download and install the unrestricted JCE policy file.
   
   For IBM Java, the unrestricted JCE policy file is available from the following location:
   
   
   You may have to complete additional configuration for cryptographic settings. For more information, see "Configuring Cryptographic Settings" (p. 225).

**Configure IBM Cognos PowerPlay**

Use the configuration tool, IBM® Cognos® Configuration, to configure IBM Cognos Business Intelligence, or to start and stop IBM Cognos services.

**Step to start IBM Cognos Configuration on a Windows computer**

- From the **Start** menu, click **Programs**, IBM Cognos 10, IBM Cognos Configuration

**Step to start IBM Cognos Configuration on a UNIX or Linux computer**

- Go to the `c10_location/bin` directory and then type
  
  `/cogconfig.sh`
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 dashboards that are sent by email. By default, the URI properties specify the localhost.

Steps
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 button. 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.

Steps
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.
   For more information about configuring IBM Cognos BI to use an authentication provider, see "Configuring IBM Cognos Components to Use an Authentication Provider" (p. 181).
For more information about configuring IBM Cognos BI to use an authentication provider, see "Configuring IBM Cognos BI Components to Use an Authentication Provider" in the Installation and Configuration Guide.

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.

In a production environment, you must use an enterprise-level database for your content store. If you have been using Cognos Content Database in a test or proof-of-concept system, you can use the features in the administration portal to back up and archive the data before moving to an enterprise-level database in your production environment. For more information, see the topic about deploying the entire content store in the Administration and Security Guide.

If Cognos Content Database is on the same computer as Content Manager in your production environment, then after you configure your IBM® Cognos Business Intelligence product to use an enterprise-level database for the content store, you must uninstall Cognos Content Database.

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.

Ensure that you used one of the supported database servers to create the content store.

Steps for DB2® on Linux®, UNIX®, or Windows® Operating Systems

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.
   - Type the appropriate values and click OK.

5. To use a type 4 JDBC connection, for the Database server and port number property, type a value, using host:port syntax.

   If you leave this property blank, a type 2 JDBC connection is used.

   For more information about the differences between the driver types, see "JDBC Driver Options for Using DB2 Database as a Content Store" (p. 90).
6. From the File menu, click Save.
   The logon credentials are immediately encrypted.

7. To test the connection between Content Manager and the content store database, from the Actions menu, click Test.
   Content Manager connects to the database, checks the database permissions, and creates and populates a table. The table is not deleted and is used each time that the test is repeated.

**Steps for DB2 on z/OS**
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. 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. To use a type 4 JDBC connection, for the Database server and port number property, type a value, using host:port syntax.
   To connect to DB2® on z/OS®, you must use a type 4 JDBC connection.
   For more information about the differences between the driver types, see "JDBC Driver Options for Using DB2 Database as a Content Store" (p. 90).
6. In the Explorer window, click Local Configuration.
7. In the Properties window, next to Advanced properties, click inside the Value box, and then click the edit button.
   The Value - Advanced properties dialog box appears.
8. To add the parameters that you used to create the tablespaces, click Add.
   All of the parameters except CMSCRIPT_USERNAME are added.
9. From the File menu, click Save.
   The logon credentials are immediately encrypted.
10. To test the connection between Content Manager and the content store database, from the Actions menu, click Test.
    This tests the connection between Content Manager and the content store database.

**Steps for Microsoft SQL Server, Oracle, Informix, and Sybase**
1. On the computer where you installed Content Manager, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Data Access**, **Content Manager**, right-click **Content Store** and click **Delete**.

   This 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**.

   If you installed more than one version of IBM Cognos BI, you must use a different content store for each version. When a content store is used by a new version of IBM Cognos BI, it cannot be used by an older version.

   **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 values depending on 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.

     **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:**

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

     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 **Service name** 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, auto-
matically 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 button 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 button.
   - 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.

10. To test the connection between Content Manager and the content store database, from the Actions menu, click Test.
    Content Manager connects to the database, checks the database permissions, and creates and populates a table. The table is not deleted and is used each time that the test is repeated.

    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.

**Steps**

1. In the **Explorer** window, under **Data Access**, click **Notification**.

2. In the **Properties** window, for the SMTP mail server property, type the host name and port of your SMTP (outgoing) mail server.

   **Tips**

   To be able to open reports that are sent by email, you must 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.

   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.

3. Click the Value box next to the Account and password property and then click the edit button when it appears.

4. 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 Yes. Ensure that the default user name has been removed. Otherwise, the default account is used and notifications will not work properly.

5. In the Properties window, type the appropriate value for the default sender account.

6. Test the mail server connections. In the **Explorer** window right-click **Notification** and click **Test**.

   IBM Cognos Business Intelligence tests the mail server connection.

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 "Configuring IBM Cognos Components to Use an Authentication Provider" (p. 181).
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.

Steps

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 button.
   - 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**.

**Configure the Web Server**

For all installations, before you use Web pages generated by IBM® Cognos® Business Intelligence, you must configure your Web server. You must create virtual directories, or aliases, so that users can connect to IBM Cognos BI in the portal. If 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. The steps for creating an application pool vary depending on your operating system.

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.

**Steps to Create Virtual Directories**

1. 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>
You can use a name other than ibmcognos in the aliases. However, you must use cgi-bin as the second part of the alias and you must change the virtual directory in the Gateway URI property to match the new IBM Cognos alias.

For Apache Web Server, ensure that you define the ibmcognos/cgi-bin alias before the ibmcognos alias in the httpd.conf file located in the Apache_installation/conf directory. The ibmcognos/cgi-bin alias must be defined as a ScriptAlias.

2. If you want to use the Report Studio image browser, enable Web Distributed Authoring and Versioning (WebDAV) on your Web server.

   If you use Apache Web Server, specify a directory in which to enable WebDAV. For information about configuring WebDAV, see your Web server documentation.

   If you use Microsoft® Internet Information Services (IIS), enable the Read and Directory Browsing properties for the URL you want to access.

3. For IBM Cognos BI for reporting, set the content expiry on the c10_location/webcontent/pat/images virtual directory in your Web server.

   Each time a user opens Report Studio, their Web browser checks with the Web server to determine if images are current. Because there are over 600 images, this can result in excess network traffic. You can postpone this check until a specified date by using the content expiry feature of the Web server.

   For information on setting content expiry, see the documentation for your Web server.

   **Note:** When you upgrade, Report Studio users must clear their Web browser cache to get the latest images.

If you use Web aliases other than ibmcognos, or your Web server is on another computer, or you are using Microsoft Internet Application Interface (ISAPI), apache_mod or a servlet gateway, change the Gateway URI when you configure IBM Cognos components.

**Steps to Create an Application Pool on Windows Server 2008**

1. For the Microsoft® Windows® operating system, from the Start menu, select Control Panel > Performance and Maintenance > Administrative Tools.

2. Launch Internet Information Services (IIS) Manager.

   Web Management Tools and World Wide Web Services are enabled automatically.

3. From the root (your system name and user), select Features View.

4. In the IIS section, launch ISAPI and CGI Restrictions.

5. Select Edit Feature Settings and enable Allow unspecified CGI modules and then click OK.

6. Add your aliases. For example, c10_location,c10_location/cgi-bin.

7. Select your cgi-bin alias and ensure that Features View is selected.

8. Right-click Application Pools and select Add.

9. In the dialog box, enter a Web alias and the corresponding path to IBM Cognos BI webcontent.
10. Repeat steps 8 and 9 to add the next Web alias.

11. Select Default Web Site.

12. Open Handler Mappings.

13. Select the CGI-cgi mapping.

14. In the right pane, click Revert to Inherited.

15. Expand the application that points to your webcontent location.

16. Expand your cgi-bin application node.

17. Add a mapping that points to *.cgi and name it CGI-cgi.

18. Select the CGI-cgi mapping.

19. In the right pane, click Revert to Inherited.

20. Restart the IIS server.

21. Find the folder that contains cgi-bin (c10_location/cgi-bin) and right-click it.

22. Select the Security tab.

23. Add the Network Services user, granting all permissions except Full Control.

24. Right-click on Cognos service and select Properties.

25. Click the Log On tab.

26. Click This account and enter Network Service as the user.

27. Delete the Password and the Confirm the password values.

28. Click OK.

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.

On a Microsoft® Windows® operating system, the IBM Cognos service is configured to start automatically by default. On UNIX® and Linux® operating systems, to start the IBM Cognos BI process automatically, you must configure the process as a daemon. For more information, see your operating system documentation.

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.
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" (p. 49).

Steps
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 logging database.
   If you are using the notification database and the mail server, they are tested as well.
   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 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.

Steps
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 connection to the IBM Cognos BI portal by typing the Gateway URI value from IBM Cognos Configuration.

   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 Computers

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.

Steps
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.

   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.

Configure the IBM Cognos Series 7 Migration Service for Migrations from Upfront in Distributed IBM Cognos Series 7 Installations

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.

Notes

- 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.

Steps

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,
     ```xml
     <series7-shared-location description="Path to shared folder">\bott93\share\s7migration</series7-shared-location>
     ```
   - Save and close the file.

3. Restart the IBM Series 7 migration service.

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.

Step

- 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/mig7` directory and start the service by typing `./configure.sh --start`
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 on Microsoft® Windows®.

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.

● 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

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.

Steps

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:
   
   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:
     
     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
Uninstall IBM Cognos Business Intelligence on Windows

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.

Steps

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.

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.

Uninstall Cognos Content Database

If you want to uninstall only Cognos® Content Database and leave other IBM® Cognos Business Intelligence components on your computer, you must use the following procedure. After you
uninstall Cognos Content Database you must configure a new content store before you can restart the IBM Cognos service.

If you installed only Cognos Content Database, use the procedure to uninstall IBM Cognos BI on a UNIX® or Linux® operating system or the procedure to uninstall IBM Cognos BI on a Microsoft® Windows® operating system.

**Steps**

1. On the computer where you installed Cognos Content Database, go to the `c10_location/bin` directory, and type the following command:
   - On Windows, type `derby.bat uninstall`
     
     This command removes the Cognos Content Database service.
   - On UNIX, type `derby.sh stop`
     
     This command stops the Cognos Content Database service.

2. In the `c10_location` directory, delete the `derby10.1.2.1` directory.

3. In the `c10_location/bin` directory, delete the following files:
   - On Windows, `derby.bat`
   - On UNIX, `derby.sh` and `derbyenv.sh`

4. On Windows, in the `c10_location/logs` directory, delete the `derby.service` file.

5. In the `c10_location` directory, open the `cmplst.txt` file in a text editor.

6. Remove lines containing Cognos Content Database values. The lines contain CCD and CMDERBY. For example:
   
   ```
   C8BISRVRCCD_version=
   C8BISRVRCCD_name=
   CCD_version=
   CCD_name=
   CMDERBY_version=
   CMDERBY_name=
   ```

   **Tip:** You can also comment the lines out by inserting `#` at the start of each line.

7. Save the file.

8. Start IBM Cognos Configuration.

9. Under **Data Access, Content Manager**, do the following:
   - Delete the Cognos Content Database.
Configure a new database resource to point to a new content store.

For more information, see "Set Up Database Connectivity for the Content Store Database" (p. 129).

10. Restart IBM Cognos BI.

Uninstall the Migration Components

The IBM® Cognos® BI migration components are uninstalled when you uninstall IBM Cognos BI. You can not uninstall only the migration components from your IBM Cognos BI installation.

You can uninstall the IBM Series 7 migration components separately from your IBM Cognos Series 7 installation. After you complete the migration from IBM Cognos Series 7, you can choose to uninstall the migration components from each IBM Cognos Series 7 computer. However, the migration components are only active during a migration and will not affect your IBM Cognos Series 7 installation if you choose to not uninstall the migration components.

Step

- On the IBM Cognos Series 7 computers, uninstall the IBM Cognos Report Migration from Series 7 component.

  For more information about uninstalling IBM Cognos Series 7 components, see the IBM Cognos Series 7 Solution Installation Guide.
Chapter 7: Installing and Configuring IBM Cognos PowerPlay 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 IBM Cognos® PowerPlay® 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 BI Server first. Both IBM Cognos PowerPlay and IBM Cognos BI Server must be the same version. For more information about distributed installation options and configuration requirements, see "IBM Cognos Products That Interoperate with IBM Cognos PowerPlay" (p. 31).

The IBM Cognos PowerPlay installation includes components that support the migration of PowerPlay content from IBM Cognos Series 7 to IBM Cognos BI. If you install IBM Cognos PowerPlay with IBM Cognos BI, the migration components also support the option to open a PowerPlay Studio report in Analysis Studio or Report Studio.

The IBM Cognos PowerPlay server components include the following:

- **Content Manager**
- **Application tier Components: PowerPlay Server and PowerPlay Administration**
  PowerPlay Administration, which appears in IBM Cognos Administration, allows you to configure options for migration and for PowerPlay reports and cubes. For more information, see the IBM Cognos PowerPlay Migration and Administration Guide.
- **Gateway**
  You must install the gateway on a computer that is also running a web server.
- **Cognos Content Database**
  If you are installing components on several computers, you need to only install one Cognos Content Database. If you install Cognos Content Database on the same computer as Content Manager, and you later decide to use another database for your content store, you must uninstall Cognos Content Database.
- **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 also install the IBM Cognos Series 7 migration components on the computer where Upfront is installed.

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 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:

- web servers that host IBM Cognos BI content
- 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 SDK applications that are running

**Upgrading your Installation**

If you are upgrading from a previous release of IBM Cognos products, you must use the upgrading steps (p. 53).

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® 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® 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 permis-
sions within the directories. However, run-time generated files, such as logs, respect the mask. Use umask 022 on the installation directory.

**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.

The sequence to stop services is also important. Stop the Application Tier Components first, followed by the standby Content Manager, and then the active Content 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" (p. 115).

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" (p. 115).

### 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" (p. 117).

In installations with multiple Content Managers, configure IBM Cognos BI to use an ISAPI gateway instead of the default CGI gateway. 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.

Use the following checklist to guide you through the required configuration tasks for the Content Manager computers.

- Install Content Manager.
- Update the Java environment.
- Set up the database connectivity for the content store database.
- Configure the Content Manager installation.
- Test the Content Manager installation.

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. A 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 want to use Cognos Content Database, select that component too unless you want to install it on a separate server.

If you are installing IBM® Cognos® PowerPlay® to work with IBM Cognos Business Intelligence, install the PowerPlay Content Manager components on the same computers that include the IBM Cognos BI 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, select it in the installation wizard. If you are installing components on several computers, you need to only install one Cognos Content Database. If you install Cognos Content Database on the same computer as Content Manager, and you later decide to use another database for your content store, you must uninstall Cognos Content Database.

Steps for UNIX and Linux

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 IBM Java, to run on Linux®.

   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® operating systems.
4. On AIX, 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 (p. 323).

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 ReportNet or 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.

If you are installing in a directory that contains other IBM Cognos BI components, you are prompted to create backup copies of the files that will be replaced.

- 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/bin directory, or by running a silent configuration or editing cogstartup.xml in c10_location/configuration 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

11. On Linux, set the PRINTER environment variable to the name of your printer.

If you want to install Cognos Content Database on a separate computer, run the installation wizard on your database server and select only the Cognos Content Database component.

If you want users to see product documentation in a language other than English, you must install the Supplementary Language Documentation in the same location as the Gateway components. For more information, see "Install Translated Product Documentation" (p. 177).

**Steps for Windows**

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 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® web servers do not support non-ASCII characters in directory names.
     If you are installing IBM Cognos BI on a computer that has ReportNet or 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.
     If you are installing in a directory that contains other IBM Cognos BI components, you are prompted to create backup copies of the files that will be replaced.
   - 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.
   - 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 the Windows Start menu to start IBM Cognos Configuration from the shortcut folder.
   - Click Finish.

If you want to install Cognos Content Database on a separate computer, run the installation wizard on your database server and select only the Cognos Content Database component.

If you want users to see product documentation in a language other than English, you must install the Supplementary Language Documentation in the same location as the Gateway components. For more information, see "Install Translated Product Documentation" (p. 177).
Install Cognos Content Database on a Separate Server

If you want to install Cognos® Content Database on a separate server, you must do so before you configure Content Manager. In the installation wizard, clear all components and select only Cognos Content Database.

Steps

1. On your database server, insert the disk for your IBM® Cognos product.
   On UNIX® or Linux® operating systems, mount the disk using Rock Ridge file extensions.

2. If the Welcome page does not appear, start the installation wizard:
   - On UNIX or Linux, from the directory for your operating system, type ./issetup
   - On a Microsoft® Windows® operating system, in the win32 directory on the disk, double-click issetup.exe.

3. Follow the directions in the installation wizard and copy the required files to your computer.
   Install 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 the components, clear all components and then select Cognos Content Database.

4. In the Finish page of the installation wizard, 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 Business Intelligence components.

If a fix pack becomes available after your IBM Cognos product has been deployed, you must stop the service, install the fix pack in the same location as the IBM Cognos BI components, and then start the service.


IMPORTANT: Fix packs are not standalone installations. You must install them on computers that have IBM Cognos BI server components installed. Install the fix pack or 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 C8BISRVR_version=.

Before you install the fix pack, create a backup of the content store database. In addition, back up any customized files from the current installation.

Steps for the Microsoft Windows Operating System

1. If your IBM Cognos BI product is running, open IBM Cognos Configuration and stop the IBM Cognos service.

2. Back up the content store database.

3. If your IBM Cognos BI environment is customized, back up the entire IBM Cognos BI location.
4. Insert the disk for the Microsoft® Windows® operating system fix pack or go to the location where you downloaded and extracted the files.
   If more than one fix pack is available, install the fix pack with the lowest version number first.

5. On the disk or in the download location, go to the win32 directory and double-click the issetup.exe file.

6. Follow the directions in the installation wizard, installing in the same location as your existing IBM Cognos BI server components.
   The issetup program prompts you to allow the fix pack to create a backup copy in the installation folder before copying new files.

7. If an updater is available, do the following:
   • To install from a disk, insert the updater disk for the Windows operating system.
   • To install from a download, follow the instructions on the support site and then go to the location where you downloaded and extracted the files.
   • Within the updater directory on the disk or download location, go to the win32 directory and double-click the issetup.exe file.
   • Follow the directions in the installation wizard.

8. To return a deployed IBM Cognos BI product to service, open IBM Cognos Configuration, save the configuration, and then start the IBM Cognos service.

9. If you have a distributed environment, repeat these steps for all remaining IBM Cognos BI servers.

10. If you are running the IBM Cognos BI product on an application server other than the default, Tomcat, redeploy the IBM Cognos BI product to the application server.
    For instructions, see "Configure Application Server Properties and Deploy IBM Cognos Components" (p. 302).

### Steps for the UNIX and Linux Operating Systems

1. If your IBM Cognos BI product is running, open IBM Cognos Configuration and stop the IBM Cognos service.

2. Back up the content store database.

3. If your IBM Cognos BI environment is customized, back up the entire IBM Cognos BI location.

4. If using a disk, mount the fix pack disk that is appropriate for your UNIX® or Linux® operating system, using Rock Ridge file extensions.

**Important:** To mount the IBM Cognos 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.

5. If using a download, go to the location where you downloaded and extracted the fix pack files. If more than one fix pack is available, install the fix pack with the lowest version number first.

6. To start the installation wizard, type

   ```
   ./issetup
   ```

   If you do not use XWindows, run an unattended installation (p. 323).

7. Follow the directions in the installation wizard to install to the same location as your existing IBM Cognos BI server components.

   The issetup program prompts you to allow the fix pack to create a backup copy in the installation folder before copying new files.

8. If an updater is available, do the following:

   - To install from a disk, mount the updater disk that is appropriate for your operating system, using Rock Ridge file extensions.

     **Important:** To mount the disk on HP-UX, follow the bulleted instructions in step 4.

   - To install from a download, go to the location where you downloaded and extracted the updater files.

   - To start the installation wizard, type

     ```
     ./issetup
     ```

     If you do not use XWindows, run an unattended installation (p. 323).

   - Follow the directions in the installation wizard to install to the same location as your existing IBM Cognos BI server components.

9. To return a deployed IBM Cognos BI product to service, open IBM Cognos Configuration, save the configuration, and then start the IBM Cognos service.

10. If you have a distributed environment, repeat these steps for all remaining IBM Cognos BI servers.
11. If you are running the IBM Cognos BI product on an application server other than the default, Tomcat, redeploy the IBM Cognos BI product to the application server. For instructions, see "Configure Application Server Properties and Deploy IBM Cognos Components" (p. 302).

Create a Database for a DB2 Content Store on Linux Using a Script

A script named C8DB2.sh is provided to allow you to create a content store database in DB2 on Linux®. The script is located in the c10_location\C8SE directory after you install IBM® Cognos® Business Intelligence.

DB2 must be installed and configured before you run the script. The script creates and configures a database that you can use as your content store. For more information about the minimum settings for a DB2 content store, see "Suggested Settings for Creating the Content Store in DB2 on Linux, Windows and UNIX" (p. 42).

Permissions

To run the script you must be a member DB2 group named dasadm1. When you run the script you are prompted for a user account that will be given the required privileges to access and write to the database. When you configure the content store connection information for IBM Cognos BI, use the user account that you enter when you run the script, not the user account you use to run the script.

The script creates the database in the first DB2 instance in your path. If you have more than one DB2 instance, ensure that the DB2 instance in which you want to create the content store appears first in your path.

Steps

1. From the c10_location\C8SE directory where you installed IBM Cognos BI, copy the C8DB2.sh script to your database server.

2. On your database server computer, change to a user who is a member of the DB2 group named dasadm1.

3. Run the script using the following command:
   
   `./C8DB2.sh`

   You are prompted for the following information:
   
   • a name for the content store database
   
   • a user who will be granted the required privileges to access and write to the content store database

   When you set the database connection properties for the content store, you must enter this user in the User ID and password property.

   When the script has finished, a database will be created in DB2 that you can use as your content store database.
Create Tablespaces for a DB2 Content Store on z/OS

A database administrator must run a script to create a set of tablespaces required for the content store database. The script must be modified to replace the placeholder parameters with ones that are appropriate for your environment.

If you are using the same DB2 database on z/OS for both the content store and notification (the default setup), then you must run scripts to create the notification tablespaces at the same time that you create the content store tablespaces.

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. For more information, see the IBM® DB2 Information Center.

Steps

1. Connect to the database as a user with 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. Open the tablespace_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>CMSCRIPT_CREATE_IN</td>
<td>Specifies the base tables location. For example, databaseName.baseTablespaceName</td>
</tr>
<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 instance identification for the content store database.</td>
</tr>
<tr>
<td></td>
<td>The ID must not be longer than two characters.</td>
</tr>
<tr>
<td>CMSCRIPT_TABLESPACE</td>
<td>Specifies the name of the tablespace that will contain all of the base tables in the content store. Auxiliary tables are not included. The name cannot be longer than six characters.</td>
</tr>
<tr>
<td>CMSCRIPT_LARGE_BP</td>
<td>Specifies the name of the large buffer pool allocated for especially large objects.</td>
</tr>
<tr>
<td>CMSCRIPT_REGULAR_BP</td>
<td>Specifies the name of the regular size buffer pool allocated for regular and large objects.</td>
</tr>
</tbody>
</table>
4. Save and run the script.

5. Grant the IBM Cognos® user rights to the tablespaces that were created when you ran the tablespace_db2zOS.sql file script:
   - In the remote access tool, open the rightsGrant_db2zOS.sql script file and replace the placeholder parameters with values that are appropriate for your environment.
     
     **Tip:** Ensure that you use the same values that you used when you allocated resources to the buffer pools and user account.
   - Save and run the file.

6. Replace placeholder parameters in the following scripts and run them:
   - dbInitTest_db2zOS.sql
   - dbInitMeta_db2zOS.sql
   - dbInitScript_db2zOS.sql
   - dbInitLock_db2zOS.sql

7. If you are using the same database for notification that you use for the content store (the default setup), perform steps 7 to 10.

8. Open the NC_TABLESPACES.sql script file and use the following table to help you to replace the placeholder parameters with ones that are 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 content store database.</td>
</tr>
<tr>
<td>DSN8G810</td>
<td>Specifies the name of the storage group used for the content store database.</td>
</tr>
<tr>
<td>BP32K</td>
<td>Specifies the name of the buffer pool used for the tablespaces.</td>
</tr>
</tbody>
</table>

For parameters that are not in the script, add them.

9. Save and run the script.

10. Open the NC_CREATE.sql script file and replace the NCCOG placeholder parameter with the name of the content store database.
11. Save the script.

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

   The content store database is created. You can now configure a database connection.

**Update the Java Environment**

You can use an existing Java™ Runtime Environment (JRE) or the JRE that is provided with IBM® Cognos® Business Intelligence. To support the cryptographic services in IBM Cognos BI, you may be required to update or set a JAVA_HOME environment variable. Depending on your security policy, you may also have to install the unrestricted Java Cryptography Extension (JCE) policy file.

**JAVA_HOME**

If you want to use your own JRE and have JAVA_HOME set to that location on Microsoft® Windows® or if you are installing on UNIX® or Linux®, you must update JAVA_HOME for the cryptographic services.

On Windows, you can set JAVA_HOME as a system variable or a user variable. If you set it as a system variable, it may be necessary to restart your computer for it to take effect. If you set it as a user variable, set it so that the environment in which Tomcat is running can access it.

If you do not have a JAVA_HOME variable already set on Windows, the JRE files provided with the installation will be used, and you do not have to update any files in your environment. If JAVA_HOME points to a Java version that is not valid for IBM Cognos BI, you must update JAVA_HOME with the path to a valid Java version.

**Unrestricted JCE Policy File**

Whether you use the default Windows JRE or download a JRE for UNIX or Linux, the JRE includes a restricted policy file that limits you to certain cryptographic algorithms and cipher suites. If your security policy requires 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.

**Steps**

1. Ensure that the JAVA_HOME environment variable is set to the JRE location.
   
   For example, to set JAVA_HOME to a JRE that you are already using, the path is `Java_location/bin/jre/version`.

2. If your security policy requires it, download and install the unrestricted JCE policy file.
   
   For IBM Java, the unrestricted JCE policy file is available from the following location: `https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source-jcesdk`

   You may have to complete additional configuration for cryptographic settings. For more information, see "Configuring Cryptographic Settings" (p. 225).
Set Up Database Connectivity for the Content Store Database

If you are using a database other than Cognos® Content Database 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.

Steps for DB2

1. If you are using a type 2 JDBC connection, install the DB2® client software on the Content Manager computers.
   
   If you are using a type 4 JDBC connection for DB2, you are not required to install the DB2 client software where Content Manager is installed. If you use a DB2 database on z/OS® for the content store, you must use a type 4 JDBC connection.
   
   For more information about the differences between type 2 and type 4 drivers, see "JDBC Driver Options for Using DB2 Database as a Content Store" (p. 90).

2. If you are using a type 2 JDBC connection, and the content store is on a different computer than Content Manager, configure a database alias to the content store.
   
   On Microsoft® Windows® operating systems, run the DB2 Client Configuration Assistant.
   
   On UNIX® or Linux® operating systems, use the DB2 command line interface.
   
   If the content store database and Content Manager are on the same computer, the content store name automatically becomes the alias.
   
   When you configure the Content Manager computers, ensure that they are all configured to use the same content store.

3. On Windows, stop the DB2 services and the HTML Search Server.

4. Copy the following files from DB2_installation/sqlib/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, db2jcc_license_cu.jar
     
     for DB2 on z/OS, 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

5. On Windows, restart the DB2 services and the HTML Search Server.

6. On UNIX, if you are using a type 2 JDBC connection, ensure that the 32-bit DB2 libraries are in the library search path, which is usually the $DB2DIR/lib directory or the $DB2DIR/lib32 directory.
7. Repeat this entire procedure on the IBM Cognos BI computers where Content Manager is installed or where notification is sent to a DB2 database.

You can tune the database to take advantage of DB2 features. For more information, see the "Tuning a DB2 Content Store" (p. 333).

**Steps for Oracle**

1. On the computer where the Oracle client is installed, go to the ORACLE_HOME/jdbc/lib directory.

2. Copy the ojdbc5.jar file to the c10_location/webapps/p2pd/WEB-INF/lib directory on computers where Content Manager is installed and where notification is sent to an Oracle database.

   If the directory contains the classes12.jar file or ojdbc14.jar file, delete it before installing the ojdbc5.jar file.

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

**Steps for Informix**

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

**Steps for Sybase**

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 the configuration tool, IBM® Cognos® Configuration, to configure IBM Cognos Business Intelligence components during the installation and configuration process and 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 environment variables have been set.

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. 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.

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" (p. 49).

**Steps on UNIX or Linux**

1. Go to the `c10_location/bin` directory and then type
   
   `/cogconfig.sh`

2. If you want to access the help for IBM Cognos Configuration, go to the `c10_location/configuration` directory and edit the cogconfig.prefs file to add the location of your Web browser.

   For example, if you use Firefox, add the following text to the file:

   ```
   BrowserPath=Web_browser_location/firefox
   ```

   where `Web_browser_location` is a path, such as `/usr/local/bin/

   Your Web browser must support the following syntax:

   ```
   $ <Web_browser_location> <URL>
   ```

**Step on Windows**

1. From the **Start** menu, click **Programs > IBM Cognos 10 > IBM Cognos Configuration**.

2. If you want to access the help for IBM Cognos Configuration, go to the `c10_location/configuration` directory and edit the cogconfig.prefs file to add the location of your Web browser.

   For example, if you use Firefox, add the following text to the file:

   ```
   BrowserPath=Web_browser_location\firefox
   ```

   where `Web_browser_location` is a path, such as `\usr\local\bin\`

   Your Web browser must support the following syntax:

   ```
   $ <Web_browser_location> <URL>
   ```

**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.

In a production environment, you must use an enterprise-level database for your content store. If you have been using Cognos Content Database in a test or proof-of-concept system, you can use the features in the administration portal to back up and archive the data before moving to an enterprise-level 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.
If Cognos Content Database is on the same computer as Content Manager in your production environment, then after you configure your IBM Cognos BI product to use an enterprise-level database for the content store, you must uninstall Cognos Content Database.

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.

Ensure that you used one of the supported database servers to create the content store.

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" (p. 49).

Steps for DB2® on Linux®, UNIX®, or Microsoft® Windows® Operating Systems

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.
   - Type the appropriate values and click OK.
5. To use a type 4 JDBC connection, for the Database server and port number property, type a value, using host:port syntax.
   - If you leave this property blank, a type 2 JDBC connection is used.
   For more information about the differences between the driver types, see "JDBC Driver Options for Using DB2 Database as a Content Store" (p. 90).
6. From the File menu, click Save.
   - The logon credentials are immediately encrypted.
7. To test the connection between Content Manager and the content store database, from the Actions menu, click Test.
   - Content Manager connects to the database, checks the database permissions, and creates and populates a table. The table is not deleted and is used each time that the test is repeated.

Steps for DB2 on z/OS

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. 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. To use a type 4 JDBC connection, for the **Database server and port number** property, type a value, using *host:port* syntax.
   - To connect to DB2® on z/OS®, you must use a type 4 JDBC connection.
   - For more information about the differences between the driver types, see "**JDBC Driver Options for Using DB2 Database as a Content Store**" (p. 90).

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

7. In the Properties window, next to **Advanced properties**, click inside the **Value** box, and then click the edit button.
   - The **Value - Advanced properties** dialog box appears.

8. To add the parameters that you used to create the tablespaces, click **Add**.
   - All of the parameters except CMSCRIPT_USERNAME are added.

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

10. To test the connection between Content Manager and the content store database, from the **Actions** menu, click **Test**.
    - This tests the connection between Content Manager and the content store database.

**Steps for Microsoft SQL Server, Oracle, Informix, and Sybase**

1. On the computer where you installed Content Manager, start IBM Cognos Configuration.

2. In the Explorer window, under **Data Access, Content Manager**, right-click **Content Store** and click **Delete**.
   - This 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**.
If you installed more than one version of IBM Cognos BI, you must use a different content store for each version. When a content store is used by a new version of IBM Cognos BI, it cannot be used by an older version.

**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 values depending on 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.

  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`

  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 **Service name** 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:
Chapter 7: Installing and Configuring IBM Cognos PowerPlay Server Components on Different Computers

- Click the **Value** box next to the **User ID and password** property and then click the edit button 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 button.
   
   - 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.

10. To test the connection between Content Manager and the content store database, from the **Actions** menu, click **Test**.

    Content Manager connects to the database, checks the database permissions, and creates and populates a table. The table is not deleted and is used each time that the test is repeated.

    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® 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 so that they better suit your environment. For example, you can configure IBM Cognos BI components to use an authentication provider, enable and disable services on the Content Manager computers, or change global settings.
Note that if you change global settings on one Content Manager computer, you must make the same changes on the other Content Manager computers.

**Steps for the First Content Manager Computer**

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 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**.

**Steps for Standby Content Manager Computers**

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 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.

  10. From the File menu, click Save.

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.

Steps

  1. In the Explorer window, under Data Access, click Notification.

  2. In the Properties window, for the SMTP mail server property, type the host name and port of your SMTP (outgoing) mail server.

Tips

  To be able to open reports that are sent by email, you must 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.

  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.
3. Click the Value box next to the Account and password property and then click the edit button when it appears.

4. 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 Yes. Ensure that the default user name has been removed. Otherwise, the default account is used and notifications will not work properly.

5. In the Properties window, type the appropriate value for the default sender account.

6. Test the mail server connections. In the Explorer window right-click Notification and click Test.

   IBM Cognos Business Intelligence tests the mail server connection.

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.

**Steps**

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.

   For more information about configuring IBM Cognos BI to use an authentication provider, see "Configuring IBM Cognos Components to Use an Authentication Provider" (p. 181).

   For more information about configuring IBM Cognos BI to use an authentication provider, see "Configuring IBM Cognos BI Components to Use an Authentication Provider" in the Installation and Configuration Guide.

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 "Configuring IBM Cognos Components to Use an Authentication Provider" (p. 181).

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.

Steps

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 button.
   - 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.

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" (p. 49).

**Steps**

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 logging database.

   If you are using the notification database and the mail server, they are tested as well.

   **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.

Steps
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.
   
   The State value should be Running.

Installing and Configuring Application Tier Components

You can install Application Tier Components on one or more IBM® Cognos® PowerPlay® servers in your environment. Application Tier Components include PowerPlay Server and PowerPlay Administration. Both components 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 BI, 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.

If Content Manager and the Application Tier Components are installed on separate computers, on the Application Tier Components computer, you must do the following:

- Install Application Tier Components.
- Configure Application Tier Components.
- Start the IBM Cognos service.
- Test the IBM Cognos migration service.

Other configuration tasks are optional and may be performed later.

**Install the Application Tier Components**

Application Tier Components include PowerPlay® Server and PowerPlay Administration. You can install Application Tier Components on one or more computers, depending on your environment. If you are upgrading from 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.

**Printer Requirements**

To ensure that reports print properly on Microsoft® 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.

**Steps for UNIX and Linux**

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 IBM Java, to run on Linux®.

   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® operating systems.

4. On AIX, if you are using a servlet gateway, set the AIXTHREAD_SCOPE environment variable as follows:

\[
\text{AIXTHREAD_SCOPE=S}
\]

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,
  
  \[
  \text{PATH=/usr/sbin:/$PATH}
  \]
  
  \[
  \text{export PATH}
  \]

- To start the required NFS daemons and run the daemons in the background, type \text{bg pfs_mountd} and then type \text{bg pfsd}

- To mount the drive, type

  \[
  \text{pfs\_mount -t rrip <device><mount\_dir> -o xlat=unix}
  \]

  For example,

  \[
  \text{pfs\_mount /dev/dsk/c0t2d0 /cdrom -o xlat=unix}
  \]

  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 \text{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 \text{/issetup}

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

If you do not use XWindows, run an unattended installation (p. 323).

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.

If you are installing IBM Cognos BI on a computer that has ReportNet or 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.

If you are installing in a directory that contains other IBM Cognos BI components, you are prompted to create backup copies of the files that will be replaced.

- When selecting components, clear all components except **Application Tier Components**.

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 cog-config.sh in the `c10_location/bin` directory, or by running a silent configuration or editing cogstartup.xml in `c10_location/configuration` 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`

11. On Linux, set the `PRINTER` environment variable to the name of your printer.

If you want users to see product documentation in a language other than English, you must install the Supplementary Language Documentation in the same location as the Gateway components. For more information, see "Install Translated Product Documentation" (p. 177).

**Steps for Windows**

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`.

---

144 IBM Cognos Business Intelligence PowerPlay
• 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.
     If you are installing IBM Cognos BI on a computer that has ReportNet or 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.
     If you are installing in a directory that contains other IBM Cognos BI components, you are prompted to create backup copies of the files that will be replaced.
   • 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.
   • 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 the Windows Start menu to start IBM Cognos Configuration from the shortcut folder.
   • Click Finish.

If you want users to see product documentation in a language other than English, you must install the Supplementary Language Documentation in the same location as the Gateway components. For more information, see "Install Translated Product Documentation" (p. 177).

**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 Business Intelligence components.

If a fix pack becomes available after your IBM Cognos product has been deployed, you must stop the service, install the fix pack in the same location as the IBM Cognos BI components, and then start the service.

IMPORTANT: Fix packs are not standalone installations. You must install them on computers that have IBM Cognos BI server components installed. Install the fix pack or 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 `C8BISRVR_version=`.

Before you install the fix pack, create a backup of the content store database. In addition, back up any customized files from the current installation.

Steps for the Microsoft Windows Operating System

1. If your IBM Cognos BI product is running, open IBM Cognos Configuration and stop the IBM Cognos service.

2. Back up the content store database.

3. If your IBM Cognos BI environment is customized, back up the entire IBM Cognos BI location.

4. Insert the disk for the Microsoft® Windows® operating system fix pack or go to the location where you downloaded and extracted the files.
   If more than one fix pack is available, install the fix pack with the lowest version number first.

5. On the disk or in the download location, go to the win32 directory and double-click the `issetup.exe` file.

6. Follow the directions in the installation wizard, installing in the same location as your existing IBM Cognos BI server components.
   The `issetup` program prompts you to allow the fix pack to create a backup copy in the installation folder before copying new files.

7. If an updater is available, do the following:
   • To install from a disk, insert the updater disk for the Windows operating system.
   • To install from a download, follow the instructions on the support site and then go to the location where you downloaded and extracted the files.
   • Within the updater directory on the disk or download location, go to the win32 directory and double-click the `issetup.exe` file.
   • Follow the directions in the installation wizard.

8. To return a deployed IBM Cognos BI product to service, open IBM Cognos Configuration, save the configuration, and then start the IBM Cognos service.

9. If you have a distributed environment, repeat these steps for all remaining IBM Cognos BI servers.

10. If you are running the IBM Cognos BI product on an application server other than the default, Tomcat, redeploy the IBM Cognos BI product to the application server.
Steps for the UNIX and Linux Operating Systems

1. If your IBM Cognos BI product is running, open IBM Cognos Configuration and stop the IBM Cognos service.

2. Back up the content store database.

3. If your IBM Cognos BI environment is customized, back up the entire IBM Cognos BI location.

4. If using a disk, mount the fix pack disk that is appropriate for your UNIX® or Linux® operating system, using Rock Ridge file extensions.

   **Important:** To mount the IBM Cognos 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.

5. If using a download, go to the location where you downloaded and extracted the fix pack files.
   If more than one fix pack is available, install the fix pack with the lowest version number first.

6. To start the installation wizard, type
   ```
   ./issetup
   ```
   If you do not use XWindows, run an unattended installation (p. 323).

7. Follow the directions in the installation wizard to install to the same location as your existing IBM Cognos BI server components.
   The issetup program prompts you to allow the fix pack to create a backup copy in the installation folder before copying new files.

8. If an updater is available, do the following:
To install from a disk, mount the updater disk that is appropriate for your operating system, using Rock Ridge file extensions.

**Important:** To mount the disk on HP-UX, follow the bulleted instructions in step 4.

- To install from a download, go to the location where you downloaded and extracted the updater files.
- To start the installation wizard, type
  
  `/issetup`

  If you do not use XWindows, run an unattended installation (p. 323).

- Follow the directions in the installation wizard to install to the same location as your existing IBM Cognos BI server components.

9. To return a deployed IBM Cognos BI product to service, open IBM Cognos Configuration, save the configuration, and then start the IBM Cognos service.

10. If you have a distributed environment, repeat these steps for all remaining IBM Cognos BI servers.

11. If you are running the IBM Cognos BI product on an application server other than the default, Tomcat, redeploy the IBM Cognos BI product to the application server.

   For instructions, see "Configure Application Server Properties and Deploy IBM Cognos Components" (p. 302).

### Start IBM Cognos Configuration

Use the configuration tool, IBM® Cognos® Configuration, to configure IBM Cognos Business Intelligence components during the installation and configuration process and 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 environment variables have been set.

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. 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.

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" (p. 49).

### Steps on UNIX or Linux

1. Go to the `c10_location/bin` directory and then type

   `/cogconfig.sh`
2. If you want to access the help for IBM Cognos Configuration, go to the c10_location/configuration directory and edit the cogconfigprefs file to add the location of your Web browser.

   For example, if you use Firefox, add the following text to the file:
   
   **BrowserPath=Web_browser_location/firefox**
   
   where *Web_browser_location* is a path, such as /usr/local/bin/

   Your Web browser must support the following syntax:
   
   $ <Web_browser_location> <URL>

---

**Step on Windows**

1. From the **Start** menu, click **Programs > IBM Cognos 10 > IBM Cognos Configuration**.

2. If you want to access the help for IBM Cognos Configuration, go to the c10_location/configuration directory and edit the cogconfigprefs file to add the location of your Web browser.

   For example, if you use Firefox, add the following text to the file:
   
   **BrowserPath=Web_browser_location/firefox**
   
   where *Web_browser_location* is a path, such as /usr/local/bin/

   Your Web browser must support the following syntax:
   
   $ <Web_browser_location> <URL>

---

**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" (p. 240).

If you installed more than one Content Manager, you must list all Content Manager URIs on each Application Tier Components computer.

**Steps**

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 dashboards 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.

To use IBM® Cognos® Business Intelligence 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" (p. 49).

Steps

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 logging database.
If you are using the notification database and the mail server, they are tested as well.

**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.

**Steps**

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

   If the response includes the string State: Running, the dispatcher is available.

### 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.

**Steps**

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 button appears on the toolbar.

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 Component

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. 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 component.
- Configure the Gateway component.
- Configure the web server.
- Test the Gateway computer.

Install the Gateway Components

You can install the gateway on one or more web server computers.

If you are installing PowerPlay to work with IBM Cognos BI, install the PowerPlay gateway components on the same computers that include the IBM Cognos BI gateway components.

Steps for UNIX and Linux

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 IBM Java, to run on Linux®.
   
   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® operating systems.

4. On AIX, 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,
     
     ```bash
     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
     
     ```bash
     pfs_mount -t rrip <device><mount_dir> -o xlat=unix
     ```
     
     For example,
     
     ```bash
     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 (p. 323).

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.

     If you are installing IBM Cognos BI on a computer that has ReportNet or 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.
If you are installing in a directory that contains other IBM Cognos BI components, you are prompted to create backup copies of the files that will be replaced.

- 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 cog-config.sh in the c10_location/bin directory, or by running a silent configuration or editing cogstartup.xml in c10_location/configuration 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

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 "Install Translated Product Documentation" (p. 177).

**Steps for Windows**

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 Windows® web servers do not support non-ASCII characters in directory names.
     If you are installing IBM Cognos BI on a computer that has ReportNet or 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.
     If you are installing in a directory that contains other IBM Cognos BI components, you are prompted to create backup copies of the files that will be replaced.
   - 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.
   - 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 the Windows Start menu to start IBM Cognos Configuration from the shortcut folder.
   - 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 "Install Translated Product Documentation" (p. 177).

### 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 Business Intelligence components.

If a fix pack becomes available after your IBM Cognos product has been deployed, you must stop the service, install the fix pack in the same location as the IBM Cognos BI components, and then start the service.


**IMPORTANT**: Fix packs are not standalone installations. You must install them on computers that have IBM Cognos BI server components installed. Install the fix pack or 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 `C8BISRVR_version=`.
Before you install the fix pack, create a backup of the content store database. In addition, back up any customized files from the current installation.

**Steps for the Microsoft Windows Operating System**

1. If your IBM Cognos BI product is running, open IBM Cognos Configuration and stop the IBM Cognos service.
2. Back up the content store database.
3. If your IBM Cognos BI environment is customized, back up the entire IBM Cognos BI location.
4. Insert the disk for the Microsoft® Windows® operating system fix pack or go to the location where you downloaded and extracted the files.
   If more than one fix pack is available, install the fix pack with the lowest version number first.
5. On the disk or in the download location, go to the win32 directory and double-click the isetup.exe file.
6. Follow the directions in the installation wizard, installing in the same location as your existing IBM Cognos BI server components.
   The isetup program prompts you to allow the fix pack to create a backup copy in the installation folder before copying new files.
7. If an updater is available, do the following:
   - To install from a disk, insert the updater disk for the Windows operating system.
   - To install from a download, follow the instructions on the support site and then go to the location where you downloaded and extracted the files.
   - Within the updater directory on the disk or download location, go to the win32 directory and double-click the isetup.exe file.
   - Follow the directions in the installation wizard.
8. To return a deployed IBM Cognos BI product to service, open IBM Cognos Configuration, save the configuration, and then start the IBM Cognos service.
9. If you have a distributed environment, repeat these steps for all remaining IBM Cognos BI servers.
10. If you are running the IBM Cognos BI product on an application server other than the default, Tomcat, redeploy the IBM Cognos BI product to the application server.
    For instructions, see "Configure Application Server Properties and Deploy IBM Cognos Components" (p. 302).

**Steps for the UNIX and Linux Operating Systems**

1. If your IBM Cognos BI product is running, open IBM Cognos Configuration and stop the IBM Cognos service.
2. Back up the content store database.
3. If your IBM Cognos BI environment is customized, back up the entire IBM Cognos BI location.

4. If using a disk, mount the fix pack disk that is appropriate for your UNIX® or Linux® operating system, using Rock Ridge file extensions.

   **Important:** To mount the IBM Cognos 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 pfssd`.
   - 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 `pfssd` and `pfs_mountd` daemons to unmount the disk.

5. If using a download, go to the location where you downloaded and extracted the fix pack files. If more than one fix pack is available, install the fix pack with the lowest version number first.

6. To start the installation wizard, type

   ```
   ./issetup
   ```

   If you do not use XWindows, run an unattended installation (p. 323).

7. Follow the directions in the installation wizard to install to the same location as your existing IBM Cognos BI server components.

   The issetup program prompts you to allow the fix pack to create a backup copy in the installation folder before copying new files.

8. If an updater is available, do the following:

   - To install from a disk, mount the updater disk that is appropriate for your operating system, using Rock Ridge file extensions.
     
     **Important:** To mount the disk on HP-UX, follow the bulleted instructions in step 4.
   - To install from a download, go to the location where you downloaded and extracted the updater files.
   - To start the installation wizard, type
Start IBM Cognos Configuration

Use the configuration tool, IBM® Cognos® Configuration, to configure IBM Cognos Business Intelligence components during the installation and configuration process and 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 environment variables have been set.

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. 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.

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" (p. 49).

Steps on UNIX or Linux

1. Go to the $c10_location/bin directory and then type
   
   ./cogconfig.sh

2. If you want to access the help for IBM Cognos Configuration, go to the $c10_location/configuration directory and edit the cogconfig.prefs file to add the location of your Web browser.
   
   For example, if you use Firefox, add the following text to the file:
   
   BrowserPath=Web_browser_location/firefox
   
   where Web_browser_location is a path, such as /usr/local/bin/
Chapter 7: Installing and Configuring IBM Cognos PowerPlay Server Components on Different Computers

Step on Windows
1. From the Start menu, click Programs > IBM Cognos 10 > IBM Cognos Configuration.

2. If you want to access the help for IBM Cognos Configuration, go to the c10_location/configuration directory and edit the cogconfig.prefs file to add the location of your Web browser.

   For example, if you use Firefox, add the following text to the file:

   **BrowserPath=Web_browser_location\firefox**

   where Web_browser_location is a path, such as \usr\local\bin\

   Your Web browser must support the following syntax:

   $ <Web_browser_location> <URL>

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. 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.

Steps
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.

$ <Web_browser_location> <URL>
This will ensure that users in different locations can connect to reports and dashboards that are sent by email.

**Tip:** If you want to send requests to the dispatcher from an SDK 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 SDK application or modeling tool that is outside the firewall. Ensure that you configure appropriate security for this dedicated gateway, such as SSL. 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**.

**Configure the Web Server**

For all installations, before you use web pages generated by IBM® Cognos® Business Intelligence, you must configure your web server. You must create virtual directories, or aliases, so that users can connect to IBM Cognos BI in the portal. If 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. The steps for creating an application pool vary depending on your operating system.

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®, the account under which the web server runs must have read access to the cogstartup.xml file in the \texttt{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.

**Steps to Create Virtual Directories**

1. Create the virtual directories from the following table:

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

   You can use a name other than ibmcognos in the aliases. However, you must use cgi-bin as the second part of the alias and you must change the virtual directory in the \texttt{Gateway URI} property to match the new IBM Cognos alias.

   For Apache Web Server, ensure that you define the ibmcognos/cgi-bin alias before the ibmcognos alias in the httpd.conf file located in the \texttt{Apache\_installation/conf} directory. The ibmcognos/cgi-bin alias must be defined as a ScriptAlias.

2. If you want to use Report Studio’s image browser, enable Web Distributed Authoring and Versioning (WebDAV) on your web server.

   If you use Apache Web Server, specify a directory in which to enable WebDAV. For information about configuring WebDAV, see your web server documentation.

   If you use Microsoft® Internet Information Services (IIS), enable the Read and Directory Browsing properties for the URL you want to access.

3. For IBM Cognos BI for reporting, set the content expiry on the \texttt{c10\_location/webcontent/pat/} images virtual directory in your web server.

   Each time a user opens Report Studio, their web browser checks with the web server to determine if images are current. Because there are over 600 images, this can result in excess network traffic. You can postpone this check until a specified date by using the content expiry feature of the web server.

   For information on setting content expiry, see the documentation for your web server.

   **Note:** When you upgrade, Report Studio users must clear their web browser cache to get the latest images.
If you use Web aliases other than ibmcognos, or your Web server is on another computer, or you are using Microsoft Internet Application Interface (ISAPI), apache_mod or a servlet gateway, change the Gateway URI when you configure IBM Cognos components.

**Steps to Create an Application Pool on Windows Server 2008**

1. For the Microsoft® Windows® operating system, from the Start menu, select Control Panel > Performance and Maintenance > Administrative Tools.
2. Launch Internet Information Services (IIS) Manager.
   
   Web Management Tools and World Wide Web Services are enabled automatically.
3. From the root (your system name and user), select Features View.
4. In the IIS section, launch ISAPI and CGI Restrictions.
5. Select Edit Feature Settings and enable Allow unspecified CGI modules and then click OK.
6. Add your aliases. For example, c10_location, c10_location/cgi-bin.
7. Select your cgi-bin alias and ensure that Features View is selected.
8. Right-click Application Pools and select Add.
9. In the dialog box, enter a Web alias and the corresponding path to IBM Cognos BI webcontent.
10. Repeat steps 8 and 9 to add the next Web alias.
11. Select Default Web Site.
12. Open Handler Mappings.
13. Select the CGI-cgi mapping.
14. In the right pane, click Revert to Inherited.
15. Expand the application that points to your webcontent location.
16. Expand your cgi-bin application node.
17. Add a mapping that points to *.cgi and name it CGI-cgi.
18. Select the CGI-cgi mapping.
19. In the right pane, click Revert to Inherited.
20. Restart the IIS server.
21. Find the folder that contains cgi-bin (c10_location/cgi-bin) and right-click it.
22. Select the Security tab.
23. Add the Network Services user, granting all permissions except Full Control.
24. Right-click on Cognos service and select Properties.
25. Click the Log On tab.
26. Click This account and enter Network Service as the user.

27. Delete the Password and the Confirm the password values.

28. Click OK.

**Test the Gateway**

You can test the installation using a Web browser.

**Steps**

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 Computers**

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.

**Steps**

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 isetup.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**.
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.

**Configure the IBM Cognos Series 7 Migration Service for Migrations from Upfront in Distributed IBM Cognos Series 7 Installations**

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.

**Notes**

- 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.

**Steps**

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,
     ```xml
     <series7-shared-location description="Path to shared folder">\bott93\share7\s7migration</series7-shared-location>
     ```
   - Save and close the file.

3. Restart the IBM Series 7 migration service.

   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.

Step
- 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

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 on Windows®.

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.
- 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 BI on UNIX or Linux

If you no longer require IBM Cognos BI or if you are upgrading, 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.

**Steps**

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:
   
   ```
   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:
     
     ```
     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
     
     ```
     ./uninst -u
     ```
   - If you do not use XWindows, do an unattended uninstallation (p. 323).

4. Follow the prompts to complete the uninstallation.

5. Delete all temporary Internet files from the web browser computers.

**Uninstall IBM Cognos BI on Windows**

If you no longer require IBM Cognos BI 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 Microsoft® Windows®. 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.

**Steps**

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.

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.

**Uninstall Cognos Content Database**

If you want to uninstall only Cognos Content Database and leave other IBM Cognos BI components on your computer, you must use the following procedure. After you uninstall Cognos Content Database you must configure a new content store before you can restart the IBM Cognos service.

If you installed only Cognos Content Database, use the procedure to uninstall IBM Cognos BI on UNIX or Linux or the procedure to uninstall IBM Cognos BI on Windows.

**Steps**

1. On the computer where you installed Cognos Content Database, go to the `c10_location\bin` directory, and type the following command:
   
   - On Windows, type
     ```
     derby.bat uninstall
     ```
     This command removes the Cognos Content Database service.
   - On UNIX, type
     ```
     derby.sh stop
     ```
     This command stops the Cognos Content Database service.

2. In the `c10_location` directory, delete the `derby10.1.2.1` directory.

3. In the `c10_location\bin` directory, delete the following files:
   
   - On Windows, `derby.bat`
   - On UNIX, `derby.sh` and `derbyenv.sh`
4. On Windows, in the `c10_location\logs` directory, delete the derby.service file.

5. In the `c10_location` directory, open the cmplst.txt file in a text editor.

6. Remove lines containing Cognos Content Database values. The lines contain CCD and CMDERBY. For example:
   
   ```
   C8BISRVRCCD_version=
   C8BISRVRCCD_name=
   CCD_version=
   CCD_name=
   CMDERBY_version=
   CMDERBY_name=
   ```

   **Tip:** You can also comment the lines out by inserting `#` at the start of each line.

7. Save the file.

8. Start IBM Cognos Configuration.

9. Under **Data Access, Content Manager**, do the following:
   
   - Delete the Cognos Content Database.
   - Configure a new database resource to point to a new content store.

   For more information, see "Set Up Database Connectivity for the Content Store Database" (p. 129).

10. Restart IBM Cognos BI.
Chapter 7: Installing and Configuring IBM Cognos PowerPlay Server Components on Different Computers
Chapter 8: Install and Configure Optional Components

Optional components provide extended functionality for users. After you install and configure IBM® Cognos® PowerPlay®, you can install the following optional components.

- IBM Cognos BI Samples
- Translated Product Documentation
- Additional fonts for Japanese and Korean currency symbols

PowerPlay Samples

The Great Outdoors Company samples illustrate product features and technical and business best practices. You can also use them for experimenting with and sharing report design techniques and for troubleshooting. The samples include PowerCubes and reports that you can use in IBM® Cognos® PowerPlay® to try the following features:

- Migrate sample cubes and reports from IBM Cognos Series 7 to IBM Cognos PowerPlay
  
  To support migration, some samples must be copied to your IBM Cognos Series 7 PowerPlay servers.
  
  For more information about using the samples to test the migration process, see the IBM Cognos PowerPlay Migration and Administration Guide.

- View published IBM Cognos PowerPlay reports in PowerPlay Studio and PowerPlay Client
  
  For more information about using the sample reports, see the IBM Cognos PowerPlay Studio User Guide and the IBM Cognos PowerPlay Client User Guide.

- Drill through from an IBM Cognos PowerPlay report to other reports and cubes
  
  For more information about using drill through in IBM Cognos PowerPlay, see the IBM Cognos PowerPlay Migration and Administration Guide.

The Great Outdoors Company, or GO Sales, or any variation of the Great Outdoors name, is the name of a fictitious business operation whose sample data is used to develop sample applications for IBM and IBM customers. Its 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. Unauthorized duplication is prohibited.

Before you can use the samples, your IBM Cognos Business Intelligence product must be installed, configured, and running.

If your IBM Cognos environment includes Report Studio, Analysis Studio, Metric Studio, or IBM Cognos Transformer, you can set up other IBM Cognos samples to use with them. For information
about setting up the other IBM Cognos BI samples, see the Samples topic in the Installation and Configuration Guide for your other IBM Cognos BI products.

Install the IBM Cognos BI Samples

Install the samples from the IBM® Cognos® Business Intelligence Samples CD.

The IBM Cognos Samples installation includes a variety content, data sources, models, cubes, reports, and other types of content, to support all IBM Cognos BI components. Only some of the samples content is of interest to PowerPlay® users. Instead of adding the entire IBM Cognos Samples installation to the PowerPlay computer, install the samples to a shared network location and then copy relevant content to the PowerPlay computer. Users of other IBM Cognos BI components can copy samples from the same network location.

Steps for UNIX and Linux

1. Mount the IBM Cognos product disk using Rock Ridge file extensions or go to the location where the installation files were downloaded.

   To mount the IBM Cognos 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.

2. To start the installation wizard, go to the operating system directory and 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®, 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 run an unattended installation.

   If you do not use XWindows, run an unattended installation.
3. Follow the directions in the installation wizard and copy the required files to your computer. Install the samples in the same location as the server components.

4. In the **Finish** page of the installation wizard, click **Finish**.

**Steps for Windows**

1. Do one of the following:
   - Insert the IBM Cognos BI Samples 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 double-click issetup.exe.

2. Select the language to use for the installation.
   The language that you select determines the language of the user interface. You can change the language to any of the installed languages after installation.

3. Follow the directions in the installation wizard to copy the required files to your computer.
   Install the samples in the same location as the other PowerPlay components. In a distributed installation, install them on the gateway computer.

4. In the **Finish** page of the installation wizard, click **Finish**.

**Setting Up the IBM Cognos PowerPlay Samples**

After you install the samples from the IBM® Cognos® Business Intelligence Samples CD, use the following checklist to guide you through the tasks of setting up the samples.

- Create a data source connection to the sample PowerCube.
- Import the sample reports.
- Set up PowerCubes and reports for drill-through examples and migration.

**Create a Data Source Connection to the Sample PowerCube**

Before you can open the sample reports in PowerPlay® Studio, you must create a data source connection to the sample PowerCube.

**Steps**

1. Connect to the IBM Cognos BI portal.

2. Start IBM Cognos Administration:
   - In the **Welcome** page, click **Administer IBM Cognos Content**.
   - In IBM Cognos Connection, from the toolbar, click **Launch, IBM Cognos Administration**.

3. In IBM Cognos Administration, click the **Configuration** tab.
4. Click the new data source button.

5. In the Name box, type `great_outdoors_sales_en` and then click Next.
   The name must be all lowercase and include the underscore characters.

6. In the Type box, select IBM Cognos PowerCube and then click Next.

7. In the location box, type the path and file name for the `great_outdoors_sales_en.mdc` PowerCube. For example, if you are creating a connection to samples installed to the default installation location on the local computer, type `C:\Program Files\ibm\cognos\c10\webcontent\samples\datasources\cubes\PowerCubes\EN\great_outdoors_sales_en.mdc`

8. To confirm that you entered all parameters correctly, click Test the Connection.
   After you test the connection, click Close on both the View the Results and Test the Connection pages to return to the connection string page.

9. Click Finish.

10. On the Finish page click OK. Do not select Create a Package.

   The `great_outdoors_sales_en` entry appears on the Data Source Connections list.

**Import the Sample Reports**

You can make the sample reports available for use in Cognos Viewer or PowerPlay Studio by importing them using a deployment archive. The sample PowerPlay data is packaged in a deployment archive for PowerPlay and migration and a deployment archive for drill-through examples. You import the deployment archives in IBM Cognos Administration before users can access the reports.

Another method to make reports available in Cognos Viewer or PowerPlay Studio is to publish them using PowerPlay Client. For more information, see the IBM Cognos PowerPlay Client User Guide.

Before you import the content, ensure that you set up the sample PowerCube (p. 173).

**Steps to Import the PowerPlay and Migration Samples**

1. On the computer where the samples are installed, go to the `c10_location\webcontent\samples\content` directory.
   For example, if the samples were installed to the default installation location, the path is `C:\Program Files\ibm\cognos\c10\webcontent\samples\content`

2. Copy `IBM_Cognos_PowerPlay.zip` to the `c10_location\deployment` directory on the computer where the Content Manager component is installed.

3. Connect to the IBM Cognos BI portal.

4. Start IBM Cognos Administration:
   - In the Welcome page, click Administer IBM Cognos Content.
   - In IBM Cognos Connection, from the toolbar, click Launch, IBM Cognos Administration.
5. Click the Configuration tab.
6. Click Content Administration.
7. Click the new import button.
8. Select IBM_Cognos_PowerPlay and click Next.
9. Keep the default name and location and then click Next.
10. Select the Samples folders and click Next.
11. Keep the default options and click Next.
12. Review the summary and click Next.
13. Select Save and run once and click Finish.
15. Click OK.

IBM_Cognos_PowerPlay appears in Administration and a Samples folder appears in Public Folders in IBM Cognos Connection.

**Steps to Import the Drill-through Samples**

1. On the computer where the samples are installed, go to the c10_location\webcontent\samples\content directory.
   For example, if the samples were installed to the default installation location, the path is C:\Program Files\ibm\cognos\c10\webcontent\samples\content
2. Copy IBM_Cognos_DrillThroughSamples.zip to the c10_location\deployment directory on the computer where the Content Manager component is installed.
3. Connect to the IBM Cognos BI portal.
4. Start IBM Cognos Administration:
   - In the Welcome page, click Administer IBM Cognos Content.
   - In IBM Cognos Connection, from the toolbar, click Launch, IBM Cognos Administration.
5. Click Configuration.
6. Click Content Administration.
7. Click the new import button.
8. Select IBM_Cognos_DrillThroughSamples and click Next.
9. Keep the default name and location and then click Next.
10. Select the Samples folder and click Next.
11. Keep the default options and click Next.
12. Review the summary and click **Next**.

13. Select **Save and run once** and click **Finish**.

14. Select **Now** and click **Run**.

15. Click **OK**.

   *IBM_Cognos_DrillThroughSamples* appears in Administration. Two folders are added to Public Folders, Samples, Models folder: Go Data Warehouse (analysis) and Go Data Warehouse (query). You must have Analysis Studio or Query Studio installed to view these drill-through samples.

**Test a Sample Report**

You can test the import by opening a sample report in Cognos Viewer or PowerPlay Studio. Cognos Viewer is the default viewer when you open a report in IBM Cognos Connection.

**Steps to Test a Report in Cognos Viewer**

1. Connect to the IBM Cognos BI portal.

2. Start IBM Cognos Connection:
   - In the **Welcome** page, click **IBM Cognos content**.
   - In IBM Cognos Administration, from the toolbar, click **Launch, IBM Cognos Connection**.

3. In the **Public Folders** list, open **Samples, PowerPlay**.

4. Click **great_outdoors_sales_en**.

5. Click any report in the list.
   The report opens in IBM Cognos Viewer.

**Steps to Test a Report in PowerPlay Studio**

1. Connect to the IBM Cognos BI portal.

2. Start IBM Cognos Connection:
   - In the **Welcome** page, click **IBM Cognos content**.
   - In IBM Cognos Administration, from the toolbar, click **Launch, IBM Cognos Connection**.

3. Go to Public Folders, Samples, PowerPlay.

4. Click **More** beside the **great_outdoors_sales_en** entry.

5. Click **View package contents**.

6. Click the **Open with PowerPlay Studio** button for any report in the list.
   The report opens in PowerPlay Studio.
Set Up the Sample PowerCubes and Reports for Migration

Before you can do a sample migration from IBM® Cognos® Series 7 to IBM Cognos PowerPlay®, you must copy the IBM Cognos Series 7 PowerCube and sample reports from the IBM Cognos BI Samples installation to the IBM Cognos Series 7 PowerPlay Enterprise Server computer.

After you set up the sample PowerCube and reports, you can migrate the reports. After the migration, users can then view the reports in Cognos Viewer or PowerPlay Studio. By default, the migrated reports are in PDF format.

For information about running a migration, see the Migration and Administration Guide.

Steps

1. From the computer where the IBM Cognos BI Samples are installed, copy the following content to the IBM Cognos Series 7 computer.
   - all reports from the `c10_location\webcontent\samples\powerplay_reports\powerplay_7\reports_for_remote_cubes\language` directory
   - `great_outdoors_7.mdc` from the `c10_location\webcontent\samples\datasources\cubes\PowerCubes\language` directory

2. In IBM Cognos Series 7 PowerPlay Administration, add the cube and reports to PowerPlay Enterprise Server.
   
   For more information, see the IBM Cognos Series 7 PowerPlay Enterprise Server Guide.

3. To update the cube mapping, in IBM Cognos Series 7 PowerPlay Client, open each report using a remote connection to `great_outdoors_7.mdc`, and then save the report.

The cube and reports are now ready for use in IBM Cognos Series 7.

Install 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 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

Steps

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.

### Install and Configure Additional Language Fonts

To add support for the Japanese Yen or Korean Won character, you must install additional fonts from IBM® Cognos® BI Supplementary Language Documentation.

The Unicode code point “U+005C” is officially assigned to the backslash. However, in Japan and Korea, that code point is historically assigned to their currency symbols and many people still prefer to see a yen or won sign in certain parts of software, for example in file paths. To accommodate this, you can install the “Andale WT J” and “Andale WT K” fonts.

Before installing the additional fonts, ensure that

- IBM Cognos BI is installed and configured correctly
- adequate disk space is available to install additional fonts
  
  You need at least 220 MB of disk space.
- your software environment is supported

### Steps

1. In the location where Application Tier Components are installed, insert the IBM Cognos BI Supplementary Language Documentation disk.

   On UNIX® or Linux® operating systems, mount the disk using Rock Ridge file extensions.

2. Go to the directory on the disk that is appropriate for your operating system.

3. Start the installation wizard by typing the following command:
   - On Windows®,
4. Follow the instructions in the installation wizard to copy the required files to the same location where you installed Application Tier Components.

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.

When you are prompted to select components, clear **IBM Cognos Business Intelligence Supplementary Languages Documentation**, expand **Additional Language Fonts**, and then select the font.

These fonts are copied to the `c10_location/bin/fonts` directory. This font location is defined in the **Physical fonts location** property value in IBM Cognos Configuration under **Environment**. If you move the fonts to another location, ensure that the new location is added to the **Physical fonts location** property value.

Fonts used to display data in a report are selected using a matching process between the fonts requested when the report is designed and the fonts that are available when the report is rendered. For PDF output and charts, this process occurs on the server where all fonts on the server that generates the report can be used.

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

After you install the additional fonts, you must configure support for them. For more information, see "Configure Support for Japanese Yen and Korean Won Characters" (p. 179).

## Configure Support for Japanese Yen and Korean Won Characters

For Japanese and Korean currency characters to display correctly, you must define the additional fonts in the global style sheet.

Before you configure these fonts, you must install them from the IBM® Cognos® BI Supplementary Language Documentation disk.

### Steps to Configure the Fonts for Yen and Won Characters


   The GlobalReportStyles.css style sheet is located in the `c10_location/bin` directory.

2. Enable one of the following sections and modify it as shown below:

   ```
   /* For Japanese: */
   .pg,
   .pp
   { ...
   ```
Chapter 8: Install and Configure Optional Components

The PDF generator uses the first available font on the server and includes all the characters in the string to be displayed. If you prefer to use other fonts on your server, you can insert them into the list.


4. Restart the IBM Cognos BI server.

Any changes that you make to the style sheet are overwritten if you upgrade IBM Cognos BI. You must repeat this procedure following an upgrade.
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:

- Active Directory Server
- IBM Cognos Series 7
- Custom Authentication Provider
- LDAP
- eTrust SiteMinder
- NTLM
- 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 non-Linux computer:

- IBM Cognos Series 7 namespace
- Active Directory Server
- NTLM
• eTrust SiteMinder

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 eTrust SiteMinder namespaces from users.

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

By default, IBM® Cognos® components do not require user authentication. Users can log on anonymously.

If you want to use authenticated logon only, you can use IBM Cognos Configuration to disable anonymous access.

#### Steps

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 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.

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.

Steps

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.

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 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 (p. 186) and single signon using Kerberos delegation (p. 188).

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.

For more information, see "Configure an LDAP Namespace for Active Directory Server" (p. 197).
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.

To use an Active Directory Server namespace and to set up single signon, do the following:

- Configure IBM® Cognos® components to use an Active Directory Server namespace
- Enable secure communication to the Active Directory Server, if required
- Enable single signon between Active Directory Server 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.

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 *Administration and Security Guide*.

**Steps**

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**.
    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 **Administration and Security Guide**.

**Steps**

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 button.

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.

Steps

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.

Authentication in One Domain Tree

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 above the original authenticated domain or in a different domain tree cannot log in.
Authentication in All Domain Trees in the Forest

If you set a parameter named MultiDomainTrees to true, users in all domain trees in the forest can log in to IBM Cognos.

Steps
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 button.
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>
<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.

Enabling Single Signon Between Active Directory Server and IBM Cognos Components

By default, the Active Directory provider uses Kerberos delegation and integrates with the IIS Web server for single signon if integrated authentication (formerly named NT Challenge Response) on Microsoft® Windows® operating system is enabled on the IIS Web server.

If Windows integrated authentication is enabled, you are not prompted to reenter authentication information when accessing IBM® Cognos® content that is secured by the Active Directory namespace.
If you do not want Kerberos delegation, 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 integrated authentication. If Kerberos authentication is bypassed, single signon to Microsoft OLAP (MSAS) data sources will not be possible.

**Steps for Single Signon Using Kerberos Delegation**

1. Set up Windows integrated authentication on the IIS Web server.
2. Install Content Manager in a location that is part of the 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 for delegation.
   
   When setting up the computers using the Active Directory user tool, do not select the **Account** attribute, which is sensitive and cannot be delegated.

**Steps for Single Signon Using REMOTE_USER**

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. Click in the **Value** column for **Advanced properties** and then click the edit button.
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. Click **OK**.
8. Click in the **Value** column for **Binding credentials**, and then click the edit button.
9. In the **Value - Binding credentials** dialog box, specify a user ID and password and then click **OK**.

The Active Directory provider now uses REMOTE_USER for single signon.

**Tip:** To switch back to Kerberos delegation, edit **Advanced properties** and, in the **Value** column, type **KerberosAuthentication**.

**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.

If you plan to run IBM Cognos BI products within a 64-bit application server, you cannot configure an IBM Cognos Series 7 namespace as your authentication source.

If you want to configure an IBM Cognos Series 7 namespace as your authentication source, you must install Content Manager in a location that supports IBM Cognos Series 7.

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. To use an IBM Cognos Series 7 namespace and to set up single signon, do the following:

- Configure IBM Cognos to use an IBM Cognos Series 7 namespace
- Enable secure communication to the directory server used by the IBM Cognos Series 7 namespace, if required
- 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.

**Steps**

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 button.
   - 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.

**Steps**

1. Ensure that you configured IBM Cognos components to use an IBM Cognos Series 7 namespace as an authentication provider (p. 188).

2. For IBM Cognos Series 7, start Configuration Manager.

3. Click **Open the current configuration**.

4. On the **Components** tab, in the **Explorer** window, expand **Services, Access Manager - Web Authentication** and click **Cookie Settings**.

5. In the **Properties** window, ensure that the **Path**, **Domain**, and **Secure Flag Enabled** properties match the settings configured for IBM Cognos.

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**.

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>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[in] envVar</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>[in] reqEnvVarList</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>[out] trustedSignonName</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>[out] trustedSignonNameLength</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>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[out] trustedDomainName</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>[out] trustedDomainNameLength</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>[out] userType</td>
<td>A value that indicates the type of user that Access Manager will authenticate. This value is mandatory.</td>
</tr>
<tr>
<td></td>
<td>The following return values are required for Access Manager to successfully authenticate users:</td>
</tr>
<tr>
<td></td>
<td>SAFER_NORMAL_USER</td>
</tr>
<tr>
<td></td>
<td>A named user. OS signons must exist and be enabled in the current namespace.</td>
</tr>
<tr>
<td></td>
<td>SAFER_GUEST_USER</td>
</tr>
<tr>
<td></td>
<td>A guest user. A guest user account must exist and be enabled in the current namespace.</td>
</tr>
<tr>
<td></td>
<td>SAFER_ANONYMOUS_USER</td>
</tr>
<tr>
<td></td>
<td>An anonymous user. An anonymous user account must exist and be enabled in the current namespace.</td>
</tr>
<tr>
<td>[in/out] implementerData</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.

Steps
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.
   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.

Steps
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.

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 Sun Java™ System 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 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" (p. 195).

To use an LDAP namespace and set up single signon, do the following:

- Configure IBM Cognos components to use an LDAP namespace
- Make custom user properties available to IBM Cognos components, if required
- Enable secure communication to the LDAP server, if required
- 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 eTrust 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 Sun Java™ System Directory Server, see [Configure an LDAP Namespace for Sun Java System 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 *Administration and Security Guide*.

### Steps

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.

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.

**Steps**

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**, specify `(sAMAccountName=${userID})`
- If you use single signon, for **Use external identity**, set the value to **True**.
- If you use single signon, for **External identity mapping**, specify `(sAMAccountName=${environment("REMOTE_USER")})`

  If you want to remove the domain name from the REMOTE_USER variable, specify `(sAMAccountName=${replace(${environment("REMOTE_USER")}, "domain\", ",")})`.

- For **Bind user DN and password**, specify `user@domain`
- For **Unique identifier**, specify `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:

- 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 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>Mappings</td>
<td>LDAP property</td>
<td>LDAP value</td>
</tr>
<tr>
<td>----------</td>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>Account</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></td>
<td>Object class</td>
<td>user</td>
</tr>
<tr>
<td></td>
<td>Business phone</td>
<td>telephonenumber</td>
</tr>
<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>displayName</td>
</tr>
<tr>
<td></td>
<td>Pager phone</td>
<td>pager</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>unicodePwd</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>sAMAccountName</td>
</tr>
</tbody>
</table>

These mapping properties represent changes 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.

IBM Cognos loads, initializes, and configures the provider libraries for the 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.

Steps

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>
<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>telefononenumber</td>
</tr>
<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>
</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.

**Steps**

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 **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 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>
<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>
<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>(leave blank)</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 Sun Java System Directory Server**

If you configure a new LDAP namespace for use with Sun Java™ System Directory Server, you must modify the necessary settings and change the values for all properties of the Sun Java System Directory objects.

**Steps**

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 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.

The following settings are examples:
• For **User lookup**, type `(uid=${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:
  
  \[
  \text{ntuserdomainid} = \text{environment}("REMOTE\_USER")
  \]
  
  \[
  \text{uid} = \text{environment}("REMOTE\_USER")
  \]

• 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 Sun Java System Directory Server objects, use the values 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</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>Mappings</td>
<td>LDAP property</td>
<td>LDAP value</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------</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>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 Sun Java System 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. 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 with Oracle lightweight connections and virtual private databases. For more information, see the Administration and Security Guide.

**Steps**

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 button.
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.

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.

**Steps**

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

${replace(str , old , 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>
Configuring IBM Cognos Components to Use eTrust SiteMinder

You can configure IBM® Cognos® components to use a Netegrity SiteMinder namespace as the authentication source, provided that you installed Content Manager on a non-Linux® computer.

To configure an authentication provider in an eTrust SiteMinder environment, you configure an LDAP, NTLM, or Netegrity SiteMinder namespace depending on your eTrust SiteMinder configuration. Supported eTrust SiteMinder configurations are LDAP, Active Directory Server, and NTLM user directories.

Note: The authentication provider uses an eTrust SiteMinder Software Development Kit to implement a custom agent. The custom agent deployment requires that you set the Agent Properties in the eTrust SiteMinder Policy server administration console to support 4.x agents.

If you plan to run IBM Cognos Business Intelligence products within a 64-bit application server, you cannot configure a Netegrity SiteMinder namespace as your authentication source.

If eTrust SiteMinder is Configured For More Than One User Directory

If you configured eTrust SiteMinder for more than one user directory, you must use the Netegrity SiteMinder namespace. After configuring the Netegrity SiteMinder namespace in IBM Cognos, you must also add a corresponding LDAP, Active Directory Server, or NTLM namespace to the IBM Cognos configuration for each user directory defined in eTrust SiteMinder.

When configuring a corresponding LDAP namespace, ensure that the External identity mapping property is enabled and that you include the token REMOTE_USER in the value for the property. This does not mean that you must configure eTrust SiteMinder to set REMOTE_USER. The IBM Cognos Netegrity SiteMinder namespace passes user information internally to the corresponding LDAP namespace when it receives successful user identification from the eTrust SiteMinder environment.

When configuring a corresponding Active Directory namespace, ensure that the singleSignOnOption property is set to IdentityMapping. The IBM Cognos Netegrity 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 eTrust SiteMinder environment. For more information, see "Enabling Single Signon Between Active Directory Server and IBM Cognos Components" (p. 187).

If eTrust SiteMinder is Configured With Only One User Directory

If eTrust SiteMinder is configured with only one user directory, the Netegrity SiteMinder namespace is not required. You can use the user directory as your authentication source by configuring the appropriate namespace, or you can configure the eTrust SiteMinder provider with one user directory. For example, if the eTrust SiteMinder user directory is NTML, you can configure IBM Cognos components with an NTLM namespace or configure IBM Cognos components with one Netegrity SiteMinder namespace, referring to one user directory that is an NTLM namespace.
If the eTrust 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 Netegrity SiteMinder namespace, configure the appropriate LDAP (p. 196), Active Directory (p. 197), or NTLM (p. 213) namespace. In this case, verify the Agent Configuration Object properties in eTrust SiteMinder Policy Server. Ensure that SetRemoteUser is activated.

When configuring the LDAP namespace, in this case, ensure that the External identity mapping property is enabled and that you include the token REMOTE_USER in the value for the property.

When configuring the Active Directory namespace, in this case, ensure that the singleSignOnOption property is set to IdentityMapping. For more information, see "Enabling Single Signon Between Active Directory Server and IBM Cognos Components" (p. 187).

To use an eTrust SiteMinder namespace and to set up single signon, do the following:

- Configure IBM Cognos components to use a Netegrity SiteMinder namespace
- Enable secure communication to the eTrust SiteMinder user directory, if required
- Enable single signon between eTrust SiteMinder and IBM Cognos
- Protect the IBM Cognos Web alias

You can hide the namespace from users during login (p. 194).

**Configure a Netegrity SiteMinder Namespace**

If you configured eTrust SiteMinder for more than one user directory, you must use the Netegrity SiteMinder namespace. After adding the Netegrity SiteMinder namespace, you must also add a corresponding LDAP or NTLM namespace for each user directory.

You can also configure an Netegrity SiteMinder namespace if users are stored in

- an LDAP server
- an NTLM server
- an Active Directory server

**Steps**

1. In the location where you installed Content Manager, 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 the Netegrity SiteMinder 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.

7. In the Explorer window, under Security > Authentication, right-click the namespace and click New resource > SiteMinder Policy Server.

8. In the Name box, type a name for the policy server and click OK.

9. In the Properties window, specify the Host property and any other property values you want to change.

10. In the Explorer window, right-click the new SiteMinder Policy Server and click New resource > User directory.
   
   Tip: Configure a user directory for each user directory in the SiteMinder policy server.

11. In the Name box, type a name for the user directory and click OK.
   
   The name of the user directory must match the name that appears on the policy server.

12. In the Properties window, type a value for the Namespace ID reference property.

13. From the File menu, click Save.

14. Test the connection to a new namespace. In the Explorer window, under Authentication, right-click the new authentication resource and click Test.

15. Configure a corresponding LDAP, Active Directory, or NTLM namespace for each LDAP, Active Directory, or NTLM user directory.

   Ensure that you use the same value for the Namespace ID property that you use for the Namespace ID property for the Netegrity SiteMinder namespace.

**Enabling Secure Communication to the eTrust SiteMinder User Directory**

If you use an SSL connection to the directory server, you must appropriately configure the Cognos namespace for the user directory.

For more information, see "Configure an LDAP Namespace" (p. 196).

**Enable Single Signon Between eTrust SiteMinder and IBM Cognos**

By configuring single signon, you are not prompted to reenter authentication information.

IBM® Cognos® components automatically refer to the eTrust SiteMinder session cookie for user session data.

If the eTrust SiteMinder user directory is LDAP or Active Directory, you must configure the eTrust SiteMinder user directory to use external identity mapping to the REMOTE_USER environment variable.

If the eTrust SiteMinder user directory is NTLM, integrated authentication on Microsoft® Windows® operating system is used for single signon and no additional configuration is required.
Protecting the IBM Cognos Web Alias

Ensure that eTrust SiteMinder is configured correctly to protect the IBM® Cognos® Web alias.

Use the test tool provided with eTrust SiteMinder to verify that the resource is protected, authenticated, and authorized. For more information, see your eTrust SiteMinder documentation.

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 login.

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.

Steps

1. In each location where you configured an eTrust SiteMinder authentication provider, open IBM Cognos Configuration.
2. In the Explorer window, under Security, > Authentication, click the Netegrity Siteminder authentication provider.
3. In the Properties window, click the box next to Selectable for authentication and then click False.
4. From the File menu, click Save.

The namespace is not shown on the selection list that is presented at login.

Configuring IBM Cognos Components to Use an NTLM Namespace

You can configure IBM® Cognos® components to use the Microsoft® Windows® operating system native security, NT LAN Manager (NTLM), as the authentication source.

If you are not using NTLM in your IS environment, you cannot use an NTLM namespace.

If you want to use an NTLM user directory as your authentication source with eTrust SiteMinder, you must verify the Agent Configuration Object properties in the eTrust SiteMinder Policy Server. Ensure that SetRemoteUser is activated.

To use NTLM and to set up single signon, do the following:

- configure an NTLM namespace
- enable single signon between NTLM and IBM Cognos components
Chapter 9: Configuring IBM Cognos Components to Use an Authentication Provider

**Configure an NTLM Namespace**

You can configure IBM® Cognos® components to use an NTLM namespace when users are stored in an NTLM user directory. The NTLM user directory may also be accessed using an eTrust Site-Minder authentication provider.

**Steps**

1. In the location where you installed Content Manager, 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 NTLM and 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 NamespaceID property.

6. Specify the values for all other required properties to ensure that IBM Cognos components 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.

IBM Cognos loads, initializes, and configures the provider libraries for the namespace.

**Enable Single Signon Between NTLM and IBM Cognos Components**

By default, the IBM® Cognos® NTLM provider integrates with the IIS Web server for single signon if integrated authentication (formerly named NT Challenge Response) on Microsoft® Windows® operating system is enabled on the IIS Web server.

If Windows integrated authentication is enabled, you are not prompted to reenter authentication information when accessing IBM Cognos content that is secured by the NTLM namespace.

**Steps**

1. Set up Windows integrated authentication on the IIS Web server.

2. Install Content Manager in a location that is part of the 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 for delegation.
4. Test the connection to a new namespace. In the Explorer window, under Authentication, right-click the new authentication resource and click Test.

IBM Cognos loads, initializes, and configures the provider libraries for the 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.

To configure a RACF namespace and to set up single signon, do the following:

- Configure IBM® Cognos® components to use a RACF namespace
- Configure secure communication
- 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 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.

**Steps**

1. If running on a 64-bit server, do the following:
   - Go to the RACF installation directory on the 64-bit server.
   - Copy all 64-bit RACF 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 RACF library files to `c10_64_location\bin`.

2. If running on a 32-bit server, copy all 32-bit RACF library files from the RACF installation directory to the `c10_location\bin` directory.

3. In the location where you installed Content Manager, open IBM Cognos Configuration.

4. 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.

5. 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.

6. For the Host and port property, type the value that corresponds to the Tivoli Directory Server.

7. For the Base Distinguished Name property, type the value that matches the suffix that is configured for SDBM in the Tivoli Directory Server.

8. If you are using an SSL connection to the RACF provider, set the Enable SSL property to true.

9. 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.

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.

**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.

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 using anonymous 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.

**Steps**

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 button.

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.

---

**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 *Administration and Security Guide*.

**Steps**

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 *Administration and Security Guide*.

After you delete a namespace, it appears as Inactive in the portal.
Chapter 10: 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 may want to 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.

If you are upgrading from ReportNet, you have several configuration options depending on if you want to continue to use your existing installation. For information about upgrade options, see "Upgrading from an Earlier Version of IBM Cognos PowerPlay" (p. 67).

As shown in the following diagram, 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. We recommend that you use the test feature in IBM Cognos Configuration to validate changes.

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.

- Change default configuration settings.
- Create a new content store using Cognos Content Database.
- Configure the SSL protocol.
- Configure a repository for log messages.
Chapter 10: Configuration Options

- Change global settings.
- Change the gateway.
- Change IP address version.
- Configure the router to test dispatcher availability.
- Update file location properties on Windows Vista.

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,

- Go to the c10_location/bin directory and then type ./cogconfig.sh

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

configure font support for Simplified Chinese

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 (p. 104).

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.

Steps to Change the Default User Password

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:
**Steps to Create a New User and Password**

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:

   ```
   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:

   ```
   disconnect;
   ```

**Steps to Remove a User**

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=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:

     ```
     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 above 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:

```
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:

```
disconnect;
```

**Change a Port or URI Setting**

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>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>Specifies the protocol used to request and transmit information, either Hyper Text Transfer Protocol or Hyper Text Transfer Protocol (Secure).</td>
</tr>
<tr>
<td>host name or IP</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Example:** http or https

**Example:** localhost or 192.168.0.1 or [2001:0db8:0000:0000:0000:0000:148:57ab]:80
<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>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.</td>
<td>9300 or 80</td>
</tr>
<tr>
<td>context root</td>
<td>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.</td>
<td>p2pd</td>
</tr>
<tr>
<td>alias path</td>
<td>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.</td>
<td>servlet/dispatch</td>
</tr>
<tr>
<td>virtual directory</td>
<td>Used by the Web server to map a virtual directory or alias to a physical location. For example, in the default Gateway URI of <a href="http://localhost:80/ibmcognos/cgi-bin/cognos.cgi">http://localhost:80/ibmcognos/cgi-bin/cognos.cgi</a>, the virtual directory is ibmcognos/cgi-bin.</td>
<td>ibmcognos/</td>
</tr>
<tr>
<td>gateway application</td>
<td>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.</td>
<td>cognos.cgi</td>
</tr>
</tbody>
</table>

**Steps**

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

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.

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.

Steps

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.

   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 the following cryptographic settings for the cryptographic provider:

- 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.

**Steps**

1. If you are using a JRE other than the one provided with IBM Cognos server, ensure that the following files from IBM Cognos exist in the location where the JRE is installed:
   - From c10_location/bin/jre/version/lib/ext, copy bcpov-jdk14-134.jar to JRE_location/lib/ext.
From `c10_location/bin/jre/version/lib/security`, copy `local_policy.jar` and `US_export_policy.jar` to `JRE_location/lib/security`.

2. 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 [https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk](https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk).


4. In the Explorer window, under Security, Cryptography, click Cognos.

5. 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 Cryptography Extension (JCE) policy file. For Java that IBM provides, the unrestricted JCE policy file can be downloaded from [https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk](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 button.

     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 BI Components to Use a Another Certificate Authority" (p. 316).

6. From the **File** menu, click **Save**.

If you use another Certificate Authority (CA) server, configure IBM Cognos components to use the CA. For more information, see "Configuring IBM Cognos BI Components to Use a Another Certificate Authority" (p. 316).

### 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.

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.

**Steps**

1. If you are using a JRE other than the one provided with IBM Cognos server, ensure that the following files from IBM Cognos and Entrust exist in the location where the JRE is installed:
   • From `c10_location/bin/jre/version/lib/ext`, copy `bcprov-jdk14-134.jar` to `JRE_location/lib/ext`.
   • From `c10_location/bin/jre/version/lib/security`, copy `local_policy.jar` and `US_export_policy.jar` to `JRE_location/lib/security`.
   • From the Entrust Authority Security Toolkit that you download from Entrust, copy the .jar file, such as `enttoolkit.jar`, to `JRE_location/lib/ext`.

2. 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 https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk.


4. In the **Explorer** window, under the **Security** group, click **Cryptography**.

5. 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.

6. In the **Explorer** window, under the **Security** group and the **Cryptography** component, right-click the **IBM Cognos** resource, and click **Delete**.

7. Under the **Security** group, right-click **Cryptography**, and click **New resource > Provider**.
8. In the Name field, type a name for the encryption service you are creating.

9. In the Type field, click the arrow, and click Entrust, and then click OK.
   A branch with the name you assigned appears below Cryptography.

10. Click the branch you created.
    Resource properties appear in the properties window.

11. In the 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.

12. From the File menu, click Save.

13. Update to Entrust Java Toolkit 7.2 SP2 Patch 152842.
Configure IBM Cognos Components to Use 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.

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.

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 more information, see "Configure the Web Server" (p. 160).

  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( )`

**Steps**

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 button.
   - 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 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.

**Steps**

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.

**Steps**

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 dis-
tributed 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.

**Steps**

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. In the case of 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 will read the HTML 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.
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.

**Steps**

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.

   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.

**Steps**

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, by following the steps below. 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.

Steps

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 button.

   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 button. 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.

Now, if required, you must specify the installation location of the fonts.

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 Windows®, support is provided for the GB18030-2000 character set in the NSimSun-18030 font that is provided by Microsoft®. If you install on other operating systems, or if you use Internet Explorer 6 on Windows, additional installation tasks are required:
On operating systems other than Windows, you must install a font that supports GB18030-2000.

If you use Internet Explorer 6 on Windows, you must update the registry entries for fonts that reference SimSun.

### Update the Registry Entries for Windows Font Links

The GB18030-2000 character set includes CJK Unified Ideographs Extension A characters. When these characters are encoded as UTF-8 in Internet Explorer 6, they may not appear correctly in Web pages. To ensure that these characters appear correctly, you must add SimSun-18030 to all font link registry entries that specify SimSun.

**Steps**

1. From the **Start** menu, select **Run**.
2. In the **Run** dialog box, type **regedit**.
3. Open the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink` directory.
4. In **Registry Editor**, right-click a font that contains SimSun in the **Data** field and select **Modify**.
5. In the **Edit Multi-String** dialog box, under **Value data**, click under the selected strings and type the following string:
   
   `SimSun18030.ttc,SimSun-18030`

6. Click **OK**.
7. Repeat steps 4 to 6 for every font that contains SimSun.
8. When complete, close **Registry Editor**.

### 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. After you make the change, the font 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.

**Steps**

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.

**Steps**

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 button.

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 *Administration and Security Guide*.

**Steps**

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 `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:

   `file://\servername\directory`

6. To confirm that the correct location will be used, click Test.

7. Click OK.

8. From the File menu, click Save.

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 *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 Administration and Security Guide.

To protect the security of the report output when using this feature, the file system must have third-party encryption.

**Steps**

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.

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 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. 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. 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.

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 Administration and Security Guide.

**Steps**

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 button.

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.

**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:

- Create a notification database.
  
  For DB2, Oracle, Microsoft® SQL Server, or Sybase, use the same procedure that was used to create the content store database.
  
  For DB2 on z/OS, use the instructions in "Suggested Settings for Creating a DB2 Notification Database on z/OS" (p. 240).

- Set 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" (p. 91).

- Change the connection properties for the notification database.

**Suggested Settings for Creating a DB2 Notification Database on z/OS**

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

To ensure a successful installation, use the following guidelines when creating the notification database.

Use the following checklist to help you help you set up the notifications database in DB2 on z/OS®.

- Create a database instance, storage group, and a user account for the notification database.
  
  A user must have permissions to create and delete tables in the database.
  
  IBM® Cognos® BI uses the credentials of the user account to communicate with database server.

- Ensure you reserve a buffer pool with a page size of 32 k, and a second one with a page size of 4 k for the database instance.

- Administrators must run a script to create tablespaces to hold Large Objects and other data for the notification database to use the tablespaces.
For information about running the script, see "Create Tablespaces for the DB2 Notification Database on z/OS" (p. 241).

☐ 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.

Create Tablespaces for the DB2 Notification Database on z/OS

A database administrator must run scripts to create a set of tablespaces required for the notification database. The scripts must be modified to replace the placeholder parameters with ones that are appropriate for your environment.

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. For more information, see the IBM® DB2 Information Center.

Steps
1. Connect to the database as a user with 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. Open the 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>
<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 may be added in the future.

4. Save and run the script.

5. Open the NC_CREATE.sql script file and replace the NCCOG placeholder parameter with the name of the notification database.

6. Save the script.

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

The notification database is created. You can now change the notification database in IBM Cognos® Configuration (p. 242).
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.

Steps

1. In each location where Content Manager or Application Tier Components is installed, start IBM Cognos Configuration.

2. In the Explorer window, under Data Access, click Notification.

3. Identify the database that is used for notification:
   - In the Explorer window, right-click Notification and select New resource > Database.
   - Type a name for the database resource.
   - Select the type of database from the pull-down menu.
   - Click OK.

4. In the Properties window, enter the values for the notification database resource.

5. From the File menu, click Save.

6. 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.
   Ensure that the values used to identify the notification database resource are the same on all Content Manager and Application Tier Components computers. To use the default notification database, you do not have to edit the values in the Properties window.

Create a New Content Store Using Cognos Content Database

Follow the steps below if you want to create another content store database using Cognos Content Database. This may 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.

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.

**Steps**

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;
   ```

**Configuring the SSL Protocol**

The Secure Sockets Layer (SSL) protocol is used to secure communication between IBM® Cognos® components installed on the same computer or on different computers.

In addition, you may want to set up SSL connections between IBM Cognos components and other servers. You must ensure that SSL is set up for the other servers before you set up a shared trust between IBM Cognos components and the other servers.

Use the following checklist to configure SSL protocol.

- Configure SSL for IBM Cognos components (p. 243).
- Set up shared trust between IBM Cognos components and other servers, if required (p. 246).
- Select and rank Cipher Suites to be used in an SSL connection, if required (p. 247).
- Enable SSL on your Web server (p. 248).

After configuring the SSL protocol, you can select and rank cipher suites, which control the quality of protection used in the SSL connection.

**Configure SSL for IBM Cognos Components**

You can configure IBM® Cognos® components to use the SSL protocol for

- internal connections only
external connections only

internal and external connections

connections to local and remote log servers

If you configure SSL for internal connections only, IBM Cognos components on the local computer 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 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.

You must also update the Content Manager URIs, Dispatcher URI for external applications, and Gateway URI to use SSL, if required.

**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 protocol 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 single computer installations, if you are running IBM Cognos without SSL, you must stop the service before adding SSL to your configuration. After you save the configuration with SSL settings, you can restart the service.

**Distributed Installations**

In distributed installations, if you are using the IBM Cognos certificate authority service, you must first configure all IBM Cognos computers to use the non-secure (http) protocol before you configure IBM Cognos components to use the SSL protocol. You must do this because you cannot set up the SSL protocol before trust has been established.

Also, ensure that you follow the required order of configuring computers in a distributed environment. That means that you must first configure the computer where the default active Content Manager is installed and then start the services on this computer before you configure other computers or start services on other computers. By first configuring the default active Content Manager computer and starting the services, you ensure that the certificate authority service on the default active Content Manager computer can issue certificates to other computers in the IBM Cognos environment.
After you configure all computers in the distributed installation to use the default, non-secure protocol, test your installation to ensure that IBM Cognos components are working properly. After you test your installation, you can configure the SSL protocol.

When you configure IBM Cognos to use the SSL protocol, ensure that you first configure the default active Content Manager computer to use the protocol and start the services on the default active Content Manager computer. After you do this, you can configure the SSL protocol on other IBM Cognos computers in your environment.

**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 Content Manager computer.

**Add a Component to a Computer**

You can later add a component to the same location as other IBM Cognos components. If you add the component to a different location on the same computer as other IBM Cognos components, 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 between the new component and the Content Manager computer.

**Steps**

1. Start IBM Cognos Configuration.

2. In the **Explorer** window, click **Environment**.

3. In the **Properties** window, type the appropriate values for the **Internal dispatcher URI** and **External dispatcher URI** values:

   - **To configure SSL for internal connections only**, for the **Internal dispatcher URI** property, type **https** and a port for SSL communication. For the **External dispatcher URI** property, type **http** and use the default or another available port.

     If you use Tomcat, the **Internal dispatcher URI** property must specify **localhost**. The ports in the two dispatcher URIs must be different.

   - **To configure SSL for external connections only**, for the **External dispatcher URI** property, type **https** and a secure port. For the **Internal dispatcher URI** property, type **http** and use the default or another available port.

     If you use Tomcat, the **Internal dispatcher URI** property must also specify **localhost**. The ports in the two dispatcher URIs must be different.

   - **To configure SSL for all connections**, type the same URI for both the **Internal dispatcher URI** and **External dispatcher URI** properties. Type **https** and a secure port, such as 9343.

     **Note:** You do not have to use port 9343, the default SSL port. You can choose any available port.
4. Configure the SSL protocol for the other environment URIs, including the Content Manager URIs, the Dispatcher URI for external applications, and Gateway URI.
   - For internal connections only, type https in the URIs that contain localhost.
   - For external connections only, type https in the URIs that do not contain localhost.
   - For all connections, type https in all the URIs.

5. In the Explorer window, click Security > Cryptography.

6. To use SSL protocol, you must specify passwords for the IBM Cognos encryption key stores. There are more settings under Security > Cryptography > Cognos.

7. From the File menu, click Save.

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.

Steps to Copy the IBM Cognos Certificate to Another Server

1. Go to the c10_location/bin directory.

2. Extract the IBM Cognos certificate by typing the following command:
   - On UNIX® or Linux®, type
     
     ThirdPartyCertificateTool.sh -E -T -r destination_file -k c10_location/configuration/signkeypair/jCAKeystore -p password
   - On Windows®, type
     
     ThirdPartyCertificateTool.bat -E -T -r destination_file -k c10_location\configuration\signkeypair\jCAKeystore -p password

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.

Steps to Copy the CA Certificate to IBM Cognos Servers

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, type
     `ThirdPartyCertificateTool.sh -T -i -r CA_certificate_file -k c10_location/configuration/signkeypair/jCAKeystore -p password`
   - On Windows, type
     `ThirdPartyCertificateTool.bat -T -i -r CA_certificate_file -k c10_location\configuration\signkeypair\jCAKeystore -p password`

Select and Rank Cipher Suites for SSL

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.

Steps

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 button
   - 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.
Enable SSL on the Web Server

Enable secure sockets layer (SSL) to encrypt a user’s communication with the Web server.

To enable SSL on your Web server, you must obtain a Web server certificate signed by a Certificate Authority 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.

To enable IBM Cognos components to use an SSL-enabled Web server, you must have copies of the trusted root certificate (the certificate of the root Certificate Authority which signed the Web server certificate) and all other certificates which make up the chain of trust for the Web server’s certificate. These certificates must be in Base64 encoded in ASCII (PEM) or DER format, and must not be self-signed. The certificates must be installed on every computer where you have installed Application Tier Components.

For more information about installing certificates into your Web server, see your Web server documentation.

Steps

1. Configure the Web server for SSL and start the Web server.
   
   For more information, see your Web server documentation

2. On each Application Tier Components computer that points to the gateway on the Web server, in IBM Cognos Configuration, change the gateway URI from HTTP to HTTPS, and save the configuration.
   
   Do not start the IBM Cognos service yet.

3. On each Application Tier Components computer, go to the $c10_location/bin directory and import all the certificates that make up the chain of trust, in order starting with the root CA certificate, into the IBM Cognos trust store.

   Import the certificates by typing the following command:

   On UNIX® or LINUX®, type

   `ThirdPartyCertificateTool.sh -T -i -r certificate_fileName -D ../configuration/signkeypair -p password`

   On Windows®, type

   `ThirdPartyCertificateTool.bat -T -i -r certificate_fileName -D ../configuration/signkeypair -p password`

   Note: The password should have already been set. If not, the default password is NoPassWord-Set.

4. On each Application Tier Components computer, in IBM Cognos Configuration, start the IBM Cognos service.
You can verify trust, by creating and running a PDF report that contains pictures that are not stored locally but which the gateway gets from a remote computer. If the pictures appear, trust is established.

To avoid being prompted by a security alert for each new session, install the certificate into one of your Web browser’s certificate stores.

In addition, you may want to set up SSL connections between IBM Cognos components and other servers. You must ensure that SSL is set up for the other servers and then you must set up a shared trust between IBM Cognos components and the other servers. For more information, see "Configuring the SSL Protocol" (p. 243).

### Configuring a Repository for Log Messages

Log messages are 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.

- **Plan log message processing**
- **Configure logging**
- **Set up 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 *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 configuring logging, see the *Installation and Configuration Guide*.

When setting up logging, specify the level of detail to log to focus messages on the information that is relevant in your organization. Audit reports may also be set up to track user and report activity. For information about setting up logging, see the *Administration and Security Guide*.

For information about using log messages to solve problems and resolving logging-related issues, see the Troubleshooting section of the *Administration and Security 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, Informix Dynamic Server, or Sybase, use the same procedure that was used to create the content store database.

  For DB2 on z/OS, use the instructions in "Suggested Settings for Creating the DB2 Logging Database on z/OS" (p. 250).

- Set up the database connectivity.

- Specify the log messages repository.

### Suggested Settings for Creating the DB2 Logging Database on z/OS

The database you create must contain the specified configuration settings.

Use the following checklist to help you set up the logging database on DB2.

- Log on to the z/OS system as a user with administrator privileges in DB2 on z/OS.

- Create a database instance, storage group, and a user account for the content store. IBM Cognos uses the credentials of the user account to communicate with the database server.

- Ensure that you allocate a buffer pool with a page size of 8 KB for the database instance.

- For a logging database in DB2 on z/OS, administrators must run a tablespace script to create tablespaces to hold large objects and other data for the logging database, and then grant user rights to the table. For information about running the tablespace script, see "Create Tablespaces for DB2 Logging Database on z/OS " (p. 250).

### Create Tablespaces for DB2 Logging Database on z/OS

A database administrator must run a script to create a set of tablespaces required for the logging database. The script must be modified to replace the placeholder parameters with ones that are appropriate for your environment.
Ensure that you use the name convention for DB2 on z/OS. For example, all names of parameters must start with a letter and the length must not exceed eight characters. For more information, see the IBM® DB2 Information Center.

**Steps**

1. Connect to the database as a user with privileges to create and drop tablespaces and to allow execution of SQL statements.

2. Open the LS_tablespace_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>IPFSCRIPT_DATABASE</td>
<td>Specifies the name of the logging database.</td>
</tr>
<tr>
<td>IPFSCRIPT_STOGROUP</td>
<td>Specifies the name of the storage group.</td>
</tr>
<tr>
<td>IPFSCRIPT_TABLESPACE</td>
<td>Specifies the name of the tablespace that contains the base tables in the logging database. This tablespace is not for Auxiliary tables.</td>
</tr>
<tr>
<td>IPFSCRIPT_LOB_TABLESPACE</td>
<td>Specifies the name of the tablespace that is allocated for auxiliary tables.</td>
</tr>
<tr>
<td>IPFSCRIPT_BP</td>
<td>Specifies the name of the 8 k buffer pool that is allocated for regular objects.</td>
</tr>
<tr>
<td>IPFSCRIPT_USERNAME</td>
<td>Specifies the user account that accesses the logging database.</td>
</tr>
</tbody>
</table>

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

3. Save and run the script.

4. Grant the IBM Cognos® user rights to the tablespaces that were created when you ran the LS_tablespace_db2zOS.sql script file:
   - Open the LS_rightsGrant_db2zOS.sql script file, which is located in the c10_location/configuration/schemas/logging/db2zOS directory.
   - Replace the parameter values with those that are appropriate for your environment.
     **Tip:** Ensure you use the same values that you used when you created the buffer pools and user account.
   - Save and run the LS_rightsGrant_db2zOS.sql script.

The logging database is created.
Set Up the 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.

**Note:** 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 database client software (DB2 only) is required only on the Application Tier Components computer with the remote log server that connects to the logging database.

**Microsoft SQL Server Database**

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.

**Oracle or Sybase Database**

If you use an Oracle, Informix Dynamic Server, or Sybase 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.

**DB2 Database**

IBM® Cognos uses JDBC connectivity to access the database used for the logging database.

For a DB2 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 also set up the database client software and 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.

If you use DB2 on Windows®, Linux® or UNIX® as your logging database you must choose whether to use the type 2 or type 4 JDBC driver depending on how you want to connect to the logging database.

For more information about JDBC driver options for a DB2 database, see "JDBC Driver Options for Using DB2 Database as a Content Store" (p. 90).

**Steps for Oracle**

1. On the computer where Oracle is installed, go to the ORACLE_HOME/jdbc/lib directory.
2. Copy the ojdbc5.jar file to the c10_location/webapps/p2pd/WEB-INF/lib directory on computers where Content Manager or Application Tier Components is installed.
If the directory contains the classes12.jar file or ojdbc14.jar file, delete it before installing the ojdbc5.jar file.

**Steps for DB2 on Linux, UNIX, and Windows**

1. If you are using type 2 JDBC connectivity, install the DB2 client software on the Content Manager computers.
   - If you use type 4 JDBC connectivity for DB2, you are not required to install the DB2 client software where Content Manager is installed.
   - For more information about the differences between type 2 and type 4 drivers, see "JDBC Driver Options for Using DB2 Database as a Content Store" (p. 90).

2. If you are using type 2 JDBC connectivity, and the logging database is on a different computer than log server, configure a database alias to the logging database.
   - On Windows, run the DB2 Client Configuration Assistant.
   - On UNIX or Linux, use the DB2 command line interface.

   **Note:** If the logging database and log server are on the same computer, the logging database name automatically becomes the alias.

3. On Windows, stop the DB2 services and the HTML Search Server.

4. Copy the following files from the 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, db2jcc\_license\_cu.jar
     - for DB2 on z/OS, db2jcc\_license\_cisuz.jar

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

5. On Windows, restart the DB2 services and the HTML Search Server.

6. Repeat this entire procedure on the IBM Cognos computers where the software must be installed.

**Steps for DB2 on z/OS**

1. Go to the DB2\_installation/sqllib/java directory.

2. Copy the following files to the c10\_location/webapps/p2pd/WEB-INF/lib directory and c10\_location/bin directories.
   - the universal driver file, db2jcc.jar
   - the license file, for example, db2jcc\_license\_cisuz.jar

   If you are using a DB2 database on z/OS for the logging database, you must use type 4 JDBC connectivity.
The driver version must be at least JCC 3.7 from Linux, UNIX, or Windows version 9.1 fix pack or JCC 3.42 from Linux, UNIX, or Windows version 9.5 fix pack 2.

**Steps for Informix**
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 Application Tier Components are installed.
   - the universal driver file, db2jcc.jar
   - the license file, db2jcc_license_cisuz.jar

**Steps for Sybase**
1. On the computer where Sybase is installed, enable the JDBC driver using the following script:
   *Sybase_location*/jConnect-6/sp/sql_server12.5.sql
2. Go to the *Sybase_location*/jConnect-6/classes directory.
3. Copy the jconn3.jar file to the *c10_location*/webapps/p2pd/WEB-INF/lib directory on the appropriate Content Manager or Application Tier Components computers.

**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:
- remote log server
- file
- database
- UNIX® or Linux® syslog or the Windows® NT Event log

For information about log messages, see the *Architecture and Deployment Guide*.

**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.
**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.

**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

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 specify a database as a repository, ensure that you

- created the logging database
- set up the database client

**Steps for DB2 for UNIX, Linux, and Windows**

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 its local log server</td>
<td>Set the Enable TCP property to True. UDP provides faster communication with a lower risk of lost connections than TCP. However, the risk of losing a local TCP connection is low. TCP is always used for communication between a local log server and a remote log server.</td>
</tr>
<tr>
<td>Change the number of threads available to the local log server</td>
<td>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.</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.

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.

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 **Administration and Security Guide**.

### Steps for DB2 for z/OS

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 its local log server</td>
<td>Set the <strong>Enable TCP</strong> property to <strong>True</strong>. 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.</td>
</tr>
<tr>
<td>Task</td>
<td>Action</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Change the number of threads available to the local log server</td>
<td>Type the value in the <strong>Local log server worker threads</strong> property.</td>
</tr>
<tr>
<td></td>
<td>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.</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 **Database** and then click **OK**.

7. In the **Explorer** window, under **Logging**, right-click the database name, and click **New resource > Database**.

8. In the **Name** box, type the name of the repository.

9. In the **Type** list, click **DB2 database** and then click **OK**.

10. In the **Properties** window, type the **Database server and port number**, **User ID and password**, and the **z/OS Database name**.

    Ensure that the User ID is the same as the value you specified for the **IPFSCRIPT_USERNAME** parameter in the **LS_tablespace_db2zOS.sql** script file (p. 250).

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

12. In the **Properties** window, next to **Advanced properties**, click inside the **Value** box, and then click the edit button 📊.

13. Click **Add**, and then add the configuration parameter names and values from the following table:

    | Parameter Name                   | Value                                                                                                                                                                                                                                                                                                                                 |
    |---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
    | IPFSCRIPT_CREATE_IN             | The base tables location.                                                                                                                                                                                                                                             |
    |                                 | For example, databaseName.baseTablespaceName                                                                                                                                                                                                                     |
    | IPFSCRIPT_STOGROUP              | The name of the storage group.                                                                                                                                                                                                                                        |
    | IPFSCRIPT_DATABASE              | The name of logging database.                                                                                                                                                                                                                                        |
    | IPFSCRIPT_LOB_TABLESPACE       | The name of the tablespace that is reserved for auxiliary tables in the logging database.                                                                                                                                                                             |
14. From the **File** menu, click **Save**.

15. 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.

**Steps for Informix**

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>
<tbody>
<tr>
<td>Use TCP between IBM Cognos components on a computer and its local log server</td>
<td>Set the <strong>Enable TCP</strong> property to <strong>True</strong>. 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.</td>
</tr>
<tr>
<td>Change the number of threads available to the local log server</td>
<td>Type the value in the <strong>Local log server worker threads</strong> 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.</td>
</tr>
</tbody>
</table>

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 button.

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 Administration and Security Guide.

You must install Sun Java JDK or Java Software Development Kit for IBM before you can enable user-specific logging.

**Configure JMX Connection Information using IBM Cognos Configuration**

Configure JMX connection information in IBM Cognos Configuration by specifying a cookie value and then setting the JMX port and credentials.

**Steps**

1. On the computer where Content Manager is installed, start IBM Cognos Configuration.
2. In the Explorer window, under Security, click Authentication.
3. In the Properties window, for Advanced properties, click in the Value column and then click the edit button.
4. In the **Value - Advanced properties** dialog box, click **Add**.

5. In the new row, type **newCookie** as the name, type **true** as the value, and then click **OK**.

   The values are case-sensitive.

6. In the **Explorer** window, click **Environment**.

7. 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 button 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**.

8. Save the configuration.

**Configure JMX Connection Information in a Deployment Properties File**

To support the JMX settings on your application server, specify the JMX port in the p2pd deployment properties file.

**Steps**

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.

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 *Administration and Security Guide*.

**Changing Global Settings**

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
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 "Install Translated Product Documentation" (p. 177).

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.

Steps
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.

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.

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.

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.

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.

Steps

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 code for the country 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.

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. For more information, see "Install and Configure Additional Language Fonts" (p. 178).

**Steps**

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.
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.

**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.

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.

**Steps**

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 `de` 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.

Steps
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 Administration and Security Guide.

Steps

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.

Change 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>
<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-kkr</td>
</tr>
<tr>
<td>Korean (KSC-5601)</td>
<td>ksc_5601</td>
</tr>
</tbody>
</table>
### Steps

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**.

### Customize 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>
<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, .int, .mil, .net, or .org</td>
<td>.name.suffix (two dots)</td>
</tr>
<tr>
<td></td>
<td>Example: .mycompany.com</td>
</tr>
</tbody>
</table>
### Format for domain

<table>
<thead>
<tr>
<th>Host</th>
<th>Format for domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>other</td>
<td>.name1.name2.suffix (three dots)</td>
</tr>
<tr>
<td></td>
<td>Example: .travelinfo.co.nz</td>
</tr>
</tbody>
</table>

### Steps

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.

### Changing the Gateway

To improve Web server performance, you can configure IBM® Cognos® to use alternate gateways that replace the default CGI program. You can use one of the following gateways:

- **Microsoft® Internet Server Application Programming Interface (ISAPI)** for Microsoft Internet Information Services on Windows®
- **Apache Web Server** module for Apache Web Server and IBM HTTP Server
- **Servlet Gateway Java™** application for application servers

There is no additional Web server configuration required to use ISAPI. To access IBM Cognos components using ISAPI, in IBM Cognos Configuration, change the cognos.cgi portion of the Gateway URI property to cognosisapi.dll. Then specify the ISAPI URI, http://host_name/ibmcognos/isapi, in your browser. If you use multiple Content Managers for failover protection, configure IBM Cognos to use an ISAPI gateway instead of the default CGI gateway. Otherwise, performance may be affected after failover.

Before you change the gateway, first ensure that the default CGI gateway and your configuration work in your environment.
Configure the Gateway for IBM Cognos Apache Web Server Module

IBM® Cognos® provides three Apache modules. Use IBM Cognos Apache module for Apache Server 1.3.x. Use IBM Cognos Apache 2 module for Apache Server 2.0.x and IBM HTTP Server 6.1. Use IBM Cognos Apache 2.2 module for Apache Server 2.2.x and IBM HTTP Server 7.1.

Steps for Apache Server 1.3.x
1. Stop Apache Web Server.
2. Append the c10_location/cgi-bin directory to the appropriate environment variable:
   - On Solaris or Linux®, LD_LIBRARY_PATH
   - On HP-UX, SHLIB_PATH
   - On AIX, LIBPATH
3. On HP-UX PA-RISC, do the following:
   - Ensure that the LD_PRELOAD environment variable contains /usr/lib/libcl.2.
   - Set the COG_CGIBIN_DIR environment variable to c10_location/cgi-bin.
4. Go to the Apache_installation/conf directory.
5. Open the httpd.conf file in an editor.
6. Add the following to the end of the load module list:
   LoadModule cognos_module "c10_location/cgi-bin/mod_cognos.suffix"
   where suffix is as listed in the following table:

<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</td>
<td>so</td>
</tr>
<tr>
<td>HP-UX PA-RISC</td>
<td>sl</td>
</tr>
<tr>
<td>HP-UX IA, Linux®</td>
<td>so</td>
</tr>
</tbody>
</table>

7. Add the following to the end of the add module list:
   AddModule mod_cognos.cpp
8. Add the following Apache Directive:
   ScriptAlias /ibmcognos/cgi-bin "c10_location/cgi-bin"
   Alias /ibmcognos "c10_location/webcontent"
   <Directory "c10_location/webcontent">
The `<Directory>` directive is optional.

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

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

```
<Location /ibmcognos/cgi-bin/mod_cognos.suffix>
  SetHandler cognos-handler
</Location>
```

Enter the code exactly as specified, except for `suffix`. Replace `suffix` with the appropriate value from the table in step 6.

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

```
<Location /ibmcognos/cgi-bin/diag_mod_cognos.suffix>
  SetHandler cognos-handler
</Location>
```

Enter the code exactly as specified, except for `suffix`. Replace `suffix` with the appropriate value from the table in step 6.

11. On Windows, Solaris, and AIX, add the following to the user directory section:

```
<IfModule mod_cognos.cpp>
  CGIBinDir "c10_location/cgi-bin"
</IfModule>
```

12. Save and close the file.


14. Users must then specify the Apache module URI in their browser, as follows:

   `http://host_name:port/ibmcognos/cgi-bin/cognos_module`

   The cognos_module string must be entered exactly as specified.

   For example,

   `http://123.432.154.12:5562/c10/cgi-bin/cognos_module`

**Steps for Apache Server 2.0.x and IBM HTTP Server 6.1**

1. Stop the Web Server.

2. 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`
3. On HP-UX PA-RISC, ensure that the LD_PRELOAD environment variable contains /usr/lib/libcl.2.

4. Go to the Webserver_installation/conf directory.

5. Open the httpd.conf file in an editor.

6. For successful portal integration, ensure that both SERVERNAME and SERVER_PORT are specified in the ServerName property.

7. Add the following to the end of the load module list:
   
   ```
   LoadModule cognos_module "c10_location/cgi-bin/mod2_cognos.suffix"
   
   where suffix is as as listed in the following table:
   ```

<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</td>
<td>so</td>
</tr>
<tr>
<td>HP-UX PA-RISC</td>
<td>sl</td>
</tr>
<tr>
<td>HP-UX IA, Linux®</td>
<td>so</td>
</tr>
</tbody>
</table>

8. Add the following Apache Directive:

   ```
   ScriptAlias /ibmcognos/cgi-bin "c10_location/cgi-bin"
   Alias /ibmcognos "c10_location/webcontent"
   <Directory "c10_location/webcontent">
   Options Indexes MultiViews
   </Directory>
   
   The <Directory> directive is optional.
   
   Tip: Ensure that you define the ibmcognos/cgi-bin alias before the ibmcognos alias.
   ```

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

   ```
   <Location /ibmcognos/cgi-bin/mod2_cognos.suffix>
   SetHandler cognos-handler
   </Location>
   
   Enter the code exactly as specified, except for suffix. Replace suffix with the appropriate value from the table in step 6.
   ```

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

    ```
    <Location /ibmcognos/cgi-bin/diag_mod2_cognos.suffix>
    SetHandler cognos-handler
    </Location>
    ```
11. Add the following to the user directory section:

```xml
<IfModule mod2_cognos.c>
    CGIExecDir "c10_location/cgi-bin"
</IfModule>
```

12. Save and close the file.

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

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


15. Users must then specify the Apache module URI in their browser, as follows

   ```
   http://host_name:port/ibmcognos/cgi-bin/cognos_module
   ```

   The cognos_module string must be entered exactly as specified.

   For example,

   ```
   http://123.432.154.12:5562/c10/cgi-bin/cognos_module
   ```

**Steps for Apache Server 2.2.x and IBM HTTP Server 7.0**

1. Stop the Web server.

2. 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

3. On HP-UX PA-RISC, ensure that the LD_PRELOAD environment variable contains `/usr/lib/libcl.2`.

4. Go to the `Apache_installation/conf` directory.

5. Open the httpd.conf file in an editor.

6. For successful portal integration, ensure that both SERVERNAME and SERVER_PORT are specified in the ServerName property.

7. 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:
### 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</td>
<td>so</td>
</tr>
<tr>
<td>HP-UX PA-RISC</td>
<td>sl</td>
</tr>
<tr>
<td>HP-UX IA, Linux®</td>
<td>so</td>
</tr>
</tbody>
</table>

8. Add the following Apache Directive:

ScriptAlias /ibmcognos/cgi-bin "c10_location/cgi-bin"

Alias /ibmcognos "c10_location/webcontent"

<Directory "c10_location/webcontent">
Options Indexes MultiViews
</Directory>

The `<Directory>` directive is optional.

Tip: Ensure that you define the ibmcognos/cgi-bin alias before the ibmcognos alias.

9. Add the following Apache Directive:

ScriptAlias /ibmcognos/cgi-bin "c10_location/cgi-bin"

Alias /ibmcognos "c10_location/webcontent"

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

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

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

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

Enter the code exactly as specified, including the cognos_module string.

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

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

   Enter the code exactly as specified, including the diag_cognos_module string.

12. On Windows, Solaris, and AIX, add the following to the user directory section:

   <IfModule mod2_2_cognos.c>
      CGIBinDir "c10_location/cgi-bin"
   </IfModule>

13. Save and close the file.


15. Users must then specify the Apache module URI in their browser, as follows

   http://host_name:port/ibmcognos/cgi-bin/cognos_module

   The cognos_module string must be entered exactly as specified.

   For example,

   http://123.432.154.12:5562/c10/cgi-bin/cognos_module

**Configure the Servlet Gateway**

If you configure the IBM® Cognos® Servlet Gateway to run on a supported application server, your environment does not require a Web server. The application server and the IBM Cognos Servlet Gateway replace the functions provided by a Web server and other IBM Cognos gateways.

Before you build and deploy the IBM Cognos Servlet Gateway, ensure the following:

- The application server is installed and running on each computer where the servlet gateway is to be installed.
- IBM Cognos Gateway components are installed on the same system as the application server.
- The IBM Cognos dispatcher and Content Manager components are installed and running in the environment.
- The application server user account has full access permissions for the IBM Cognos installation.

Create a new UNIX® or Linux® group named ibmcognos. 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 ibmcognos group, and change the file
permissions for all IBM Cognos files to GROUP READABLE/WRITABLE/EXECUTABLE. For simplicity, you can also use the application server user account to install and run IBM Cognos components.

To set up the IBM Cognos Servlet Gateway to run on your application server, do the following:

- 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.

- Check that IBM Cognos components are properly set up.

- Set environment variables.

- Configure IBM Cognos Servlet Gateway to run on the application server.

- Change the application server startup script, if necessary.

- Configure application server properties and deploy IBM Cognos Servlet Gateway.

- Enable SSL, if required.

- Configure the Web server.

You can then access IBM Cognos components using the IBM Cognos Servlet Gateway, by entering the gateway URI. For example,

\[
http[s]:host_name:port/ServletGateway
\]

The IBM Cognos Servlet Gateway URI is case-sensitive.

**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
- IPv6: [2001:0db8:0000:0000:0000:148:57ab]: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.

**Steps to Set the IP Version**

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.

**Steps to Manually Enable the IPv6 Option When Opening IBM Cognos Configuration**

1. Go to the c10_location/bin 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.

**Steps to Always Open IBM Cognos Configuration With the IPv6 Option on Windows**

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.
Configure the Router to Test Dispatcher Availability

If you use a router to distribute requests to IBM® Cognos® dispatchers, and the router can test the availability of a server using a test URL, you can configure the router to test the availability of an IBM Cognos dispatcher.

**Step**
- Configure the router to use a URL with the path /p2pd/servlet/ping.

  If the dispatcher is not ready, the following response is returned:

  503 Service Unavailable

  If the dispatcher is ready, the following response is returned:

  200 OK

Update 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.

**Steps**
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.

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.

Steps
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:
     ```bash
     ./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 assign the user account to the services, ensure that a user account is set up with a password that never expires.

Steps
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: Configuration Options
Chapter 11: 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 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 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 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.
Chapter 11: Configuring Portal Services

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.

Steps
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.

You can now deploy the IBM Cognos portlets to your portal server. For instructions, see the 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.

If your security infrastructure requires you to use another method for single signon, use one of the following methods:

- "Enable Single Signon for WebSphere Portal Using the Application Server" (p. 289)
- "Enable Single Signon for Oracle WebCenter Interaction Portal Using Basic Authentication" (p. 289)
- "Enable Single Signon for Oracle WebCenter Interaction Portal Using SiteMinder" (p. 290)

❑ 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.

Steps
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 NTLM, LDAP, or IBM Cognos Series 7 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 WebPart (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.

Steps to Configure the Required Namespaces
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

\[(\text{uid}=$\{\text{replace}($\{\text{environment}("\text{REMOTE}\_\text{USER}"\})","SharePoint\_\text{Server}\",""\})})\]

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 namespace ID of the LDAP, NTLM, or IBM Cognos Series 7 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 of type LDAP, NTLM, or IBM Cognos Series 7.
   
   - 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.

**Steps to Configure Access to the Portal Services Web Content**

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
5. From the File menu, click **Save**.

**Steps to Configure the Cognos Portlets for WebSphere Portal**

1. For each Cognos portlet application, click **Modify Parameters**.

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
     
     \[ \text{Gateway URI}/wsrp/cps4/portlets/nav?wsdl&b_action=cps.wsdl \]
     
     Example for a CGI gateway:
     
     \[ \text{http://myserver/ibmcognos/cgi-bin/cognos.cgi/wsrf/cps4/portlets/nav?wsdl&b_action=cps.wsdl} \]
     
     Example for a servlet gateway:
     
     \[ \text{http://172.0.16.1:9500/wsrf/cps4/portlets/nav?wsdl&b_action=cps.wsdl} \]

   - For Cognos Extended Applications
     
     \[ \text{Gateway URI}/wsrp/cps4/portlets/sdk?wsdl&b_action=cps.wsdl \]
     
     Example for a CGI gateway:
     
     \[ \text{http://myserver/ibmcognos/cgi-bin/cognos.cgi/wsrf/cps4/portlets/sdk?wsdl&b_action=cps.wsdl} \]
     
     Example for a servlet gateway:
     
     \[ \text{http://172.0.16.1:9500/wsrf/cps4/portlets/sdk?wsdl&b_action=cps.wsdl} \]

   - For Metrics Manager Watchlist portlets
     
     \[ \text{Gateway URI}/wsrp/cps4/portlets/cmm?wsdl&b_action=cps.wsdl \]
     
     Example for a CGI gateway:
     
     \[ \text{http://myserver/ibmcognos/cgi-bin/cognos.cgi/wsrf/cps4/portlets/cmm?wsdl&b_action=cps.wsdl} \]
     
     Example for a servlet gateway:
     
     \[ \text{http://172.0.16.1:9500/wsrf/cps4/portlets/cmm?wsdl&b_action=cps.wsdl} \]

**Steps to Configure the Remote Server for Oracle WebCenter Interaction Portal**

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>
<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/cognosisapi.dll/wsrp/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.

Single signon is configured.

**Steps to Configure Properties for the Cognos WebPart for SharePoint Portal**

1. Using a plain ASCII editor, such as Notepad, edit the web.config file in the `drive\Program Files\Common Files\Microsoft Shared\web server extensions\12\CONFIG` directory.
2. Find the following string:
   ```xml
   <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 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 NTLM, LDAP, or IBM® Cognos® Series 7 authentication namespace to provide single signon.

**Steps**

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/
```


- 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 SiteMinder**

If you use eTrust 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 SiteMinder authentication namespace in IBM® Cognos® BI. WebCenter Interaction Portal sends the SiteMinder active authentication token to the remote server, which sends the token to the IBM Cognos gateway.

**Steps**

1. In IBM Cognos Configuration, configure a 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 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/
   ```

   - Change the `cps_auth_namespace` property to the namespace that you want to use for authentication.
Chapter 12: Configuring IBM Cognos BI for an Application Server other than Tomcat

IBM® Cognos® Business Intelligence installs and uses Tomcat as the application server by default. You can choose to run IBM Cognos BI within another supported server instead:

- BEA WebLogic Server
- IBM WebSphere® Application Server
- Oracle Application Server
- Red Hat JBoss
- Sun Java™ Systems Application Server (for Microsoft® Windows®, Linux®, and Solaris operating systems only)

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.

To review an up-to-date list of environments supported by IBM Cognos products, such as operating systems, patches, browsers, Web servers, directory servers, database servers, and application servers, visit the IBM Cognos Customer Center (www.ibm.com/software/data/cognos/customercenter/).

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.

You can choose to run the IBM Cognos Servlet Gateway on a supported application server instead of using a Web server (p. 276). 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.

For information about configuring a multi-server distributed installation of IBM Cognos BI in an application server environment, contact the IBM Cognos Customer Center (http://www.ibm.com/software/data/cognos/customercenter/).

IBM Cognos BI must be installed and running prior to configuring and deploying the IBM Cognos Servlet Gateway.

To set up IBM Cognos BI to run on your application server, do the following:

- Create a separate JVM instance, if necessary.
- Create additional profiles, if you are distributing IBM Cognos BI components
- 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.

Import any backed up content store data.

After setting up IBM Cognos BI to run on your application server, you can perform some additional configuration tasks to customize the behavior of IBM Cognos components to better suit your reporting environment (p. 219).

Tip: Do not use install paths that contain spaces for the application server or IBM Cognos BI. Spaces interfere with the internal scripts and command parameters. If you must use an install path that includes spaces, use the 8.3 DOS naming convention when referring to these locations.

Create a Separate JVM Instance

To eliminate potential Java™ class or system resource conflicts, IBM® Cognos® BI must be run in a Java Virtual Machine (JVM) instance isolated from other existing applications. This ensures that IBM Cognos BI does not affect any existing customer applications. When possible, IBM Cognos BI must be installed in a 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.

An isolated JVM instance can be established by creating one of the following:

- a separate managed server in BEA WebLogic
- a separate server instance in IBM WebSphere®
- a separate OC4J instance in Oracle 10g Application Server
- a separate server instance for Red Hat JBoss
- a separate domain for Sun Java Systems Application Server

If you are using the IBM Cognos Servlet Gateway, it must be run in an instance that is separate from IBM Cognos BI.
Create Additional Profiles to Distribute IBM Cognos BI Components for Linux on System z

If you are installing IBM® Cognos® BI components in multiple locations for Linux® operating system on System z, you must create additional profiles for your WebSphere® application server. Each profile can be used to run a IBM Cognos BI component.

For example, you can have the Content Manager component installed and running using one WebSphere profile, while the Application Tier Components can run using another WebSphere profile. The profiles allow each component to run using unique port numbers.

A script named create_profile.sh is provided to allow you to create additional profiles in WebSphere. You can use the default profile for one IBM Cognos BI component. But, for each additional IBM Cognos BI component you install, you must create an additional profile.

When you run the script, you are prompted for the location of your WebSphere installation, and you will be allowed to review and change the port numbers the script will use for the profile.

While the script will configure many port numbers, the port number for WC_adminhost is the port number needed to launch the WebSphere administration console in a browser. The port number for WC_defaulthost is the port number on which the IBM Cognos services, such as the dispatcher, will run. If you intend to use SSL for IBM Cognos BI, the port numbers for WC_adminhost_secure and WC_defaulthost_secure are needed to configure and run IBM Cognos BI components.

To run the script you must have the same permissions as were required to install WebSphere.

Steps
1. Go to the c8_location/C8SE directory.
2. Run the script using the following command:
   
   `/create_profile.sh profile_name`

   where `profile_name` is the name of profile the script will create. The default profile created when you installed WebSphere is named server1. You must enter a different profile name.

3. When prompted, do one of the following:
   - Enter Y to review or change the port numbers the script will use for the profile.
     When you enter Y, a properties file is opened in the vi editor. Use the vi editor commands to edit and save the file.
   - Press any other key to run the script using the selected port numbers. The script will use available port numbers.

   When the script has finished, you must start WebSphere with your new profile.

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 BI, the database for the content store must be set up. Install and configure the database clients, if required (p. 131), 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 (p. 234). 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 ibmcognos. 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 ibmcognos group and change the file permissions for all IBM Cognos files to GROUP READABLE/WRITABLE/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 BI 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 \texttt{c10\_location/configuration} directory. Cryptographic keys exist if this directory includes the following subdirectories: \texttt{csk}, \texttt{encryptkeypair} or \texttt{signkeypair}.

Steps

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 \textit{Administration and Security Guide}.

2. In IBM Cognos Configuration, from the \textit{File} menu, click \textbf{Export As} and save the configuration information in a decrypted format. When naming the file, use a name such as "\texttt{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
   
   - \texttt{c10\_location/configuration/cogstartup.xml}
   
   - \texttt{c10\_location/configuration/caSerial}
   
   - \texttt{c10\_location/configuration/cogconfig.prefs}
   
   - \texttt{c10\_location/configuration/coglocale.xml}
   
   The directories are
   
   - \texttt{c10\_location/configuration/csk}
   
   - \texttt{c10\_location/configuration/encryptkeypair}
   
   - \texttt{c10\_location/configuration/signkeypair}

5. Delete the \texttt{caSerial} and \texttt{cogconfig.prefs} files and the three directories: \texttt{csk}, \texttt{encryptkeypair}, and \texttt{signkeypair}.

6. Replace the \texttt{c10\_location/configuration/cogstartup.xml} file with the file that contains the data exported from IBM Cognos Configuration (for example, "\texttt{decrypted.xml}").
   
   In the \texttt{c10\_location/configuration} directory, the file must use the name "\texttt{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" (p. 300).

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, WebLogic ships with setEnv.cmd or setEnv.sh, and Oracle ships with iasenv.bat or iasenv.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.

Steps

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>
<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.
Tip: To install multiple instances of IBM Cognos BI 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.

Note: The CRN_ROOT and COG_ROOT variables are no longer required in a non-clustered environment and should be removed if they were used in a previous installation.

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.

Adjust the Default Connection Time-out for IBM Cognos BI

The default connection pool time-out value used in IBM® Cognos® BI is 25 seconds. Some application servers, such as IBM WebSphere®, use a shorter value for the default connection time-out. To avoid conflicts between the default connection time-out settings, set the connection pool time-out value in IBM Cognos BI to a shorter duration than that configured for the application server.

Steps

1. Using an editor, open the c10_location\configuration\BIBusTK_Config.xml file.
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 on every computer where you installed IBM Cognos BI.

The setting will be applied when you deploy IBM Cognos BI to the server instance that you create for it.

Configure IBM Cognos Components to Run Within the Application Server

IBM® Cognos® BI 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 and then copy the security provider files before you run IBM Cognos Configuration to ensure valid encryption keys are generated.

**Steps**

1. From the `c10_location/bin` directory, start IBM Cognos Configuration:
   - On Microsoft® Windows® operating system, type `cogconfig.bat` in a command window or select IBM Cognos Configuration from the Start menu.
   - On UNIX® or Linux® operating systems, type `cogconfig.sh`

   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.

2. 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.
3. 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.

4. 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.

5. 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 (p. 219).

6. Save the configuration.

New cryptographic keys are created using the JVM that is defined by the JAVA_HOME variable.

7. Close IBM Cognos Configuration.

### 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.

**Steps**

1. Open the WebLogic9_location/common/bin/commEnv.sh file.

2. Modify the file to include the following command:
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 BI. 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 BEA WebLogic Server, you must make changes to the application server startup script. The startup script must be modified to specify Java Virtual Machine (JVM) settings. For JBoss, you must also specify a log4j argument. For WebLogic 9, use the Administration Console to modify the WebLogic environment.

If you are using IBM WebSphere Application Server or Oracle Application Server, no changes to its startup script are required unless you want to add the environment variable changes. If you do make changes, the Administrative Console can be used.

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.

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

Steps for WebLogic

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 (UNIX® operating system) or startManagedWebLogic.cmd (Microsoft® Windows® operating system).

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:
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.

**Steps for JBoss**

1. Go to the JBoss_location/bin directory and open the application server startup script in an editor. Do one of the following:
   - For Windows, open run.bat
   - For UNIX or Linux® operating systems, open run.sh

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 Deploy IBM Cognos Components

You must configure application server properties and deploy the IBM® Cognos® components.

Steps for WebSphere

1. Start the WebSphere® Application Server, and then access the WebSphere Administrative Console.

2. Create a new server instance into which the IBM Cognos BI 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. 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.

6. Stop and then restart the WebSphere application server instance used for IBM Cognos components.

7. 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.

Steps for WebLogic

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

-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

-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.

**Steps for Oracle Application Server Release 3**

1. Create an OC4J instance for IBM Cognos components to run within.
2. On Windows only, comment out the following entries in the `Oracle_location\j2ee\Cognos_OC4j_instance\config\global-web-application.xml` file:

```xml
<welcome-file-list>
  <welcome-file>index.html</welcome-file>
  <welcome-file>default.jsp</welcome-file>
  <welcome-file>index.htm</welcome-file>
  <welcome-file>index.jsp</welcome-file>
</welcome-file-list>
```


4. Add an environment variable that references the `installation_location/bin` directory and set variables for data sources.

   Here is an example for Windows and DB2:

   ```xml
   <environment>
     <variable id="PATH" value="c10_location/bin" append="true"/>
     <variable id="DB2DIR" value="location"/>
     <variable id="DB2INSTANCE" value="instance_name"/>
     <variable id="INSTHOME" value="location"/>
   </environment>
   ``

   The following table lists the environment variables for each operating system that must reference the `c10_location/bin` directory.

<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</td>
<td>LD_LIBRARY_PATH</td>
</tr>
<tr>
<td>HP-UX</td>
<td>SHLIB_PATH</td>
</tr>
</tbody>
</table>

5. Set the memory used by the JVM.

   A minimum of 256 MB and a maximum of 768 MB 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.

   Here is an example:

   ```xml
   <data id="java-options" value="-server -Xmx768m -XX:MaxNewSize=384m -XX:NewSize=192m -XX:MaxPermSize=128m -classpath c10_location\bin;c10_location\webapps\p2pd\WEB-INF\lib -"
   ``

6. Define the OC4J userThreads setting.

   Here is an example:

   ```xml
   <data id="oc4j-options" value="-userThreads"/>
   ```
7. Add the -Dcom.sun.management.jmxremote option to the start parameters section.
   For example:

   ```xml
   <category id="start-parameters">
     <data id="java-options" value="-Dcom.sun.management.jmxremote"/>
   </category>
   ```

   You can also set this by selecting the Enable J2SE 5.0 Platform MBeans option in the server properties page for the OC4J instance.

8. Save and close the Oracle_location/opmn/conf/opmn.xml file.

9. Deploy the IBM Cognos application file (named p2pd.ear for IBM Cognos BI or ServletGateway.ear for IBM Cognos Servlet Gateway, by default) created by IBM Cognos Configuration.
   The value of the Map to URL parameter must be the same as the context root value entered in IBM Cognos Configuration.

10. Start the OC4J instance that you created for IBM Cognos components.

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.

**Steps for JBoss**

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,

   ```xml
   <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"/>
   </Service>
   ```

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

   ```cmd
   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.

Steps for Sun Java System Application Server

1. Use the Sun Java System Application Server Admin Console to add a new JVM Option to set the XML Parser that will be used by the IBM Cognos Application. For example:


2. Add a JVM Option to set the Maximum Java Heap Size to limit the maximum amount of memory that can be used by the Java process.

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.

For example, add "-Xmx768M" to set 768M of memory as a maximum value for the Java process.

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.

3. Increase the "Maximum number of request processing threads" from the default of 5 to a value appropriate for your environment.

Tip: Start with a value of 250. If the value is too low, system instability and failed processes occur. If the value is too high, system resources are reserved unnecessarily.

4. Copy the c10_locat1on\webapps\p2pd\WEB-INF\lib\xercesImpl.jar file to SJSAS_location\domains\<domain name>\lib\ext.

5. Deploy the IBM Cognos application file (named p2pd.ear for IBM Cognos BI or ServletGateway.ear for IBM Cognos Servlet Gateway, by default) created by IBM Cognos Configuration.

   In the Sun Java System Application Server Admin Console, go to Common Tasks > Applications > Enterprise Applications, and use the local packaged file option to select the ear file you want to deploy.

Enable SSL

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 IBM Cognos components.

Steps

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 `installation_location/bin` directory and rename the file to `ca.cer`. This file must be Base-64 encoded X.509 format.

3. From the `installation_location/bin` directory:
   - On Microsoft® Windows® operating system, type:
     ```
     ThirdPartyCertificateTool.bat -T -i -r ca.cer -k ../configuration/signkeypair/jCAKeystore -p password
     ```
   - On UNIX® or Linux® operating systems, type:
     ```
     ThirdPartyCertificateTool.sh -T -i -r ca.cer -k ../configuration/signkeypair/jCAKeystore -p password
     ```

   You must type `jCAKeystore` as the name of the CA key store.

### Configuring Web Communication

For most types of supported application servers, you use a Web server and an IBM® Cognos® gateway for Web communication. In that situation, follow the steps to configure the Web server.

For information about configuring the WebSphere® Web server plugin, contact the IBM Cognos Customer Center (http://www.ibm.com/software/data/cognos/customercenter/).

If you are using SAP NetWeaver on Microsoft® Windows® operating system 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 the Web Server

For all installations, before you use Web pages generated by IBM® Cognos® BI, you must configure your Web server. You must create virtual directories, or aliases, so that users can connect to IBM Cognos BI in the portal. If 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. The steps for creating an application pool vary depending on your operating system.

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.

**Steps to Create Virtual Directories**

1. 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>

You can use a name other than ibmcognos in the aliases. However, you must use cgi-bin as the
second part of the alias and you must change the virtual directory in the **Gateway URI** property
to match the new IBM Cognos alias.

For Apache Web Server, ensure that you define the ibmcognos/cgi-bin alias before the ibmcognos
alias in the httpd.conf file located in the **Apache_installation/conf** directory. The
ibmcognos/cgi-bin alias must be defined as a ScriptAlias.

2. If you want to use the Report Studio image browser, enable Web Distributed Authoring and
Versioning (WebDAV) on your Web server.

   If you use Apache Web Server, specify a directory in which to enable WebDAV. For information
about configuring WebDAV, see your Web server documentation.

   If you use Microsoft® Internet Information Services (IIS), enable the Read and Directory
Browsing properties for the URL you want to access.

3. For IBM Cognos BI for reporting, set the content expiry on the c10_location/webcontent/pat/
images virtual directory in your Web server.

   Each time a user opens Report Studio, their Web browser checks with the Web server to
determine if images are current. Because there are over 600 images, this can result in excess
network traffic. You can postpone this check until a specified date by using the content expiry
feature of the Web server.

   For information on setting content expiry, see the documentation for your Web server.

   **Note:** When you upgrade, Report Studio users must clear their Web browser cache to get the
latest images.

   If you use Web aliases other than ibmcognos, or your Web server is on another computer, or you
are using Microsoft Internet Application Interface (ISAPI), apache_mod or a servlet gateway, change
the Gateway URI when you configure IBM Cognos components.

**Steps to Create an Application Pool on Windows Server 2008**

1. For the Microsoft® Windows® operating system, from the **Start** menu, select **Control Panel >
Performance and Maintenance > Administrative Tools**.

2. Launch **Internet Information Services (IIS) Manager**.
Web Management Tools and World Wide Web Services are enabled automatically.

3. From the root (your system name and user), select Features View.

4. In the IIS section, launch ISAPI and CGI Restrictions.

5. Select Edit Feature Settings and enable Allow unspecified CGI modules and then click OK.

6. Add your aliases. For example, c10_location/cgi-bin.

7. Select your cgi-bin alias and ensure that Features View is selected.

8. Right-click Application Pools and select Add.

9. In the dialog box, enter a Web alias and the corresponding path to IBM Cognos BI webcontent.

10. Repeat steps 8 and 9 to add the next Web alias.

11. Select Default Web Site.

12. Open Handler Mappings.

13. Select the CGI-cgi mapping.

14. In the right pane, click Revert to Inherited.

15. Expand the application that points to your webcontent location.

16. Expand your cgi-bin application node.

17. Add a mapping that points to *.cgi and name it CGI-cgi.

18. Select the CGI-cgi mapping.

19. In the right pane, click Revert to Inherited.

20. Restart the IIS server.

21. Find the folder that contains cgi-bin (c10_location/cgi-bin) and right-click it.

22. Select the Security tab.

23. Add the Network Services user, granting all permissions except Full Control.

24. Right-click on Cognos service and select Properties.

25. Click the Log On tab.

26. Click This account and enter Network Service as the user.

27. Delete the Password and the Confirm the password values.

28. Click OK.

Configure a Virtual Directory for SAP NetWeaver on Windows

If you are using SAP NetWeaver on Microsoft® Windows® operating system 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 BI or ServletGateway for the IBM Cognos Servlet Gateway). Ensure the virtual directory points to the \c10_location\webcontent folder.

**Step**

- 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**

After you start the application server and the IBM® Cognos® application, unregister any IBM Cognos dispatchers that were previously registered and that are no longer used. For example, unregister any Tomcat dispatchers that are now running under the application server.

You remove dispatchers using IBM Cognos Administration. To access this tool, you must have execute permissions for the Administration secured function.

**Steps**

1. Open IBM Cognos Connection by connecting to the IBM Cognos BI portal and clicking IBM Cognos Content on the Welcome page.
2. In the upper-right corner, 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.

The dispatcher information is removed from Content Manager.

**Import Content Store Data**

If you exported the content store before setting up IBM® Cognos® components to run in your application server (p. 294), import the deployment to restore and encrypt the data using the new encryption keys.

**Steps**

1. Start IBM Cognos BI.
2. Import the entire content store using the Deployment tool.
For more information, see the topic about importing to a target environment in the *Administration and Security Guide*.

**Upgrade to IBM Cognos BI in an Application Server Environment**

If you are upgrading from a supported release to IBM® Cognos® BI, perform the following steps.

**Steps**

1. Back up your existing IBM Cognos information *(p. 294)*.

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.
   
   In WebLogic 8.1, the cache location is `%WL_HOME%\user_projects\domains\domain-name\managed-server-name\.wlnotdelete\extract\crn_p2pd_p2pd\jarfiles`.

3. Uninstall the existing version.

4. Install 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 BI to run within the application server.
   - 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 13: Advanced Configuration Options

Advanced configuration options are changes that you make after installation to the configuration properties of the resources that IBM® Cognos® Business Intelligence components use. You cannot use IBM Cognos Configuration to make these changes. Advanced configuration options enhance security, improve performance, or change the default behavior of IBM Cognos BI components.

Changing the Version of Java Runtime Environment Used by IBM Cognos BI Components

IBM® Cognos® BI components require Java™ Runtime Environment (JRE) to operate.

If you want to change your current JRE, some configuration changes are required. Changing may be appropriate in the following situations:

- You want to use IBM Cognos BI components with an application server that requires a specific JRE version.
- You already use a JRE version with other applications.

The current version provided with IBM Cognos BI is JRE 1.5.0. For more information about the supported JRE versions, see the IBM Cognos Customer Center (http://www.ibm.com/software/data/cognos/customercenter/).

If you are using IBM Cognos BI components in an application server environment, follow the process in "Configuring IBM Cognos BI for an Application Server other than Tomcat" (p. 291). The process includes steps for updating the Java environment.

IBM Cognos Configuration and other IBM Cognos BI components use the JRE referenced by the JAVA_HOME environment variable. On Microsoft® Windows® operating system, if JAVA_HOME is not set, the JRE that is packaged with IBM Cognos BI components is used by default.

Before you begin, ensure that IBM Cognos BI components are installed and that JRE you want to use is installed.

To change JRE versions, do the following:

- Back up existing IBM Cognos data and encryption keys, if required.
- Update the Java environment.
- Import data to the content store, if required.

Back Up Existing IBM Cognos Information

You must back up existing IBM® Cognos® information if IBM Cognos BI 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.

Steps

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 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.

### Update the Java Environment

You can use an existing Java™ Runtime Environment (JRE) or the JRE that is provided with IBM® Cognos® Business Intelligence. To support the cryptographic services in IBM Cognos BI, you may be required to update or set a JAVA_HOME environment variable. Depending on your security policy, 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. To support the cryptographic services in IBM Cognos BI, you may be required to update or set a JAVA_HOME environment variable. Depending on your security policy, you may also have to install the unrestricted Java Cryptography Extension (JCE) policy file.

**JAVA_HOME**

If you want to use your own JRE and have JAVA_HOME set to that location on Microsoft® Windows® operating system or if you are installing on a UNIX® or Linux® operating system, you must update JAVA_HOME for the cryptographic services.

On Windows, you can set JAVA_HOME as a system variable or a user variable. If you set it as a system variable, it may be necessary to restart your computer for it to take effect. If you set it as a user variable, set it so that the environment in which Tomcat (or other application server) is running can access it.

If you do not have a JAVA_HOME variable already set on Windows, the JRE files provided with the installation will be used, and you do not have to update any files in your environment. If JAVA_HOME points to a Java version that is not valid for IBM Cognos BI, you must update JAVA_HOME with the path to a valid Java version.

If you do not have a JAVA_HOME variable already set on Windows, the JRE files provided with the installation will be used, and you do not have to update any files in your environment. If JAVA_HOME points to a Java version that is not valid for IBM Cognos BI, you must update JAVA_HOME with the path to a valid Java version.
Unrestricted JCE Policy File

Whether you use the default Windows JRE or download a JRE for UNIX or Linux, the JRE includes a restricted policy file that limits you to certain cryptographic algorithms and cipher suites. If your security policy requires 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.

Steps

1. Ensure that the JAVA_HOME environment variable is set to the JRE location.
   For example, to set JAVA_HOME to the JRE files provided with the installation, the path is c10_location/bin/jre/version.
2. Start IBM Cognos Configuration.
3. Save the configuration.
   IBM Cognos Configuration generates new keys and encrypts the data.
4. Download and install the unrestricted java policy file from the following location:

Import Content Store Data

If you exported the content store before changing the JVM, import the deployment to restore and encrypt the data using the new encryption keys.

Step

- To import the content store data, start the IBM® Cognos® BI service and import the entire content store using the Deployment tool. For more information, see the topic about importing to a target environment in the Administration and Security Guide.

Configuring IBM Cognos BI Components to Use a 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. You can configure IBM Cognos BI components to use another certificate authority, if you already have an existing certificate authority, such as iPlanet or Microsoft®, in your reporting environment.

When you configure IBM Cognos BI components to use another certificate authority, ensure that you specify the same information in both the command line utility tool and in IBM Cognos Configuration.

Use the following checklist to configure IBM Cognos BI components to use another certificate authority.

- Generate IBM Cognos security keys and certificate signing requests to use with your CA.
- Submit the Cognos security keys and certificates to your third-party certificate authority.
Configure IBM Cognos BI components to use a your certificate authority.

Generate Keys and Certificate Signing Requests

Use the command line utility to generate all the keys for the IBM® Cognos® key stores and to generate the certificate signing requests (CSR).

The following tables list the options for the command-line tool used to generate keys and signing requests.

Main Operation Mode

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>Create a new CSR</td>
</tr>
<tr>
<td>-i</td>
<td>Import a certificate</td>
</tr>
</tbody>
</table>

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>

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 (must be provided)</td>
</tr>
<tr>
<td>-a</td>
<td>Key pair algorithm. RSA or DSA.</td>
</tr>
<tr>
<td>Default: RSA</td>
<td></td>
</tr>
<tr>
<td>-D</td>
<td>Directory location</td>
</tr>
</tbody>
</table>

The sample values from the following table are used:
Steps
1. In the `c10_location\configuration` directory, back up the cogstartup.xml file to a secure location.
2. Back up the contents of the following directories to a secure location:
   - `c10_location\configuration\signkeypair`
   - `c10_location\configuration\encryptkeypair`
3. Using IBM Cognos Configuration, export the configuration in clear text by doing the following:
   - Open IBM Cognos Configuration.
   - From the File menu, click Export As.
   - When prompted about exporting decrypted content, click Yes.
   - In the Export As dialog box, select cogstartup.xml and then click Save.
   - When prompted about replacing the existing file, click Yes.
   - When the tasks are complete, close the IBM Cognos Configuration dialog box.
   - Save the configuration.
   - Close IBM Cognos Configuration.
4. Go to the `c10_location\bin` directory.
5. Create the certificate signing request for the signing keys by typing the following command:
   
   **On UNIX® or Linux® operating system, type**
   ```bash
   ThirdPartyCertificateTool.sh -c -s -d "CN=SignCert,O=MyCompany,C=CA" -r signRequest.csr -D ../configuration/signkeypair -p password
   ```
   
   **On Microsoft® Windows® operating system, type**
   ```batch
   ThirdPartyCertificateTool.bat c -s -d "CN=SignCert,O=MyCompany,C=CA" -r signRequest.csr -D ../configuration/signkeypair -p password
   ```

   **Tip:** UNIX or Linux filenames are case-sensitive and must be entered exactly as shown.

   You can safely ignore any warnings about logging.

   The command creates the jSignKeystore file in the signkeypair directory, sets the specified password, creates a new keypair and stores it in the keystore, and exports the signRequest.csr file to the `c10_location\bin` directory.
6. Create the certificate signing request for the encryption keys by typing the following command:
   On UNIX or Linux, type
   
   ```bash
   ThirdPartyCertificateTool.sh -c -e -d "CN=EncryptCert,O=MyCompany,C=CA" -r
   encryptRequest.csr -D ../configuration/encryptkeypair -p password
   ```
   
   On Windows, type
   
   ```bat
   ThirdPartyCertificateTool.bat -c -e -d "CN=EncryptCert,O=MyCompany,C=CA" -r
   encryptRequest.csr -D ../configuration/encryptkeypair -p password
   ```
   
   You can safely ignore any warnings about logging.
   
   The command creates the jEncKeystore file in the encryptkeypair directory, sets the specified password, creates a new keypair and stores it in the keystore, and exports the encryptRequest.csr file to the `c10_location\bin` directory.

7. Copy the signRequest.csr and encryptRequest.csr files that were generated in steps 5 and 6 to a directory that is accessible by your certificate authority.

8. Input the signRequest.csr and encryptRequest.csr files into the certificate authority. The certificate authority produces a signing certificate and an encryption certificate. For more information, see your CA documentation.

9. Copy the contents of the signing certificate into a file named signCertificate.cer.

10. Copy the contents of the encryption certificate into a file named encryptCertificate.cer

11. Find the root CA certificate for the certificate authority and copy the contents into a file named ca.cer.

12. Copy ca.cer, signCertificate.cer, and encryptCertificate.cer to `c10_location/bin`. These files must be PEM (Base-64 encoded ASCII) format.

13. Import the signing certificate from step 10 into the IBM Cognos signing key store by typing the following command:
   
   On UNIX or Linux, type
   
   ```bash
   ThirdPartyCertificateTool.sh -i -s -r signCertificate.cer -D ../configuration/signkeypair -p password -t ca.cer
   ```
   
   On Windows, type
   
   ```bat
   ThirdPartyCertificateTool.bat -i -s -r signCertificate.cer -D ../configuration/signkeypair -p password -t ca.cer
   ```
   
   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.

14. Import the encryption certificate from step 11 into the IBM Cognos encryption key store by typing the following command:
On UNIX or Linux, type

```
ThirdPartyCertificateTool.sh -i -e -r encryptCertificate.cer -D ../configuration/encryptkeypair
-p password -t ca.cer
```

On Windows, type

```
ThirdPartyCertificateTool.bat -i -e -r encryptCertificate.cer -D ../configuration/encryptkeypair
-p password -t cacert.cer
```

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.

15. Import the CA certificate from step 12 into the IBM Cognos trust store by typing the following command:

On UNIX or Linux, type

```
ThirdPartyCertificateTool.sh -i -T -r ca.cer -D ../configuration/signkeypair -p password
```

On Windows, type

```
ThirdPartyCertificateTool.bat -i -T -r ca.cer -D ../configuration/signkeypair -p password
```

The command reads the `ca.cer` file and imports the contents into the `jCAKeystore` file in the `signkeypair` directory using the specified password.

The certificates are now ready to be configured for IBM Cognos BI.

**Configure IBM Cognos BI Components to Run Within Another Certificate Authority**

You must configure each IBM® Cognos® computer to use an external certificate authority by setting the appropriate property in IBM Cognos Configuration.

By setting this property, IBM Cognos BI components assume that all required keys have been generated and vetted by the external certificate authority.

Ensure that the key store locations and password in IBM Cognos Configuration match the ones you typed in the command-line tool.

**Steps**

1. Start IBM Cognos Configuration.

2. In the Explorer window, under Security > Cryptography, click Cognos.

3. In the Properties window, under Certificate Authority settings property group, click the Value box next to the Use third party CA property and then click True.

   **Note:** When you set this property to true, all properties for the certificate authority and identity name are ignored.

4. Configure the following properties to match the ones you typed in the command line utility:
• Signing key store location
• Signing key store password
• Encryption key store location
• Encryption key store password
• Certificate Authority key store password

5. From the File menu, click Save.

6. If you want to start the IBM Cognos service, from the Actions menu, 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.
Setting Up an Unattended Installation and Configuration

Set up an unattended installation and configuration to:

- 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 XWindow

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.

To set up an unattended installation and configuration, perform the following tasks:

- Configure a transfer specification file (.ats) to specify installation options.
- Run the installation tool in silent mode.
- Use a pre configured configuration file from another computer.
- Run the configuration tool in silent mode.

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.

Set Up an Unattended Installation

Use a transfer specification file (.ats) to copy IBM® Cognos® BI components, including Framework Manager or Metric Designer, to your computer without being prompted for information.

By default, 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 that is available on the disk. 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.

Steps Using a File Generated by an Installation on Another Computer

1. Use the installation wizard to install IBM Cognos BI components on one computer.
2. Go to c10_location/instlog.

3. Locate the transfer specification file (.ats) that was generated. The filename format is ts-product_code-version-yyymmd_hhmm.ats

4. Copy the 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, insert the appropriate disk and copy the contents of the disk to your computer.

6. Open the transfer specification file that you copied 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 response.ats file - in the c10_location/license\product directory

8. Save the transfer specification file in the directory where you copied the contents of the installation disk.

9. Install IBM Cognos BI:
   - On Windows®, open a Command Prompt window, and change to the win32 directory where you copied the contents of the disk, and then type the following command, where location is the directory where you copied filename, the transfer specification file:
     issetup -s location/filename.ats
   - On UNIX® or Linux®, change to the directory where you copied the contents of the disk, and in the directory for your operating system, type the following command, where location is where you copied filename, the transfer specification file:
Installation and Configuration Guide 325

Chapter 14: Setting Up an Unattended Installation and Configuration

`.issetup -s location/filename.ats`

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-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 `tl-product_code-version-yyyyymmdd-hhmm.txt`.

Also ensure that the installation directory is protected from unauthorized or inappropriate access.

After all errors are resolved, you can set up an unattended configuration.

**Steps Using the Response.ats File**

1. On the target computer, insert the disk and copy the contents to your computer.
2. Go to the directory for your operating system and open the response.ats file in a text editor. Each section in the response.ats file corresponds to a dialog box in the installation wizard.
3. 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 the root installation directory for the operating system on the product disk.
4. Type the installation location of the program files for IBM Cognos BI in APPDIR=location.
   
   **Tip:** There should be no space on either side of the equal sign, (=).
5. For the server components of IBM Cognos BI, in the section named [Component List], next to each component:
   - To install the component, type 1
   - To not install the component, type 0
   
   **Note:** You do not select components for Framework Manager.

   All required files are installed.
6. For a Windows installation, for the APPFOLDER= property, type the name of the Start menu folder that contains your program shortcuts.
   
   **Tip:** To ensure that the shortcut folder is visible to all users, type 1 for the ALLUSERS_FLAG= property.
7. For the install information in the [Install Conditions] section:
   - To specify the condition is true, type 1
   - To specify the condition is false, type 0
8. Save the response.ats file to a local directory after you make the necessary changes.
9. Go to the directory where you saved the response.ats file.
10. At the command prompt type the following command, where location is the directory where you copied response.ats:

- On Windows,
  
  \texttt{isssetup -s location/response.ats}

- On UNIX or Linux,
  
  \texttt{./isssetup -s location/response.ats}

If a return status other than zero (0) is returned, check the log files for error messages. Errors are recorded in the \texttt{c10_location/instlog} directory in a summary error log file. The filename format is \texttt{tl-product_code-version-yyyymmdd-bhmm_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 \texttt{tl-product_code-version-yyyymmdd-bhmm.txt}.

Also ensure that the installation directory is protected from unauthorized or inappropriate access. After all errors are resolved, you can set up an unattended configuration.

**Set Up an Unattended Configuration**

Before you set up an unattended configuration, you must export a configuration from another computer 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 the source computer. If you made changes to the global configuration, you must also copy the global configuration file from the source computer to the computer where you plan to run an unattended configuration. Global configuration includes such settings as content locale, product locale, currencies, fonts, and cookie settings. For more information, see "Changing Global Settings" (p. 261).

Ensure that the configuration settings on the local computer are appropriate to use to configure another IBM Cognos BI computer with the same installed components. For example, if you changed the host name portion of the Gateway URI property from local host to an IP address or computer name, ensure this setting is appropriate for the new computer’s configuration.

**Steps**

1. In IBM Cognos Configuration, from the \textbf{File} menu, click \textbf{Export as}.

2. When prompted about exporting decrypted content, click \textbf{Yes}.

3. If you want to export the current configuration to a different folder, in the \textbf{Look in} box, locate and open the folder.
   
   Ensure that the folder is protected from unauthorized or inappropriate access.

4. In the \textbf{File name} box, type a name for the configuration file.

5. Click \textbf{Save}.
6. Copy the exported configuration file from the source computer or network location to the \textit{c10\_location/configuration} directory on the computer where you plan to do an unattended configuration.

7. Rename the file to \textit{cogstartup.xml}.

8. If you changed the global configuration on the source computer, copy the \textit{coglocale.xml} file from the source computer to the \textit{c10\_location/configuration} directory on the computer where you plan to do an unattended configuration.

9. Go to \textit{c10\_location/bin}.

10. Type the configuration command:
   - On UNIX\textsuperscript{®} or Linux\textsuperscript{®}, type 
     \texttt{./cogconfig.sh -s}
   - On Windows\textsuperscript{®}, type 
     \texttt{cogconfig.bat -s}

   \textbf{Tip:} To view log messages that were generated during an unattended configuration, see the \textit{cogconfig\_response.csv} file in the \textit{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.

IBM Cognos Configuration applies the configuration settings specified in the local copy of \textit{cogstartup.xml}, encrypts credentials, generates digital certificates, and if applicable, starts IBM Cognos service or process.

### Set Up an Unattended Uninstallation

Set up an unattended installation and configuration to
- automate the removal of components on several computers that have the same components
- remove components on a UNIX\textsuperscript{®} or Linux\textsuperscript{®} environment that does not have XWindows

#### Steps

1. Go to \textit{c10\_location/instlog}.

2. Open the transfer specification .ats file for the product in a text editor.

   The filename format of the transfer specification .ats file is \textit{ts-product\_code-version-yyyy-mm-dd_hhmm.ats}

   where \textit{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\textsuperscript{®} Cognos\textsuperscript{®} BI Server</td>
</tr>
</tbody>
</table>
You only need to edit one .ats file per product.

3. In the section named [Component List], specify the components to remove.
   - To remove the component, type 1
   - To leave the component installed, type 0

   By default, all installed components are set to be removed (1).

4. Save and close the file.

5. Repeat steps 2 to 4 for each installed product.

6. From the operating system command line, change to the c10_location\uninstall directory.

7. At the command prompt, type the following command:
   - On Windows®,
     ```
     uninist -u -s
     ```
   - On UNIX or Linux,
     ```
     ./uninst -u -s
     ```

   All installed components that are set to 1 in the .ats files are removed.
Chapter 15: Performance Maintenance

This section includes topics about using IBM® Cognos® 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 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 troubleshooting chapter of the Administration and Security 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.

You must install Sun Java JDK or the Java Software Development Kit from IBM before you can use the external monitoring feature.

Steps
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 button, 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,
     
     \[\text{service:jmx:rmi:///Content_Manager_server/jndi/rmi://monitoring_server:<JMX-port>/proxyserver}\]
     
     where \text{JMXport} is the value that you typed for External JMX port, and \text{Content_Manager_server} and \text{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.

Notes

- 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>
<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 Dashboard. These comments persist across versions of the report.</td>
</tr>
<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>
<tr>
<td>Content Manager service</td>
<td>• Performs object manipulation functions in the content store, such as add, query, update, delete, move, and copy</td>
</tr>
<tr>
<td></td>
<td>• Performs content store management functions, such as import and export</td>
</tr>
<tr>
<td>Data movement service</td>
<td>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.</td>
</tr>
<tr>
<td>Delivery service</td>
<td>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</td>
</tr>
<tr>
<td>Event management service</td>
<td>Creates, schedules, and manages event objects that represent reports, jobs, agents, content store maintenance, deployment imports and exports, and metrics</td>
</tr>
<tr>
<td>Graphics service</td>
<td>Produces graphics on behalf of the Report service. Graphics can be generated in 4 different formats: Raster, Vector, Microsoft® Excel XML or PDF.</td>
</tr>
<tr>
<td>Human task service</td>
<td>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.</td>
</tr>
<tr>
<td>Service</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Index data service</td>
<td>Provides basic full-text functions for storage and retrieval of terms and indexed summary documents.</td>
</tr>
<tr>
<td>Index search service</td>
<td>Provides search and drill-through functions, including lists of aliases and examples.</td>
</tr>
<tr>
<td>Index update service</td>
<td>Provides write, update, delete, and administration functions.</td>
</tr>
<tr>
<td>Job service</td>
<td>Runs jobs by signaling the monitor service to run job steps in the background. Steps include reports, other jobs, import, exports, and so on.</td>
</tr>
</tbody>
</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.          |
### Purpose

<table>
<thead>
<tr>
<th>Service</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 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. |
| Report service        | Manages interactive requests to run reports and provides output for a user in IBM Cognos Connection or a studio. |

### 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. For more information, see "Configuring IBM Cognos BI for an Application Server other than Tomcat" (p. 291).

The IBM Cognos service is available only on the computers where you installed Content Manager or the Application Tier Components.

### Steps

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.

### Tune Apache Tomcat Settings

If you use Apache Tomcat, you can edit settings to improve performance.

You can edit the maxProcessor and acceptCount settings in the server.xml file.

### Steps

1. Open the server.xml file.
2. Edit the settings that appear after the following comment:

```
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8080 -->
```

Find the following line:

`maxProcessors="75"`

and change it to the following:

`maxProcessors="1000"`

3. Find the following line:

`acceptCount="100"`

and change it to the following:

`acceptCount="500"`

4. Save the updated server.xml file.

**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.

**Steps**

1. In the `c10_location\bin` directory, open the derby.sh file.

2. Find the following line:

`MEM_SETTINGS=-Xmx256m`

and change it to the following:

`MEM_SETTINGS="-Xmx1152m -XX:MaxPermSize=128M -XX:MaxNewSize=576m -XX:NewSize=288m"`

3. In the `c10_location\configuration` directory, rename `derby.properties.sample` to `derby.properties`.

4. In the same directory, open the `derby.properties` file.

5. 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.

**Steps**
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® BI Administration and Security Guide.

To resolve this problem, increase the wait timeout.

**Steps**
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.
Appendix A: Manually Configuring IBM Cognos BI

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.

- Manually change default configuration settings by editing the cogstartup.xml file, located in the c10_location/configuration directory.
- Manually 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 starting the IBM Cognos services in silent mode.
- Deploy IBM Cognos BI into an application server environment by manually creating an IBM Cognos application file.

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 Configuring IBM Cognos BI on UNIX and Linux

The console attached to the UNIX® or Linux® operating system computer on which you are installing IBM® Cognos® BI may not support a Java™-based graphical user interface. You must

- manually change default configuration settings by editing the cogstartup.xml file, located in the c10_location/configuration directory
- manually 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 on UNIX and Linux Computers**

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 to configure IBM® Cognos® BI to work in your environment.

**Note:** 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

**Steps**

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.

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`. 
Add a Component to Your Configuration

The cogstartup.xml file contains configuration settings used by IBM® Cognos® BI 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.

Steps

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:
   ```xml
   <!--
   ==================================================
   (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, don’t 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.

**Manually Change 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.

**Steps**

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`
   
   The new settings are saved and encrypted.
Manually Change the Global Settings on UNIX and Linux Computers

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 located in the c10_location/configuration directory.

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.

**Steps**
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><code>&lt;supportedProductLocales&gt;</code></td>
<td><code>&lt;/supportedProductLocales&gt;</code></td>
</tr>
<tr>
<td>Content Locales</td>
<td><code>&lt;supportedContentLocales&gt;</code></td>
<td><code>&lt;/supportedContentLocales&gt;</code></td>
</tr>
<tr>
<td>Currency</td>
<td><code>&lt;supportedCurrencies&gt;</code></td>
<td><code>&lt;/supportedCurrencies&gt;</code></td>
</tr>
<tr>
<td>Product Locale Mapping</td>
<td><code>&lt;productLocaleMap&gt;</code></td>
<td><code>&lt;/productLocaleMap&gt;</code></td>
</tr>
<tr>
<td>Content Locale Mapping</td>
<td><code>&lt;contentLocaleMap&gt;</code></td>
<td><code>&lt;/contentLocaleMap&gt;</code></td>
</tr>
<tr>
<td>Fonts</td>
<td><code>&lt;supportedFonts&gt;</code></td>
<td><code>&lt;/supportedFonts&gt;</code></td>
</tr>
<tr>
<td>Cookie settings, archive</td>
<td><code>&lt;parameter name=&quot;setting&quot;&gt;</code></td>
<td><code>&lt;/parameter&gt;</code></td>
</tr>
</tbody>
</table>

**Tip:** To remove support, delete the element.

4. Save and close the file.

**Tip:** Use a validating XML editor to validate your changes against the rules in the cogstartup.xsd file, located in the `c10_location/configuration` directory.

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 IBM Cognos BI in Silent Mode on UNIX and Linux Computers**

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.

**Steps to Start IBM Cognos BI**

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 UNIX and Linux Computers" (p. 340).

2. Go to the $c10_location/bin directory.

3. Type the following command

   ```bash
   ./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.

IBM Cognos Configuration applies the configuration settings specified in the cogstartup.xml file, encrypts credentials, generates digital certificates, and if applicable, starts the IBM Cognos service or process.

**Steps to Stop IBM Cognos BI**

1. Go to the $c10_location/bin directory.

2. Type the following command

   ```bash
   ./cogconfig.sh -stop
   ```

**Manually Create an IBM Cognos Application File**

IBM® Cognos® BI and the servlet gateway must be packaged into an application file for deployment to supported application servers (p. 300), (p. 276). IBM Cognos BI 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.

**Steps to Create an IBM Cognos BI Application File**

1. Go to the $c10_location/war/p2pd directory.
2. Run the build script by using the following command syntax:
   - For Microsoft® Windows® operating system,
     `build.bat file_type option`
   - For UNIX® or Linux® operating systems,
     `build.sh file_type option`

   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>
<tr>
<td>ear</td>
<td>EAR file with static content</td>
</tr>
<tr>
<td>ear_without_webcontent</td>
<td>EAR file with no static content</td>
</tr>
<tr>
<td>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_webcontent</td>
<td>directory containing the application with no 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>
<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>
</tbody>
</table>
## Steps to Create a Servlet Gateway Application File

1. Go to the `c10_location/war/gateway` directory.

2. 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>
<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>
</tbody>
</table>
directory containing the application with static content and with no documentation and sample files

and where option can be one or more of the values listed in the following table:

<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>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 ../../ServletGateway.war</td>
<td></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 ../../ServletGateway.ear</td>
<td></td>
</tr>
<tr>
<td>-Dexpand_location=value</td>
<td>path/directory</td>
<td>Path to directory where the application files are to be expanded</td>
</tr>
<tr>
<td></td>
<td>Default is ../../tempexpand</td>
<td></td>
</tr>
</tbody>
</table>
Appendix B: Troubleshooting

Use this troubleshooting reference information and solutions as a resource to help you solve specific problems you may encounter during or after the installation of IBM® Cognos® PowerPlay® 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 Cognos Customer Center (http://www.ibm.com/software/data/support/cognos_crc.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 IBM Cognos 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.

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 learn about logging categories and how to set the level of detail to log for each category.

For more information, see the IBM Cognos BI 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. For more information, see the IBM Cognos Configuration User Guide.

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:
Appendix B: Troubleshooting

tl-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:

tl-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 file, 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 receive 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`, `mod` (Apache 1.3 module), `mod2` (Apache 2.0 module), or `isapi`.

```
gwgateway_interface.log (for example, gwcgi.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.

### The ReportNet to IBM Cognos BI Upgrade File

This file contains a summary of the results of an upgrade from ReportNet® to IBM Cognos BI. The log file is named `upgradeLog.xml` and is located in the `c10_location/logs` directory. The file is in xml format and references an xslt style sheet. You can double-click the file to have it display in your browser.

### 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>
</tbody>
</table>
Ensure that you use other software that is supported by IBM Cognos components. You can view an up-to-date list of environments, such as operating systems, patches, browsers, Web servers, directory servers, and database servers on the IBM Cognos Customer Center (http://www.ibm.com/software/data/cognos/customercenter/).

### CFG-ERR-0106 Error When Starting the IBM Cognos service in IBM Cognos Configuration

When you start the IBM® Cognos® BI service, you may receive the following error message:

```plaintext
CFG-ERR-0106 IBM Cognos Configuration received no response from the IBM Cognos service in the allotted time. Check that IBM Cognos service is available and properly configured.
```

There are two possible causes for this problem:

- **The IBM Cognos service needs more time to start.**
- **A standby Content Manager computer may be configured incorrectly.**

#### The IBM Cognos service Needs More Time

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 displays.

To avoid this error, you can change the amount of time that IBM Cognos Configuration waits to receive a response from the IBM Cognos service. You do this by configuring the ServiceWaitInterval and ServiceMaxTries properties in the `c10_location/configuration/cogconfig.prefs` file.

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.

#### Content Manager Is Configured Incorrectly

If the error message displays on a standby Content Manager computer, the setting for storing the symmetric keys may be incorrect.
To avoid this problem, configure the standby Content Manager computer to store the symmetric keys locally.

**Steps to Change the Wait Time**

1. Using IBM Cognos Configuration, stop the IBM Cognos service.
2. Open the `c10_location/configuration/cogconfigprefs` 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.

**Steps to Store Symmetric Keys Locally**

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.
   - 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.

**Cryptographic Error When Starting IBM Cognos BI**

You received the following error when you tried to start the IBM® Cognos® BI service after installing server or client components:

```
[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.

**Step**

- Copy the bcprov-jdknm-nnn.jar file from the `c10_location/bin/jre/version/lib/ext` directory to the `Java_location/jre/lib/ext` directory.
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® BI 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 URIs 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 URIs with the new port number.

**Steps to Change the Default Port**

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 URIs, 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 URIs 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® BI 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.
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 HPUX and Solaris.

To review an up-to-date list of environments supported by IBM Cognos products, such as operating systems, patches, browsers, Web servers, directory servers, database servers, and application servers, visit the IBM Cognos Customer Center (http://www.ibm.com/software/data/cognos/customercenter/).

**IBM Cognos BI 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.

**IBM Cognos BI Server Not Available When Starting IBM Cognos BI**

After you configure IBM® Cognos® components and start the IBM Cognos services, when you connect to the IBM Cognos BI 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:
Appendix B: Troubleshooting

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>
<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".

Failed Logon:com.jndirect.jsql.x: Cannot open database requested in login 'cm'. Login fails.


- 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.

**Steps for Microsoft SQL Server, Oracle, DB2, and Sybase**

1. On the computer where you installed Content Manager, start IBM Cognos Configuration.

2. In the Explorer window, under Data Access > Content Manager, right-click Content Store and click Delete.

   This deletes the default resource. Content Manager must be configured to 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, type a name for the resource.

   If you are upgrading and want to use an existing content store, ensure that you select the type of database you use for the older version of ReportNet® or IBM Cognos BI.

   If you installed more than one version of IBM Cognos BI, you must use a different content store for each version. When a content store is used by a new version of IBM Cognos BI, it cannot be used by an older version of ReportNet or IBM Cognos BI.

   **Tip:** If you want to use Oracle Net8 keyword-value pair to manage the database connection, select Oracle database (Advanced).

6. In the Properties window, provide values depending on 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 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

   - If you use a DB2 database, for the Database name property, type the database alias.

   - If you use an Oracle database, type the appropriate values for the Database server and port number and Service name 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:
If you use a Sybase database, type the appropriate values for the **Database server and port number** and **Database name** properties.

7. If you want to change the 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 button when it displays.
   - Type the appropriate values and click **OK**.

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

9. Test the connection between Content Manager and the content store.
   **Tip:** In the **Explorer** window, right-click the new database and click **Test**.
   Content Manager connects to the database, checks the database permissions, and creates and populates a table. The table is not deleted and is used each time that the test is repeated.

### Cannot Log On to a Namespace When Using IBM Cognos Connection

You open IBM® Cognos® BI 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. Reason: java.lang.IndexOutOfBoundsException.**

This issue may occur if you do not have the necessary permissions for the following directories:

- `c10\configuration`
- `c10\configuration\csk`
- `c10\configuration\encryptkeypair`
- `c10\configuration\signkeypair`

The solution is to enable the read and execute permissions on the directories listed above 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 then requires a manual restart after the network is restored.

To resolve the problem, configure the **Internal dispatcher URI** property in IBM Cognos Configuration to use localhost or the network host name.
Appendix B: Troubleshooting

No Warning That Installing a Later Version of IBM Cognos BI Will Automatically Update the Earlier Version of the Content Store

You have a version of ReportNet® or 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 ReportNet or IBM Cognos BI no longer works because all content is automatically upgraded.

If you want to use different versions of ReportNet and 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

You start Report Studio in Internet Explorer and the following error message displays:

_The download of the specified resource has failed._

This problem may be caused by recent Microsoft® XMLHTTP upgrades if you do not have a language preference set in Internet Explorer.

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 may 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 BI

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.

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.

**Steps Using the Bootstrap Configuration File**

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.

   ```xml
   <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.

**Steps Using the Startup Configuration File**

1. Go to the `c10_location\bin` directory and open startup.bat in a text editor.

2. Find the following line:

   ```cmd
   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:

   ```cmd
   set CATALINA_OPTS=-Xmx768m -XX:MaxNewSize=384m -XX:NewSize=192m -XX:MaxPermSize=128m
   %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, do the following:

- Start IBM® Cognos® Configuration on the Content Manager computer.
- In the Explorer pane, go to Environment > IBM Cognos services.
- 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® BI, it causes run-time errors. It also causes some product functions, such as report execution, to fail.

To resolve this issue, install IBM Cognos BI in the default directory or use a directory name that contains only ASCII Latin-1 characters.

**Cannot Open an MS Cube or PowerCube**

You are unable to open an MS Cube or PowerCube, or you can open an MS Cube but only metadata is shown. For an MS 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® BI service has access rights to the cube.

PowerCubes are accessed through mapped drives or UNC path names.

**Steps for MS Cubes**

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 user ID 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 Installation and Configuration Guide.

Step for PowerCubes

   • 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 Administration and Security Guide.

The Page Cannot Be Found When Starting IBM Cognos BI in Windows 2003

After installing IBM® Cognos® BI on Microsoft® Windows® operating system 2003, the following message may display when you try to start IBM Cognos BI:

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.

This error is caused by a security feature in Windows 2003 Internet Information Services (IIS). This security feature does not allow unknown cgi file extensions.

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 BI

After you install and configure IBM® Cognos® BI, 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 Installation and Configuration Guide.

DPR-ERR-2058 Error Displays in Web Browser When Starting IBM Cognos BI

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 Content Manager. To help you determine the specific cause, look in the cogserver.log file in the `c10_location/logs` directory. The most common causes are listed below, with 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.

**Steps to Check for an HP-UX Configuration Problem**

1. In the `/bin/startup.sh` file, find
   
   ```bash
   ../tomcat/bin/catalina.sh start "$@"
   ```

2. Change it to the following:
   
   ```bash
   ../tomcat/bin/catalina.sh run "$@"
   ```
The run command causes the Tomcat output to display in the console window for IBM Cognos BI.

3. Stop and restart IBM Cognos BI using the ./shutdown.sh and ./startup.sh commands.
   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.

### Steps to Increase the maximum Number of Threads Per Process

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.

### 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 http://host_name/ibmcognos. 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`

### Steps to Set the Oracle Database Server Name

1. In the Explorer window, click Data Access > Content Manager > Content Store.
2. 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 BI

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.
```

### Opening the Portal Too Soon

This problem can occur if you try to open the portal before IBM Cognos services are initialized.
To avoid this problem, 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.

**The system.xml File Contains Errors**

The system.xml file may have been edited.

Replace the system.xml file in the `c10_location\templates\ps\portal` directory with a copy from backup or use an XML editor to edit it.

**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 *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 BI 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>
<thead>
<tr>
<th>Alias</th>
<th>Path</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibmcognos</td>
<td><code>c10_location\webcontent</code></td>
<td>Read</td>
</tr>
<tr>
<td>ibmcognos\cgi-bin</td>
<td><code>c10_location\cgi-bin</code></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® BI components are installed in a directory with a name that includes spaces.

To resolve this problem, reinstall to a new directory and do not include spaces in the new name. 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 BI Running under WebLogic Application Server on AIX Fails**

The IBM® Cognos® BI 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. Start the IBM Cognos BI Managed Node using the WebLogic startup scripts instead.

**Deploying IBM Cognos BI to an Oracle Application Server or IBM WebSphere Application Server Fails**

Deploying IBM® Cognos® BI to an Oracle application server or an IBM WebSphere® application server may fail with any of the following errors:

- **Browser timeout in administration console**
- **HTTP 500 Internal Error**
- **Deployment failed: Base Exception: java.rmi.RemoteException** (Oracle)
- **Return to application file selection page** (IBM WebSphere)

These errors can occur because the application file that you are trying to deploy is too large.

To solve this problem, do the following:

- 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.

- If you are deploying the application file manually for an Oracle application server, type the following command:

  ```
  dcmctl deployapplication -f path_and_name_of_ear_file -a application_name -co OC4f_instance_name
  ```

  **Installation and Configuration Guide 367**

Appendix B: Troubleshooting
This command is not supported for Oracle Release 3.

For more information about deploying IBM Cognos BI to an application server, see the Installation and Configuration Guide.

Unable to Deserialize Context Attribute Error When Deploying the p2pd.war File to WebLogic

When you deploy the p2pd.war file to WebLogic, you may see the following error:

```
Error [context]Could not deserialize context attribute
java.io.NotSerializableException: com.cognos.logserver.LogService
```

This error does not affect the deployment of the p2pd.war file.

To avoid this problem, add at least one language preference in Internet Explorer.

Error Displays After Upgrading IBM Cognos BI 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>
```

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 this problem, 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.

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.

After you remove all files from the previous installation, you can 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® BI.

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.

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 BI on Linux

If you are using issetup under a UTF-8 locale, accented or double-byte characters may not display correctly.

To resolve this problem when installing in German or French, use a non-UTF-8 locale and then launch issetup 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.

To resolve this problem, increasing the async_wait_timeout_ms parameter parameter in webapps/p2pd/WEB-INF/services/reportservice.xml file. For more information, see the IBM Cognos BI Installation and Configuration Guide.

Also, increase the Queue Time Limit setting to 360. For information, see the IBM Cognos BI Administration and Security Guide.

Problems Configuring IBM Cognos Business Intelligence

After you install IBM® Cognos® BI 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

Configuration Tool cogconfig.sh Return Values Are Not Compliant with Conventional UNIX Return Values

On UNIX® platforms, the configuration tool command cogconfig.sh returns 0 for an unsuccessful execution and 1 for a successful execution. These return values are not compliant with the conven-
itional UNIX return results, where a return value of 0 indicates a successful execution and a non-
zero return value indicates an error.

The non-compliant behavior will be corrected in a future release. You may be required to make
changes to your customer applications and scripts before making use of the new behavior.

Run 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.

Steps

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 $c10_location/configuration/schemas/content.$
   - To delete tables from the notification database, go to $c10_location/configuration/schemas/delivery.$
   - To delete tables from the metric store, go to $c10_location/configuration/schemas/cmm.$
   - To delete tables from the human task and annotation database, go to $c10_location/configuration/schemas/hts.$

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>
<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>
<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>
<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>
</tbody>
</table>
The following table lists the script names for the metric store database.

<table>
<thead>
<tr>
<th>Database Type</th>
<th>Script Name</th>
</tr>
</thead>
<tbody>
<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 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 host 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 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®, 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®, 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:

*java.lang.NoClassDefFoundError: javax/net/ServerSocketFactory.*

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.

**Steps to check the configuration**

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.

**Problems Generating Cryptographic Keys in IBM Cognos Configuration**

When you uninstall IBM® Cognos® BI, some temporary folders are left behind. Reinstalling the product to the same location without first removing the temporary folders may cause problems while attempting to generate the cryptographic keys in IBM Cognos Configuration.

To resolve this problem, uninstall IBM Cognos BI, remove the c10_location/temp/cam folder, and install IBM Cognos BI again.

**CAM-CRP-1315 Error When Saving Configuration**

When you save your configuration, you may receive the following error message:

CAM-CRP-1315 Current configuration points to a different Trust Domain than originally configured.

This 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. This error can occur if the content store you originally used has been 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.

To resolve the problem, change your configuration to use the original content store or regenerate the cryptographic keys.

**Steps to Regenerate Cryptographic Keys**

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® BI 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.

Steps
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

You installed IBM® Cognos® BI using the installation wizard and later renamed the installation directory or manually copied the contents to another directory. When you attempt to run IBM Cognos BI within an application server, you may have one of the following problems:

- 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.

Steps
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 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.

If another instance of IBM Cognos Configuration is running, you should exit that instance. Otherwise, any changes you make to the local configuration may result in errors.

If no other instance of IBM Cognos Configuration is running, delete the cogstartup.lock file in c10_location/configuration.

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 replace the default database type for the content store with Oracle, DB2®, or Sybase. You cannot replace the Cognos namespace. You can recreate it, but you must then recreate your Cognos groups and roles.

For more information about creating groups and roles in IBM® Cognos® Connection, see the Administration and Security Guide.

Steps to Recreate the Cognos Namespace

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.
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 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.

Current Configuration Settings Are Not Applied to Your Computer

You change default property values or add a resource to your installation in IBM® Cognos® Configuration. After saving the current 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.

Steps to Restart the IBM Cognos service

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.

The solution is to 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 have installed IBM® Cognos® BI and after you run the C8DB2.sh script, see , an error stating that DB2® cannot be found is displayed or written to the log files:

You can solve this problem by using the following steps:

1. Create a profile that sources the sqllib/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/sqllib/db2profile ]; then
     . /home/db2user/sqllib/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.

**Steps**

1. In the **Explorer** pane, click **Security > IBM Cognos Application Firewall**.
2. In the right pane, click in the **Value** column next to **Valid domains or hosts**.
3. Click the edit button.
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 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.

1. The maximum Java memory setting is Medium (1152MB) or higher.
2. You are importing a large archive from a previous release of IBM Cognos BI.
3. The archive contains large models that require upgrading.

To resolve this issue, set the maximum Java memory setting to Small (768MB).

**Users are Prompted for Active Directory Credentials**

The single signon mechanism does not work when IBM® Cognos® BI 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

When you start IBM® Cognos® Configuration, the following error message may display:

Font specified in font.properties not found...

This is a common problem on UNIX®. It means that 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.

To avoid these errors, 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 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.

Steps

1. In the c10_location/configuration directory, open the file named qfs_config.xml.

2. Find the line of code <provider name="DB20lapODP" libraryName="essodp93" connectionCode="DO"/> 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.
- XQE-DS-0006 Unable to logon to the data source.

These IBM Cognos errors can result from Windows not having enough Windows sockets or ports available. 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 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.

**Steps**

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.

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 BI, 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
Appendix B: Troubleshooting

If the privilege is missing, there is no group membership for the authenticated user. To solve this problem, perform the following steps.

**Steps**

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 Deploying to Oracle 10G Application Server**

You are deploying IBM® Cognos® BI to an Oracle 10G Application Server, and get the following error messages:

- 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)*

This occurs because the bulk loading utilities (SQL Loader on Oracle) are not included in the deployment file created by IBM Cognos Configuration.

To resolve this error, you must use the Oracle client software on the computer where you installed the Oracle 10G Application Server to install the missing components. Ensure that you install SQL Loader.
CGI Timeout Error While Connected to IBM Cognos BI Components 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. 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.

**Steps to Change the Gateway to ISAPI**

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`

**Steps to Increase the CGI Timeout**

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:

```java
<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 servleticgss 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.

<Jul 9, 2004 3:47:37 PM EDT> <Error> <HTTP> <BEA-101216> <Servlet: "cfgss" failed to preload on startup in Web application: "p2pd".>
```
javax.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.langClassNotFoundException: 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.

Steps
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 xvf "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.

To resolve this issue, 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.

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 button
- click the Permissions tab
- ensure that the users who will run migration tasks have Read, Write, Execute, and Traverse permissions.
Appendix B: Troubleshooting
Appendix C: 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 in 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>
<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>
<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>
<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>
Glossary

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.

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.

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.

certification authority
In BI, a component that issues certificates to each computer on which components are installed.

cipher suite
The combination of authentication, key exchange algorithm, and the Secure Sockets Layer (SSL) cipher specification used for the secure exchange of data.

Common Gateway Interface
An Internet standard for defining scripts that pass information from a web server to an application program, through an HTTP request, and vice versa.

content locale
A code that is used to set the language or dialect used for browsers and report text, and the regional preferences, such as formats for time, date, money, money expressions, and time of day.
Glossary

**Content Manager**
The service that retrieves information from the content store, and saves information to the content store.

**content store**
The database that contains the data needed to operate, such as report specifications, published models, and security rights.

**credential**
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

**data source**
The source of data itself, such as a database or XML file, and the connection information necessary for accessing the data.

In TM1®, the file or data used as the source for the TurboIntegrator import process.

**deployment archive**
A file used for deployment. A deployment archive contains the data from the content store that is being moved.

**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.

**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.
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.

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.

metric store
A database that contains content for metric packages. A metric store also contains Metric Studio settings, such as user preferences.

namespace
For authentication and access control, a configured instance of an authentication provider that allows access to user and group information. In Framework Manager, namespaces uniquely identify query items, query subjects, and so on. You import different databases into separate namespaces to avoid duplicate names.

In XML and XQuery, a uniform resource identifier (URI) that provides a unique name to associate with the element, attribute, and type definitions in an XML schema or with the names of elements, attributes, types, functions, and errors in XQuery expressions.

passport
Session-based information, stored and encrypted in Content Manager memory, regarding authenticated users. A passport is created the first time a user accesses a Cognos product, 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.

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.

prompt
A report element that asks for parameter values before the report is run.

report specification
An executable definition of a report, including query and layout rules, which can be combined with data to produce a report output.
response file
An ASCII file that can be customized with the setup and configuration data that automates an installation. The setup and configuration data would have to be entered during an interactive install, but with a response file, the installation can proceed without any intervention.

user
Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.
Symbols
.
.ats file
    using to remove components, 327
32-bit installation
    requirement for 32-bit library files, 42
64-bit application server
    problem connecting to IBM Cognos BI portal, 374
64-bit installation
    requirement for 64-bit library files, 42
64-bit installations, 29
A
accented characters
    not displayed properly, 369
acceptCount
    increasing for Apache Tomcat, 334
access
    configuring secure access to the portal, 99, 139
active Content Manager, 117
Active Directory Server
    advanced properties, 186
    authenticating in multiple domains, 186
    enabling single signon, 187
    enabling SSL, 186
    missing group membership, 381
    using for authentication, 183
    with an LDAP namespace, 197
active scripting
    enabling in Web browsers, 49
additional fonts
    installing, 178
agent service, 331
AIX
    error connecting to DB2 database, 360
    support for RACF namespace, 215
aliases
    configuring on Apache Web Server, 271
    configuring on Web servers, 101, 160, 308
    definition, 389
annotation service, 331
anonymous access
    definition, 389
    disabling, 99, 139
anonymous logon
    disabling, 182
Apache gateways
    configuring, 271
Apache Tomcat
    tuning, 334
Apache Web servers
    configuring aliases, 101, 160, 308
    configuring as gateways, 271
application pool
    creating on Windows Server 2008, 102, 162, 309
application pools, 101, 160, 308
application servers
    changing from the default, 291
    configuring, 302
    problems running IBM Cognos BI, 375
    servlet class fails to load in WebLogic, 383
    servlet gateways, 276
    startup script fails, 367
    startup scripts, 300
    startup scripts for Oracle application server, 304
    upgrading IBM Cognos BI, 312
Application servers
    startup scripts for Sun Java System application server, 307
application tier components
    configuration requirements, 28
    configuring, 141
    definition, 389
    installing on separate computer, 27
Application Tier Components
    log server, 249
Architect models
    migration to IBM Cognos BI, 31
archiving
    report output, 239
ASCII
    requirements for installation directory, 362
Index

Asynchronous timeout, 336
audience of document, 13
audit
  logs, 249
audit logs
  log destinations, 249
  See Also log messages
  See Also troubleshooting
authentication
  Active Directory Server, 183
  configuring IBM Cognos Series 7 namespace, 189
  custom authentication providers, 193, 194
  custom properties for Active Directory Server, 185
  custom user properties for LDAP, 206
  definition, 389
  deleting namespaces, 217
  disabling anonymous logon, 182
  domain trees for Active Directory Server, 186
  eTrust Siteminder, 210, 211, 213
  LDAP, 195, 196
  LDAP using Active Directory Server, 197
  LDAP using IBM Directory Server, 200
  LDAP using Novell Directory Server, 202
  LDAP using Sun Java System Directory Server, 204
  NTLM, 213
requirements for single signon with Microsoft
  Analysis Server or Microsoft SQL Server, 184
  SaferAPIGetTrustedSignon function, 191
  single signon for NTLM, 214
  single signon using Active Directory Server, 187
  single signon using eTrust SiteMinder, 212
  single signon using IBM Cognos Series 7 namespace, 190
  single signon using LDAP, 209
  single signon using RACF, 216
  SSL for eTrust Siteminder, 212
  SSL using LDAP, 207
  trusted signon plug-ins for IBM Cognos Series 7, 191
  using namespaces, 181
authentication provider
  configuring IBM Cognos BI to use security, 94, 138
authentication providers
  definition, 389
B
backing up
  IBM Cognos BI information, 294, 313
backslashes appear instead of currency, 179
basic installations
  multiple locations, 115
batch report service, 331
Batch report service
  list of embedded fonts for PDF reports, 237
BEA WebLogic, 291
BI bus
  upgrade considerations, 68
Bind user DN and password property
  special characters for LDAP namespace, 195
bookmark conversion utility, 23
builds
  running in IBM Cognos Connection by using Data
    Movement service, 34
C
C8DB2.sh script
  error, 378
CA, See certification authority
CAM-CRP-1157 error, 354
certificate authority
  configuring, 316
certificates
  definition, 389
certificate signing requests
  generating, 317
certification authority
  configuring the service, 316
definition, 389
CGI gateway
  limitations with multiple Content Manager computers, 116
CGI timeout errors, 383
changing
  configuration template, 334
default configuration settings, 220
e-mail encoding, 267
IBM Cognos BI gateway, 270
Java versions, 313
URIs, 223
characters
  encoding not supported, 355
characters improperly displayed, 369
chase_referral files, 186
Chinese
  characters display incorrectly after upgrade, 368
corrupt characters during installation on Linux, 366
chunking patches
  application servers, 293
cipher suites
  definition, 389
  setting a priority for SSL connections, 247
client component, 24
client setup
  DB2 databases, 91, 129
CM-SYS-5001 A Content Manager internal error occurred, 379
CM-SYS-5007 error, 361
cogconfig.sh return codes
  not UNIX compliant, 369
Cognos Content Database
  changing users and passwords, 221
  component description, 22
  improving performance, 335
  installing on a separate server, 122
  uninstalling, 109, 168
Cognos namespace
  recreating, 376
Cognos Viewer
  component description, 22
cogroot.link file, 375
cogstartup.lock file, 350
cogstartup.xml file, 340, 344
  changing properties manually, 342
  invalid file, 377
collation sequence, 42
collation sequences
  case-sensitive, 355
common gateway interface
  replacing, 270
common gateway interface (CGI)
  definition, 389
common symmetric key, 225
components, 21
  application tier components, 27, 28
  bookmark conversion utility, 23
Cognos Content Database, 22
Cognos Viewer, 22
Content Manager, 22, 28, 80
data sources, 24
gateways, 21, 26, 80
IBM Cognos Administration, 22
IBM Cognos BI samples, 23
IBM Cognos Configuration, 21
IBM Cognos Connection, 21
installation requirements for 64-bit systems, 29
installing, 80
installing on one computer, 26
Migration Assistant, 23
Migration Service, 23
Open with Analysis Studio, 23
Open with Report Studio, 23
PowerPlay Studio, 22
third-party, 21
Confidentiality algorithm, 227
configuration
  adding resources, 340
  advanced options, 313
  automating, 323
  backing up, 294, 313
  changing defaults settings, 220
  changing the template, 334
  Content Manager, 28
  cryptographic information cannot be encrypted, 373
  data locked, 376
  default settings, 220
  error when encrypting information, 373
  global settings, 261
  issues, 369
  lock file, 350
  manual, 339
requirements for single signon with Microsoft
  Analysis Server or Microsoft SQL Server, 184
  running from command line, 344
  running multiple versions of IBM Cognos BI, 75
  settings for IBM Cognos BI, 40, 220
  settings not applied, 377
  testing, 104
  Tomcat settings, 40
  unable to open IBM Cognos Configuration, 350
  unable to save, 376
  unattended, 323, 326
  upgrade considerations, 69
Index

configuration files  
  applications.xml for Portal Services, 283  
  coglocale.xml, 343  
  cogstartup.xml, 340  
  exporting, 326  
configuring  
  Active Directory namespace, 184  
  application server properties, 302  
  application tier components, 141  
  certificate authority service, 316  
  Content Manager computers, 116  
  custom authentication providers, 194  
  default time zone, 267  
  destination for log messages, 249  
  distributed installations, 113  
  environment properties for application tier components, 149  
  eTrust SiteMinder namespace, 211  
  fonts, 233  
  gateways, 159  
  IBM Cognos BI, 49  
  IBM Cognos service, 334  
  LDAP namespace, 196  
  LDAP namespace for Active Directory Server, 197  
  LDAP namespace for IBM Directory Server, 200  
  mail server, 137  
  mail server accounts, 98  
  notification databases, 242  
  NTLM namespace, 214  
  Portal Services, 283  
  properties in an unattended configuration, 342  
  RACF namespace, 215  
  required tasks, 113  
  routers, 279  
  shared trust with other servers, 246  
  SSL protocol, 243  
  standby Content Manager, 135  
  temporary file location, 231  
  transfer specification files (.ats), 323  
  unattended, 326  
  Web browsers, 49  
  Web server, 101, 160, 308  
console mode  
  for installing on UNIX and Linux, 20  
content expiry  
  images directory, 101, 160, 308  
content locale  
  definition, 389  
content locales  
  customizing, 263  
  displaying supported locales, 263  
  mapping to user locale, 264  
Content Manager  
  active and standby, 117  
  attempt to register the dispatcher, 360  
  changing time zones, 267  
  component, 28  
  component description, 22  
  configuration, 28  
  configuring, 116  
  configuring on multiple computers, 135  
  default active, 116  
  definition, 389  
  error messages, 378  
  failover protection, 28  
  fails to start, 361  
  installation options, 28  
  installing, 80  
  log server, 249  
  requirements for changing application server, 293  
  requirements if using IBM Cognos Transformer with Series 7 namespace, 80, 188  
  setting up a content store, 41, 242  
  standby, 28  
  upgrade considerations, 68  
Content Manager service, 331  
Content Manager URIs, 135, 149  
content store  
  and other locations to store report output, 238  
  backing up, 294, 313  
  compatible versions of DB2 and Java, 354  
  component description, 24  
  connection management, 95, 131  
  creating, 41, 79, 242  
  creating on DB2 using a script, 87, 125  
  creating on Oracle, 45  
  DB2 JDBC drivers, 17, 90  
  deleting tables from the database, 370  
  deploying, 60  
  importing data, 311, 316  
  invalid settings, 355  
  new default in version 8.4, 19
requirements for changing application server, 293
support for DB2 on z/OS for version 8.4, 18
upgrading, 68, 360
content stores
definition, 390
context attribute cannot be deserialized, 368
context error, 368
conversion
of bookmarks from IBM Cognos Series 7 to IBM Cognos PowerPlay, 23
of ppr reports to ppx reports, 23
cookies
customizing, 269
enabling in Web browsers, 49
settings, 269
creating
content store, 79
credentials
definition, 390
cross-script checking
configuring in IBM Cognos Application Firewall, 230
cryptographic error, 377
cogstartup.xml file invalid, 377
JRE error, 377
problems after upgrading, 374
cryptographic information cannot be encrypted, 373
cryptographic keys
backing up and deleting, 294, 313
generating for other certificate authorities, 317
regenerating, 374
cubes
cannot open, 362

cubes, See PowerCubes
currency
customizing support, 263
fonts required for Yen or Won character, 178
won, 179
yen, 179
custom authentication providers, 193
custom user properties
Active Directory Server, 185
LDAP, 206

D
dashboard application, 16
data
importing, 64
locked by IBM Cognos Configuration, 376
sharing data locations in a network, 281
database cleanup scripts, 370
database client
setting up for a logging database, 252
database connections
Informix, 95
database connections, See data source connections
database connection strings
IBM DB2, 95, 131
Microsoft SQL Server, 95, 131
Oracle, 95, 131
Sybase, 95
database connectivity
content connectivity
content store, 91
database drivers
DB2, 91, 129
Informix, 92, 130, 254
Oracle, 92, 130
Sybase, 92, 130
databases
bulk load utility missing, 382
content store, 41, 242
creating a content store on DB2 using a script, 87, 125
deleting tables, 370
logging, 255
logging, testing, 104
logging database client, 252
notification, 137
Data files location
configuring for Windows Vista, 279
data integration service, 331
Data Manager
using in IBM Cognos BI, 34
Data Movement service
using in IBM Cognos Connection, 34
data source connections
setting, 131
data sources
component description, 24
definition, 390
DB2
client setup, 91, 129
Index

database drivers, 91, 129
JDBC drivers, 17, 90
specifying as a log messages repository, 255
supported Java versions, 354
DB2 content store, 333
  error when running C8DB2.sh script, 378
DB2-ERR-0005, 381
db2java.zip
  deprecated in version 8.4, 19
default connection pool time-out
  conflicts between IBM Cognos BI and some application servers, 297
delivery
  decreasing the time to open reports, 336
delivery service, 331
deploying
  configuration objects, 63
  content store, 60
directory content, 60
exporting, 61
failure on Oracle or WebSphere Application Server, 367
importing, 64
moving archives, 63
packages, 60
partial deployment, 60
Public Folders, 60
testing, 65
deploying IBM Cognos BI, 302
deployment
  permissions, 59
  planning, 59
deployment archives
  definition, 390
  moving, 63
Deployment files location
  configuring for Windows Vista, 279
deployments
  creating an export specification, 61
Derby
  page cache size, 335
description of product, 13
diagnostics, See troubleshooting
differences
  between IBM Cognos Series 7 PowerPlay and IBM Cognos PowerPlay, 13
directories
  deploying content, 60
directory not found error, 363
 disabling
  anonymous access, 99, 139
dispatcher
  unregistering, 311
dispatchers
  Application Tier Components computer, 383
  importing, 63
  system metrics, 329
distributed installations
  configuring, 113
  creating profiles for WebSphere Application Server
    for Linux on System z, 293
  scenarios, 25
documentation
  Software Development Kit, 15
  translated files, 19
domains
  Active Directory Server domain trees, 186
  setting for cookies, 269
double-byte characters
  improperly displayed, 369
download of resource fails, 360
DPR-CMI-4006 error, 361
DPR-DPR-1035 error, 354
DuseCMLargeResultSet parameter, 361

E
EAR files, See Enterprise archive files
email
  configuring mail server accounts, 98
  email messages
    changing the encoding, 267
  embedded fonts, 237
  enabling
    IBM Cognos Application Firewall, 230
    services, 232
    SSL for an application server, 307
encryption
  changing settings in unattended configuration, 342
  configuration errors, 373
Encrypt temporary files property, 231
Enterprise archive files
  deploying IBM Cognos BI, 345
environment properties, 94
environments
  supported, 37
environment variables
  configuring for application tier components, 149
  content store, 41
  requirements on Windows Vista, 279
  setting for application servers, 296
  to install on UNIX or Linux, 81, 118, 142, 152
error messages
  CAM-CRP-1064, 359
  CAM-CRP-1315 Current configuration points to a
different trust domain, 374
  CFG-ERR-0106 Cognos Configuration received no
response, 352
  CGI timeout, 383
  CM-CFG-029 Content Manager is unable to deter-
mine, 378
  CMM-APP-3254 The initialization of the metrics
store failed, 382
  corrupt cryptographic information, 377
  could not deserialize context attribute, 368
  cryptographic information cannot be encrypted, 373
  DIS-ERR-3115 Task execution failed, 382
  download of specified resource fails, 360
  DPR-ERR-2014, 362
  DPR-ERR-2022 No response generated, 365
  DPR-ERR-2058, 360, 363
  DPR-ERR-2079, 378
  HTTP Error 404, 363
  Java Runtime Environment, 377
  malformed request, 368
  MDS-RUN-3213 Unable to locate database bulk
load utility, 382
  page not found, 363
  PRS-CSE-1255, 359
  RQP-DEF-0114, 369
  RSV-SRV-0066, 369
  servlet class fails to load on WebLogic, 383
  SocketException, 360
  SQL1224N, 360
  Unable to load balance the request, 362
  you have chosen to download a file, 366
errors
  ESSBASEPATH, 380

ESSBASEPATH
  adding, 380
eTrust SiteMinder
  configuring namespaces, 211
cross-script checking in IBM Cognos Application
  Firewall, 230
  enabling single signon, 212
  protecting the IBM Cognos BI Web alias, 213
  SSL, 212
  using for authentication, 210
event logs, 255
event management service, 331
exporting
  configuration files, 326
  creating a specification, 61
external identity mapping property
  editing for an LDAP namespace, 209
External identity mapping property
  special characters for LDAP namespace, 195

F
failover protection, 28
  ISAPI gateway required for multiple Content Man-
ger installation, 116
file locations
  requirements on Windows Vista, 279
files
  not found, 363
file system
  to save copies of report output, 238
Firefox
  browser settings, 49
fix pack
  installing, 84, 122, 145, 155
flicker, 384
folders
  deploying public, 60
font embedding lists, 237
fonts
  changing for PDF reports, 236
  changing the default, 236
  configuring, 233
  list of embedded fonts for PDF reports, 237
  not found when starting IBM Cognos Configuration
  on UNIX, 380
  requirements for support, 235
Index

Framework Manager
  cryptographic error, 353
  uninstalling, 109, 167
  upgrade considerations, 68

G
  gateway
    connection issues, 374
  gateways
    adding in a network to decrease delivery times, 336
    component description, 21
    configuration requirements, 27
    configuring, 159
    configuring for IBM Cognos BI, 270
    configuring to use a namespace, 232
    definition, 390
    installing, 80
    installing on separate computer, 26
    log file, 351
    recommended settings for Microsoft IIS, 383
    when to use ISAPI, 383
  glyphs
    definition, 390
  graphics service, 331
  Great Outdoors samples, 23, 171
    installing, 172
  groups
    definition, 390
    missing membership in Active Directory Server, 381

H
  histories
    deployment, 65
  HTML cookies, See cookies
  HTTP Error 404, 363
  human task service, 331

I
  IBM Cognos Administration
    component description, 22
  IBM Cognos Application Firewall
    configuring, 230
  IBM Cognos BI
    changing application servers, 291
    components, 21
    configuring, 49
    default settings, 79
    deploying, 302
    dispatchers, 333
    does not start on an application server, 375
    installation options, 25
    installing migration tool on Windows, 106, 164
    logging in, 94, 138
    maintenance package installation, 84, 122, 145, 155
    running on same computer as ReportNet, 75
    service does not start, 354
    services, 333
    system requirements, 38
    uninstalling, 108, 166
    updater, 84, 122, 145, 155
  IBM Cognos BI portal
    problem connecting on 64-bit WebSphere Application Server, 374
  IBM Cognos BI samples, 23
  IBM Cognos BI server
    fails to start, 355
  IBM Cognos BI service
    requirements for the user account that is used for the service, 130, 148, 158
  IBM Cognos Configuration
    component description, 21
    font not found error on UNIX, 380
    invalid settings, 355
    problems opening, 350
    problems saving a configuration, 369
    problems with keyboard navigation, 376
    starting, 93
    trouble generating cryptographic keys after install, 374
    unable to start, 376
    unattended mode, 326
  IBM Cognos Connection
    component description, 21
    unable to open, 363
  IBM Cognos Controller
    data access in IBM Cognos BI, 33
  IBM Cognos Finance
    data access in IBM Cognos BI, 33
  IBM Cognos Go! Dashboard
    renamed as IBM Cognos Business Insight, 16
  IBM Cognos Go! Mobile
    mobile reports, 34
IBM Cognos Metrics Manager
- upgrading saved reports from version 2.x to IBM Cognos BI, 68
- upgrading to IBM Cognos BI, 67
IBM Cognos NoticeCast
- duplication of functionality in IBM Cognos BI, 35
IBM Cognos Planning - Analyst
- data access in IBM Cognos BI, 32
IBM Cognos Planning - Contributor
- data access in IBM Cognos BI, 33
IBM Cognos Portal Services
- migration overview, 35
IBM Cognos PowerPlay
- installing, 80
- troubleshooting installations, 349
IBM Cognos Query
- duplication of functionality in IBM Cognos BI, 34
IBM CognosScript
- migration overview, 35
IBM Cognos Series 7
- enabling single signon, 190
- enabling SSL, 190
- migration to IBM Cognos BI, 30
- trusted signon plug-ins, 191
- using for authentication, 188
IBM Cognos Series 7 PowerCubes
- requirements for successful language conversion, 33
IBM Cognos service
- configuring, 334
- requirements for the user account that is used for the service, 220
- server not available, 355
- starting, 93, 377
- starting from IBM Cognos Configuration, 103
- starting from the command line, 344
- stopping from the command line, 344
IBM Cognos Visualizer
- duplication of functionality in IBM Cognos BI, 35
IBM Cognos Web Services
- migration overview, 35
IBM DB2
- creating connection strings, 95, 131
IBM Directory Server
- with an LDAP namespace, 200
IBM Java Software Development Kit, 260
IBM WebSphere, 291
IBM WebSphere Application Server
- single signon with RACF, 216
IBM WebSphere Portal
- configuring, 283
IIS Web servers
- single signon using Active Directory, 187
images
- content expiry, 101, 160, 308
- loading in Report Studio, 101, 160, 308
importing
- configurations, 63
- data into target environment, 64
Impromptu catalogs and reports
- migration to IBM Cognos BI, 31
Impromptu Web Reports
- migration to IBM Cognos BI, 31
index data service, 332
index search service, 332
index update service, 332
Informix
- creating a logging database, 47
- creating the content store, 47
- database connections, 95
- database drivers, 92, 130, 254
- specifying as a log messages repository, 255
installation
- basic for multiple locations, 115
- checklist, 79
- options for Content Manager, 28
- requirements for directory name, 362
- testing, 104
- unattended, 323
installation directory
- problems after renaming or moving, 375
- requirements, 113
installing
- additional fonts, 178
- Cognos Content Database separately, 122
- Great Outdoors samples, 172
- IBM Cognos BI, 79, 323
- IBM Cognos BI on Linux, 369
- IBM Cognos PowerPlay, 80
- sequence for server components, 115
Supplementary Language Documentation, 177
- testing, 141, 151, 163
- unattended install, 323
Index

using transfer specification file (.ats), 323
using transfer specification files (.ats), 323
Integrated Windows Authentication
issues, 379
interface
customizing language support, 262
Internet Explorer
browser settings, 49
requirements to support Simplified Chinese, 236
invalid cogstartup.xml file, 377
invalid settings
content store, 355
IBM Cognos Configuration, 355
IP address version, 277
IPv4, 277
IPv6, 277
ISAPI
accessing IBM Cognos BI, 270
when to use for a gateway, 383
ISAPI gateway
recommended with multiple Content Managers, 270
required with multiple Content Manager computers, 116

J
Japanese characters
corrupt during installation on Linux, 366
display incorrectly after upgrade, 368
Japanese currency, 179
Japanese Yen
font requirements, 178
jar file, 91
error when starting configuration, 377
Java
changing versions, 313
configuring servlet gateway for Java-compatible Web servers, 276
supported versions for DB2 content store, 354
updating runtime environments, 92, 128, 315
uses all of CPU, 354
JAVA_HOME
setting, 377
java.lang.NoClassDefFoundError, 353
Java Archive files, See jar file
Java error when starting configuration, 377
Java Management Extensions
configuring JMX properties for remote monitoring of system metrics, 329
with user logs, 260
Java Runtime Environment
IBM JRE replaces Sun Java Runtime Environment, 19
Java scripts
enabling in Web browsers, 49
Java Software Development Kit from IBM, 329
Java virtual machine
crashes when importing deployment, 379
JDBC
database connectivity for content store, 91
JDBC drivers, 17, 90
db2java.zip deprecated in version 8.4, 19
setting up Oracle databases, 252
jobs
definition, 390
job service, 332
job steps
definition, 390
JobStreams
running in IBM Cognos Connection by using Data Movement service, 34
JREs
updating, 92, 128, 315
JVM
changing, 294, 313
copying security provider files, 315
memory settings for Cognos Content Database, 335

K
keyboard
navigation problems, 376
keyboard shortcuts, 387
Korean characters
corrupt during installation on Linux, 366
display incorrectly after upgrade, 368
Korean currency, 179
Korean Won
font requirements, 178

L
language
customizing for user interface, 262
customizing locale content support, 263

languages
conversion tables, 368
incompatibility after upgrade, 368
new support in version 8.4, 17
user interface and message files, 20

language support, 19

latency
improving, 336

LDAP
Active Directory Server, 197
configuring a namespace, 196
custom properties, 206
editing the External identity mapping property, 209
enabling single signon, 209
enabling SSL, 207
IBM Directory Server, 200
Novell Directory Server, 202
Sun Java System Directory Server, 204
using for authentication, 195

library files
for 32-bit versus 64-bit installation, 42

Linux
characters not displayed properly, 369
console-mode installation is deprecated, 20
corrupt characters during installation, 366
environment variables, 81, 118, 142, 152
log messages, 255
on System z, creating addition WebSphere profiles
to run IBM Cognos BI components, 293
starting and stopping the IBM Cognos service, 344
system requirements, 79
unsupported features and components, 37

Linux on System z
C8DB2.sh script error, 378

Linux on System Z
support for RACF namespace, 215
load balancing, 49
configuring mail server settings, 137
enabling and disabling services, 232
setting, 27

locales
definition, 390
displaying supported content locales, 263
displaying supported product locales, 262

localhost
requirement to change to host name or IP address, 94

log database
deleting tables, 370

destinations
types of, 249
log files, 349
gateway errors, 351
locale configuration, 350
run-time, 350
silent mode, 351
startup configuration, 350
transfer, 349
transfer summary, 350
uninstallation, 351

logging
configuring, 255
database, 255
database client, 252
remote log servers, 254
using files, 255

logging database
creating on z/OS, 250
creating using DB2, 42
creating using Informix Dynamic Server database, 47
creating using Microsoft SQL Server, 46
creating using Oracle, 45
creating using Sybase, 48
support for DB2 on z/OS for version 8.4, 18

testing, 104

logging in
configuring security, 94, 138
hiding namespaces during, 194, 213

log messages
enabling for IBM Cognos Application Firewall, 230
log destinations, 249
remote log server, 249
See Also audit logs
See Also troubleshooting

logs
message processing, 249
service, 332
Index

**M**

macro
classifying ppr reports to ppx reports, 23

mail server
classifying, 137

mail server accounts
classifying, 98

maintenance
improving system performance, 329

Map files location
classifying for Windows Vista, 279

maxProcessor
increasing for Apache Tomcat, 334

Metadata service, 332

metric packages
definition, 391

metrics
for servers, dispatchers, and services, 329

Metrics Manager service, 332

metric store
improving performance, 335

metric stores
definition, 391
failure, 382

Microsoft
security update affects memory, 355

Microsoft Analysis Server
namespace requirement, 184

Microsoft Analysis Services
single signon to MSAS data sources, 187

Microsoft IIS Web servers
recommended gateway settings, 383

Microsoft Office
report data service, 333

Microsoft Registry Editor
increasing sockets or ports, 381

Microsoft SQL Server
creating connection strings, 95, 131
namespace requirement, 184
specifying as a log messages repository, 255

migration
authentication requirements, 99
failure to run, 384
from other IBM Cognos products to IBM Cognos BI, 30

Migration Assistant
classifying component description, 23
does not work, 384

migration components, 23

Migration service, 332

Migration Service
classifying component description, 23

mobile devices
using to access reports, 34

monitor service, 333

moving
deployment archives, 63

Moving from trial upgrade to production environment, 66

MS Cube, 362

multi_domain_tree, 186

**N**
namespaces
RACF, 215

namespaces
Active Directory Server missing group membership, 381
authentication, 181
cannot log on, 359
configuring custom authentication providers, 194
classifying for a gateway, 232
definition, 391
deleting, 217
hiding during login, 194, 213
IBM Cognos Series 7, 99
recreating, 376
requirements for Content Manager if using Transformer with Series 7 namespace, 80, 188

Netegrity SiteMinder, See eTrust SiteMinder

network access
sharing data locations, 281

network outage
services fail to start, 359

no response generated, 365

notification database
configuring, 242
classifying, 240
deleting tables, 370
settings for DB2 on z/OS, 240

support for DB2 on z/OS for version 8.4, 18
tablespaces for DB2 on z/OS, 241
Novell Directory Server
with an LDAP namespace, 202
NTLM, 213
  configuring, 214
  enabling single signon, 214
NTLM, See Also Windows native security (NTLM)

O
OLAP data sources, 362
  members missing or inaccessible, 381
Open with Analysis Studio
  component description, 23
Open with Report Studio
  component description, 23
operating systems
  affect on upgrade, 69
Oracle
  application server, 304
  creating connections strings, 131
  creating connection strings, 95
  database drivers, 92, 130
  database JDBC drivers, 252
  deployment errors, 382
  specifying as a log messages repository, 255
Oracle application server, 291
Oracle Application Server
  IBM Cognos BI deployment failure, 367
Oracle Essbase
  query fails, 381
Oracle WebCenter Interaction Portal
  configuring, 283
other products
  upgrading, 75
OutOfMemoryError, 361

P
p2pd.war file for WebLogic, 368
packages
  deploying, 60
page cache size
  Derby, 335
page not found error
  starting IBM Cognos BI in Windows 2003, 363
passwords
  changing for Cognos Content Database, 221
  changing in unattended configuration, 342
paths
  setting for cookies, 269
PDF fonts
  mapping to built-in PDF fonts for faster report printing, 235
performance
  improving for Apache Tomcat, 334
permissions
  deployment, 59
  for the user account that is used for the IBM Cognos BI service, 130, 148, 158
  for the user account that is used for the IBM Cognos service, 220
planning an upgrade, 54
portal
  configuring secure access for users, 99, 139
  errors in starting, 363, 365
portal problems
  unable to open, 363
Portal Services, 283
  availability on Linux, 37
  specifying the applications.xml file, 283
portlet
definition, 391
ports
  changing, 223
  default configuration settings, 40
  running multiple versions of IBM Cognos BI, 75
ports already in use, 354
PowerCubes
  access in IBM Cognos BI, 33
  cannot open, 362
  requirements for successful language conversion, 33
  setting up the sample for PowerPlay, 173
PowerPlay Administration, 384
PowerPlay Client component, 24
PowerPlay Server, 384
PowerPlay Studio
  component description, 22
  presentation service, 333
Presentation service
  requirements, 330
processing log messages, 249
Index

product
  name changes, 19
product codes
  in transfer specification files, 327
product locale
  definition, 391
product locales
  displaying supported locales, 262
  mapping for user interface, 266
product versions, 84, 122, 145, 155
profiles
  creating for WebSphere Application Server for Linux on System z, 293
prompts
  definition, 391
properties
  changing in unattended configuration, 342
  configuring for application server, 302
  temporary file location, 231
protocol
  IP address, 277
Public Folders
  deploying, 60
purpose of document, 13

Q
quality of protection in SSL connections, 247
query databases, 24
query service, 333
quick tours, 13

R
RACF
  authentication settings for IBM Cognos BI administrators, 215
  connectivity, 215
  enabling single signon, 216
RACF account properties
  mapping to RACF namespace, 215
RACF namespace, 215
recreating the Cognos namespace, 376
relational data sources
  members missing or inaccessible, 381
release notes
  reviewing before you install, 37
remote log servers, 254
  configuring, 255
removing components from multiple servers, 327
report conversion
  from ppr to ppx format, 23
report data service, 333
report distribution
  on a network, 336
ReportNet
  running on same computer as IBM Cognos BI, 75
to IBM Cognos BI upgrade file, 351
upgrading, 67
upgrading to IBM Cognos BI, 67
report output
  reusing, 239
  saving to a file system, 238
  sharing with users outside IBM Cognos BI, 238
reports
  changing default font, 236
  customizing language support, 263
decreasing delivery time, 336
testing before an upgrade, 58
Report service
  list of embedded fonts for PDF reports, 237
requirements, 330
report services, 333
report specifications
  definition, 391
Report Studio
  loading images, 101, 160, 308
required tasks
  configuring, 113
requirements
  installation directory, 362
Resource Access Control Facility
  See also RACF, 215
resources
  adding, 340
response.ats file, 323
response files
  definition, 391
return values
  cogconfig.sh not UNIX compliant, 369
reviewing the release notes before you install, 37
root directory
  for saving report output outside IBM Cognos BI, 238
routers
configuring, 279

S
SaferAPIGetTrustedSignon function
using for authentication, 191
sample PowerCube
setting up, 173
samples, 23
  Great Outdoors, 171
  installing, 172
SAP Enterprise Portal
configuring, 283
screen flicker, 384

scripts
creating a content store on DB2, 87, 125
to delete tables from databases, 370
to improve metric store performance, 335

secure flag
setting for cookies, 269
secure LDAP communication, 207
Secure Sockets Layer, See SSL protocol
security
configuring secure access to the portal, 99, 139
enabling, 94, 138
issues with Integrated Windows Authentication, 379
settings for Web browsers, 38

security provider files
copying to application server JVM, 315

Series 7 PowerCubes
requirements for successful language conversion, 33
Series 7 PowerPlay
upgrading saved reports from ReportNet to IBM Cognos BI, 68

server components, 21
  installation sequence, 115

servers
system metrics, 329
server time zones
changing, 267

service
  graphics, 331
  human task, 331
  index data, 332
  index search, 332
  index update, 332

service pack
installing, 84, 122, 145, 155

services
adjusting to improve performance, 330
agent, 331
annotation, 331
batch report, 331
Content Manager, 331
data integration, 331
delivery, 331
enabling and disabling, 232
event management, 331
fail to start after network outage, 359
IBM Cognos BI, 333
job, 332
log, 332
Metadata, 332
Metrics Manager, 332
Migration, 332
migration service not working, 384
monitor, 333
presentation, 330, 333
query, 333
report, 333
Report, 330
report data, 333
setting the user account for shared network access, 281
starting, 93
starting from the command line, 344
stopping from the command line, 344
system metrics, 329
unable to start, 354
uninstalling, 108, 166

servlet gateway
configuring, 276

shared trust
setting up between IBM Cognos BI and other servers, 246
SharePoint Portal
configuring, 283

shortcut keys, 387
silent installations, See unattended installation
silent mode, See unattended mode
silent uninstallation, 327
Index

Simplified Chinese
requirements if using Internet Explorer 6, 236

single signon
Active Directory namespace, 187
eTrust SiteMinder user directory, 212
issues with Integrated Windows Authentication, 379
LDAP namespace, 209
NTLM namespace, 214
RACF namespace, 216
using IBM Cognos Series 7 namespace, 190

Software Development Kit
documentation, 15

Solaris
JRE 1.5, 379

special characters
in LDAP namespace properties, 195

SQL scripts
to delete databases, 370

SSL
Active Directory Server, 186
enabling for an application server, 307
enabling on Web servers, 248
eTrust SiteMinder user directory, 212
LDAP namespace, 207
quality of protection, 247
setting up shared trust with other servers, 246
using IBM Cognos Series 7 namespace, 190

SSL protocol
configuring, 243

standby Content Manager, 28, 117
configuring, 135

starting
IBM Cognos Configuration, 93
the IBM Cognos service from IBM Cognos Configuration, 103

starting the IBM Cognos service
from the command line, 344

startup
configuration lock file, 350
DB2 returns SQL1224N error when connecting from AIX, 360
download of resource fails, 360
failure without error, 355
IBM Cognos service, 377
page not found, 363
problems, 351
script fails, 367
unable to download cognos.xts, 366
unable to open IBM Cognos Connection, 363
unable to start service, 354
startup scripts, See Also application servers
stopping the IBM Cognos service
from the command line, 344

Sun Java JDK, 260, 329

Sun Java System
application server, 307
Sun Java System Directory Server
with an LDAP namespace, 204

Supplementary Language Documentation
installing, 177

Supplementary Languages Documentation
new in version 8.4, 19

supported environments, 37

Sybase
creating connection strings, 95
creating the content store, 48
database drivers, 92, 130
specifying as a log messages repository, 255

syslog
destination for log messages, 255

system metrics
access from outside IBM Cognos Administration, 16
remote monitoring, 329

system requirements, 38

System z
creating addition WebSphere profiles to run IBM Cognos BI components, 293

Tab key
problems in IBM Cognos Configuration, 376

tables
deleting from a database, 370
tablespaces, 333
DB2 Notification Database on z/OS, 241

template
changing the size of template, 334
temporary directories
deleting before reinstall, 374
temporary file location, 231
  configuring, 231
Temporary files location
  configuring for Windows Vista, 279
testing
  configuration, 104
  deployment, 65
  installation, 104
testing the installation, 141, 151, 163
Thai email encoding
  JRE requirements, 267
third-party components, 24
time zones
  changing, 267
Tomcat
  default configuration settings, 40
  tuning, 334
transfer specification file
  using to remove components, 327
transfer specification files (.ats)
  configuration, 323
Transformer
  data access in IBM Cognos BI, 33
  requirements for Content Manager if using Series 7
    namespace, 80, 188
  uninstalling, 109, 167
trial upgrade, 58
  planning the move to the production environment, 66
troubleshooting, 349
  Content Manager fails to start, 361
    for a specific user, 260
    logging, 249
trust domain error
  when saving the configuration, 374
tuning
  Apache Tomcat settings, 334
  DB2 content store, 333

U
unable to open IBM Cognos Configuration, 350
unattended configuration
  changing properties, 342
  setting up, 323
unattended installation
  setting up, 323
unattended mode, 323
unattended uninstallation, 327
uninstalling
  Cognos Content Database, 109, 168
  Framework Manager, 109, 167
  IBM Cognos BI, 108, 109, 166, 167
  Transformer, 109, 167
uninst command, 327
UNIX
  console-mode installation is deprecated, 20
  environment variables, 81, 118, 142, 152
  font not found error, 380
  log messages, 255
  starting and stopping the IBM Cognos service, 344
  system requirements, 79
UNIX AIX
  support for RACF namespace, 215
unregistering dispatchers, 311
unsupported characters, 355
updater
  installing, 84, 122, 145, 155
updating
  java environment, 92, 128, 315
upgrading
  affect on Chinese, Japanese, or Korean characters, 368
  content store, 360
  create test environment, 58
  from Metrics Manager, 53
  from other IBM Cognos products to IBM Cognos BI, 30
  from ReportNet, 53
  from Series 7, 53
  IBM Cognos BI, 69
  IBM Cognos BI on an application server, 312
  other products, 75
  planning the move from test to production environment, 66
  preparation, 54
  problems with cryptographic keys, 374
  process, 54
  ReportNet, 67
  resources, 55
URI
  changing, 223
  default configuration settings, 40
Index

URI properties
  requirement to change localhost to host name or IP address, 94

User account
  requirements to run the IBM Cognos BI service, 130, 148, 158
  requirements to run the IBM Cognos service, 220

user credentials
  changing in unattended configuration, 342

user interface
  customizing language support, 262
  mapping for product locale, 266

user locale
  mapping to content locale, 264

user logs
  configuring secure access to the portal, 99, 139
  logs, 260

User lookup property
  special characters for LDAP namespace, 195

users
  changing for Cognos Content Database, 221
  definition, 392

UTF-8
  encoding for email messages, 267

versions
  supported ReportNet upgrades, 67

virtual directories
  IBM Cognos BI, 101, 160, 308

virtual servers
  configuring for IBM Cognos BI, 101, 160, 308

Web
  WAR files, See Web archive files
  Web aliases
    IBM Cognos BI, 101, 160, 308
  Web archive files
    deploying IBM Cognos BI, 345
  Web browsers
    configuring, 49
    errors in starting the Web portal, 365
    errors when starting the web portal, 363
    security settings, 38
  WebLogic
    application server, 303, 306
could not deserialize context attribute, 368
  deploying p2pd.war file, 368
  servlet class fails to load, 383
  startup script, 300
  startup script fails, 367
  WebLogic Application Server
    IBM Cognos BI fails, 367
  Web servers
    configuring, 101, 160, 308
    enabling SSL, 248
    servlet gateways, 276
    setting Report Studio load time, 101, 160, 308
    single signon using Active Directory and IIS Web server, 187
  WebSphere
    application server, 302
  WebSphere Application Server
    additional profiles for Linux on System z, 293
    IBM Cognos BI deployment failure, 367
    problem connecting to IBM Cognos BI portal, 374
    startup script fails, 367
  Windows
    installing IBM Cognos migration tool, 106, 164
    system requirements, 79
  Windows event log
    destination for log messages, 255
  Windows IIS
    recommended gateway settings, 383
  Windows integrated authentication, 187
  Windows native security (NTLM)
    enabling single signon, 214
    using for authentication, 213
  Windows Server 2008
    creating an application pool, 102, 162, 309
  Windows Vista
    affect on upgrade, 69
    requirements for file locations, 279
  won character, 179
  Won character
    font requirements, 178

X
  XQE-DS-0006, 381

Y
  yen character, 179
Yen character
  font requirements, 178