

IBM Cognos Analytics  
Version 12.0.x

*Installation and Configuration*



©

## Product Information

This document applies to IBM Cognos Analytics version 12.0.0 and may also apply to subsequent releases.

## Copyright

Licensed Materials - Property of IBM

© Copyright IBM Corp. 2015, 2024.

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

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

The following terms are trademarks or registered trademarks of other companies:

- Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

© **Copyright International Business Machines Corporation .**

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

---

# Contents

<b>Chapter 1. Preparing to install.....</b>	<b>1</b>
Review supported environments.....	1
Example: Checking the requirements for installing Red Hat Enterprise Linux (RHEL) 8.1.....	1
Verify system requirements.....	3
Memory settings.....	5
Configuring CSP headers.....	7
Java requirements.....	8
Review the default port settings.....	9
Guidelines for creating the content store.....	10
Suggested settings for creating the content store in IBM Db2 on Linux, Windows, and UNIX operating systems.....	11
Suggested settings for creating the content store in IBM Db2 on z/OS .....	13
Suggested settings for creating the content store in Oracle.....	13
Suggested settings for creating the content store in Microsoft SQL Server.....	14
Suggested settings for creating the content store in IBM Informix database server.....	15
Configure a User Account or Network Service Account for IBM Cognos Analytics.....	15
Configure web browsers.....	16
<b>Chapter 2. Easy Install.....</b>	<b>19</b>
<b>Chapter 3. Single server installation.....</b>	<b>21</b>
<b>Chapter 4. Distributed server installation.....</b>	<b>27</b>
Gateway Tier Installation.....	30
Application Tier Installation.....	31
Content Tier Installation.....	33
<b>Chapter 5. Silent installation, uninstallation, and configuration.....</b>	<b>37</b>
Use a silent installation.....	37
Use a response file template.....	39
Use a silent configuration.....	42
Use a silent uninstallation.....	43
<b>Chapter 6. Installing IBM Cognos Analytics for Jupyter Notebook Server.....</b>	<b>45</b>
Hardware requirements for Jupyter Notebook Server.....	45
Installing Jupyter Notebook Server on Linux.....	46
Uninstalling Jupyter Notebook Server.....	48
Installing Jupyter Notebook Server on Microsoft Windows 10.....	48
Uninstalling Jupyter Notebook Server.....	50
Installing a pip package in an offline Linux environment.....	50
Installing a pip package in an offline Windows environment.....	51
Configuring Jupyter Notebook Server.....	52
Configuring the Cognos Analytics gateway for Jupyter Notebook Server.....	55
Notebook performance logs.....	55
Securing Jupyter Notebook Server.....	56
Upgrading IBM Cognos Analytics for Jupyter Notebook Server.....	57
Upgrading your installation for Linux.....	57
Upgrading your installation for Microsoft Windows.....	58
Upgrading Python packages and R packages.....	59
Adding additional Ubuntu operating system packages.....	60

Troubleshooting IBM Cognos Analytics for Jupyter Notebook Server.....	60
<b>Chapter 7. Distribution options.....</b>	<b>61</b>
Cognos Analytics components.....	61
Server components.....	61
Modeling components.....	63
Required database components.....	64
Distributing components.....	64
Application Tier Components and Content Managers on separate computers.....	65
Consolidate servers for Linux on System z.....	66
Installation for optional modeling components.....	66
Firewall considerations.....	67
Distributing Framework Manager components.....	68
Distributing Transformer components.....	68
IBM Cognos Analytics with other IBM Cognos products.....	70
IBM Cognos products that interoperate with IBM Cognos Analytics.....	70
<b>Chapter 8. Upgrading Cognos Analytics.....</b>	<b>73</b>
Data upgrade tasks for Cognos Analytics.....	73
Running the ParquetMigrate utility .....	74
Converting multiple queries and analyses to reports.....	76
Changed modification time property on objects after an upgrade .....	77
Preserved files and folders when upgrading Cognos Analytics.....	77
Standard upgrade process.....	80
Reviewing the documentation.....	81
Assess applications in your environment before you upgrade.....	81
Install and configure a new version of the product.....	82
Move your content to the new version of the product.....	85
Upgrade your content store.....	85
Moving your content with a deployment archive.....	86
Upgrade your report specifications.....	89
<b>Chapter 9. Configuring server components.....</b>	<b>91</b>
Installation sequence for server components.....	92
Recommendation - Install and Configure the Basic Installation for Distributed Installations.....	93
Installation modes.....	94
Installing server components on UNIX or Linux operating systems.....	94
Installing server components on Windows operating systems.....	95
Installing and configuring Content Manager for the content repository.....	96
Active and Standby Content Manager Components.....	97
Installing Content Manager on UNIX or Linux operating systems.....	97
Installing Content Manager on Windows operating systems.....	98
Set up database connectivity for the content store database.....	99
Start IBM Cognos Configuration.....	106
Set Database Connection Properties for the Content Store.....	106
Configure Environment Properties for Content Manager Computers.....	111
Specify a connection to an email server.....	112
Enable Security.....	113
Start Content Manager.....	114
Test the Content Manager installation.....	114
Installing and configuring the Application services.....	114
Install the Application services components.....	115
Set up database connectivity for reporting databases.....	116
Start IBM Cognos Configuration.....	118
Configure Environment Properties for Application services components computers.....	119
Enabling the 64-bit version of report server.....	120
Start the Application services components.....	120

Test the Application services components.....	121
<b>Chapter 10. Configuring the gateway.....</b>	<b>123</b>
Installing the Cognos Analytics gateway.....	123
Configure Cognos Analytics with your web server.....	124
Enabling the 32-bit web gateway.....	125
Configuring dispatcher URIs.....	126
Configure Apache HTTP Server or IBM HTTP Server .....	127
Configuring IBM HTTP Server V9 .....	127
Configuring WebDAV on IBM HTTP Server or Apache HTTP Server.....	131
Configuring IBM HTTP Server with SSL.....	132
Configuring Apache HTTP Server or IBM HTTP Server with Cognos Analytics.....	134
Configuring Cognos Analytics with either Apache HTTP Server or IBM HTTP Server.....	136
Apache web server load balancing.....	137
Enabling HTTP/2 for a web server .....	137
Configure Microsoft Internet Information Services .....	138
Configuring WebDAV on IIS.....	138
Configuring IIS with SSL.....	139
Configuring IIS in Cognos Analytics.....	139
Configuring the CGI gateway on IIS version 7 or later.....	145
Configuring the gateway and web server to use specific namespaces.....	147
Configuring a gateway namespace.....	147
Configuring a namespace to use with IIS.....	148
Configuring a namespace to use with Apache or IBM HTTP server .....	148
Testing the gateway.....	149
<b>Chapter 11. Installing and configuring optional modeling components .....</b>	<b>151</b>
IBM Cognos Framework Manager.....	151
System requirements for IBM Cognos Framework Manager.....	151
Installing IBM Cognos Framework Manager.....	152
Configuring IBM Cognos Framework Manager.....	152
Setting variables for data source connections for Framework Manager.....	156
Testing the Framework Manager installation.....	158
IBM Cognos Transformer.....	158
System requirements for Cognos Transformer .....	158
Installing IBM Cognos Transformer.....	159
Configuring Transformer authentication using WebView2.....	160
Setting up data sources for Transformer.....	161
Configuring communication between Transformer and Cognos Analytics.....	162
Testing the Transformer installation.....	163
Additional configuration tasks for Cognos Transformer.....	164
<b>Chapter 12. Configuration options.....</b>	<b>167</b>
Start IBM Cognos Configuration.....	167
Critical configuration actions to take first!.....	167
Changing the version of Java used by IBM Cognos Analytics components.....	168
Changing default configuration settings.....	169
Port and URI settings.....	169
Verifying configuration settings.....	171
Managing the Configuration Group.....	172
Configuring cryptographic settings.....	175
IBM Cognos Application Firewall.....	179
Encrypt temporary file properties.....	180
Enable and Disable Services.....	181
Configuring fonts.....	181
Configure Embedded Fonts for PDF Reports.....	184
Changing the location of temporary report output.....	184

Changing the location of data files.....	185
Tuning WebSphere Liberty Profile.....	186
Enabling session replication for standby Content Manager services .....	186
Use an external object store for report output and datasets.....	187
Verify access to the external object store.....	188
Configuring query settings.....	188
Changing the cache size of dynamic queries.....	188
Reverting to missing values in list reports.....	190
Ensuring that root members in a Planning Analytics data source match those in the TM1 client..	190
Disabling filler members in a Planning Analytics package.....	191
Configuring the Dataset service port number exchange timeout .....	192
Saved Report Output.....	193
Save Report Output Outside IBM Cognos Analytics.....	193
Save Report Output Inside IBM Cognos Analytics.....	194
Customizing Server-side Printing for UNIX and Linux Platforms.....	194
Change the notification database.....	195
Suggested settings for creating a notification database on IBM Db2 on z/OS .....	195
Creating tablespaces for a notification database on IBM Db2 for z/OS .....	196
Change the Connection Properties for the Notification Database.....	197
External certificate management in Cognos Analytics.....	197
ThirdPartyCertificateTool commands and usage examples.....	198
Configuring Cognos Analytics to use another certificate authority (CA) certificate.....	200
Configuring Cognos Analytics to use an existing certificate authority (CA) certificate .....	203
Configuring the SSL protocol for IBM Cognos components.....	206
Configuring SSL for Cognos Analytics components.....	206
Set up shared trust between IBM Cognos servers and other servers.....	209
Select and rank cipher suites for Secure Socket Layer.....	210
Using the SSL protocol for database communications.....	210
Enabling SSL for communications with Microsoft SQL Server databases.....	211
Enabling SSL for communications with Db2 and Informix databases.....	212
Enabling SSL for communications with Oracle databases.....	213
Configure JDBC data source connections for single sign-on using Kerberos.....	214
Editing the bootstrap_wlp_*.xml file for Oracle connections with Kerberos SSO.....	215
Creating Kerberos initialization files.....	216
Creating an SPN for the query service.....	217
Creating a keytab file.....	217
Configuring the Kerberos login module.....	217
Verifying the Kerebos configuration.....	218
Verifying the JDBC driver capabilities.....	218
Configuring data source connections when using Kerberos.....	219
Configuring a repository for log messages.....	219
Guidelines for creating a logging database.....	220
Database connectivity for the logging database.....	221
Log message repositories.....	223
Changing Global Settings.....	228
Customize Language Support to the User Interface.....	228
Customizing Currency Support.....	229
Customize content locale support.....	229
Content Locales.....	230
Map Product Locales.....	231
Customize the Server Time Zone.....	232
Encoding for Email Messages.....	232
Customizing cookie settings.....	234
Change the IP Address Version.....	234
Setting the IP version.....	235
Manually configuring IBM Cognos Configuration to start with the IPv6 option.....	235
Configuring IBM Cognos Configuration to always start with the IPv6 option on Windows .....	236
Configuring the Collaboration Discovery URI.....	236

Configure the Router to Test Dispatcher Availability.....	236
Configuring IBM Cognos Analytics to Work with Other IBM Cognos Products.....	237
Enable Scheduled Reports and Agents for IBM Cognos Planning Contributor Data Sources.....	237
Configuring the Software Development Kit.....	237
<b>Chapter 13. Configuring authentication providers .....</b>	<b>239</b>
Disabling anonymous access.....	240
Restricting user access to the Cognos namespace.....	240
Configuring Lightweight Third-Party Authentication.....	241
Configuring LTPA using an LDAP namespace.....	242
Configuring LTPA using an Active Directory namespace.....	243
OpenID Connect authentication provider.....	244
Configuring an OpenID Connect namespace .....	246
Generic OIDC provider type.....	247
Configuring IBM Cognos Components to Use Active Directory Server.....	251
Configuring an Active Directory Namespace.....	252
Make Custom User Properties for Active Directory Available to IBM Cognos Components.....	253
Enabling Secure Communication to the Active Directory Server .....	253
Include or Exclude Domains Using Advanced Properties.....	254
Enable single signon between Active Directory Server and IBM Cognos components.....	254
Configuring IBM Cognos to Use IBM Cognos Series 7 Namespace.....	257
Configuring an IBM Cognos Series 7 Namespace.....	258
Enabling Secure Communication to the Directory Server Used by the IBM Cognos Series 7 Namespace.....	259
Enabling Single Signon Between IBM Cognos Series 7 and IBM Cognos .....	259
IBM Cognos Series 7 Namespaces and the IBM Cognos Series 7 Trusted Signon Plug-in.....	259
Configuring IBM Cognos to Use a Custom Java Authentication Provider.....	261
Configure a Custom Authentication Namespace.....	262
Hide the Namespace from Users During Login.....	262
Configuring IBM Cognos components to use LDAP.....	263
LDAP mapping.....	263
Configuring an LDAP namespace.....	264
Configuring an LDAP namespace for Active Directory Server.....	265
Configuring an LDAP namespace for IBM Directory Server.....	266
Configuring an LDAP namespace for Novell Directory Server.....	266
Configuring an LDAP namespace for Oracle Directory Server.....	268
Making custom user properties for LDAP available to IBM Cognos components.....	269
Enabling secure communication to the LDAP server .....	270
Enable single signon between LDAP and IBM Cognos components.....	272
Replace operation.....	272
SiteMinder authentication provider.....	273
Configuring a SiteMinder namespace.....	274
Configure IBM Cognos to use SAP.....	275
Configure an SAP Namespace.....	277
Enable Single Signon Between SAP and IBM Cognos .....	278
Delete an Authentication Provider.....	278
<b>Chapter 14. Performance Maintenance.....</b>	<b>279</b>
System Performance Metrics.....	279
Monitoring System Metrics Externally.....	279
Enabling Only Services That are Required.....	280
Tuning a IBM Db2 Content Store.....	283
Adjusting the memory resources for the IBM Cognos service.....	283
Reduce Delivery Time for Reports in a Network.....	284
Increase Asynchronous Timeout in High User Load Environments.....	284

<b>Chapter 15. Manually configuring Cognos Analytics on UNIX and Linux operating systems.....</b>	<b>285</b>
Manually change default configuration settings.....	285
Adding a component to your configuration.....	286
Changing manually encrypted settings.....	287
Global settings on UNIX and Linux operating systems.....	287
Changing manually the global settings on UNIX and Linux operating systems.....	288
Starting and stopping Cognos Analytics in silent mode on UNIX and Linux operating systems.....	289
Starting Cognos Analytics in silent mode on UNIX and Linux operating systems.....	289
Stopping Cognos Analytics in silent mode on UNIX and Linux operating systems.....	290
<b>Chapter 16. Uninstalling IBM Cognos Analytics.....</b>	<b>291</b>
Uninstall IBM Cognos Analytics on UNIX or Linux operating systems.....	291
Uninstall Cognos Analytics on Microsoft Windows operating systems.....	292
Recovering from an unsuccessful uninstall.....	292
<b>Chapter 17. IBM Cognos content archival.....</b>	<b>295</b>
Configure content archival.....	296
Creating a file location for a file system repository.....	296
Importing custom classes definitions and properties into IBM Content Manager 8.....	297
Specifying an available time to run the archival process.....	298
Specifying thread execution time.....	299
Archiving selected formats of report outputs.....	299
Specifying that report specifications are not archived.....	300
<b>Appendix A. IBM Cognos Configuration command-line options.....</b>	<b>301</b>
<b>Appendix B. About this guide.....</b>	<b>303</b>
<b>Index.....</b>	<b>305</b>



---

# Chapter 1. Preparing to install

Before you install IBM® Cognos® Analytics, you must set up resources in your environment so that the components can operate. For example, you must create a database to use as a Cognos Analytics content store, and create a user account for Cognos Analytics.

If you use the **Easy Install** option to install Cognos Analytics (on Windows only), you do not need to create and configure a content store database. An Informix database is already configured as your content store, and Cognos Analytics can use it right away.

After you complete these tasks, continue with [Chapter 9, “Configuring server components,”](#) on page 91.

---

## Review supported environments

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

To review an up-to-date list of environments that are supported by IBM Cognos Analytics products, including information on operating systems, patches, browsers, web servers, directory servers, database servers, and application servers, see [IBM Cognos Analytics on Premises 12.0.x Supported Software Environments](https://www.ibm.com/support/pages/node/6966712) (<https://www.ibm.com/support/pages/node/6966712>).

## Example: Checking the requirements for installing Red Hat Enterprise Linux (RHEL) 8.1

In this example, you use the Supported Software Environments page to run Software Product Compatibility Reports (SPCR) reports that identify component requirements.

### Before you begin

Review the tasks outlined in [Chapter 1, “Preparing to install,”](#) on page 1.

### About this task

You want to install Red Hat Enterprise Linux (RHEL) 8.1 as the operating system on which you will later install Cognos Analytics 11.2.3. You have a Windows x86 computer with a 64-bit processor. Before you can install RHEL 8.1 successfully, you must identify and install any prerequisite software.

**Note:** If you don't complete this task, you may be unable to start Cognos Configuration and an [error message](#) will appear.

### Procedure

1. Read the topic [“Review supported environments”](#) on page 1.
2. Click the link [IBM Software Product Compatibility Reports page](#).
3. Scroll to the **Cognos Analytics on Premises 11.2.3** section, and in the **Requirements by platform** column, click **Linux**.

## Cognos Analytics on Premises 11.2.3

Requirements by type	Requirements by platform	Supplementary information
<ul style="list-style-type: none"> <li>Operating Systems</li> <li>Software (including application servers, data sources, and web browsers)</li> <li>Hardware</li> <li>Hypervisors</li> </ul>	<ul style="list-style-type: none"> <li>AIX</li> <li><b>Linux</b></li> <li>Mobile OS</li> <li>Windows</li> </ul>	<ul style="list-style-type: none"> <li>Supported and tested client drivers 11.2.3 <a href="#">[Relational]</a>   <a href="#">[OLAP]</a></li> </ul>

The Software Product Compatibility Reports (SPCR) report appears.

4. Find the x86-64 row, and in the **Details** column, click **View**.

Continuous Delivery Product

### Cognos Analytics 11.2.3.0

Detailed System Requirements

Report filters

Available Reports: 11.2.3.0

Utilities: Regenerate Anytime, Download PDF, Print

Notes: Data as of 2022-11-24 01:39:14 EST, Disclaimers

Operating Systems | Hypervisors | Prerequisites | Supported Software | Hardware | Packaging List

Show notes | Hide notes

Linux

Operating System	Operating System Minimum	Hardware	Bitness	Components	Notes	Details
Red Hat Enterprise Linux (RHEL) 8	8.1	IBM z Systems	64-Exploit		(1)	View
Red Hat Enterprise Linux (RHEL) 8	Base	POWER System - Little Endian	64-Exploit		No	View
Red Hat Enterprise Linux (RHEL) 9	Base	POWER System - Little Endian	64-Exploit		No	View
Red Hat Enterprise Linux (RHEL) 8	8.1	x86-64	64-Exploit		(8)	View
Red Hat Enterprise Linux (RHEL) Server 7	7.1	IBM z Systems	64-Exploit		(3) (13) (15)	View

5. Find the **Cognos Analytics Server** row, and in the **Update 8.1** column, note the reference to **Notes (8)**.



Product: Cognos Analytics 11.2.3.0 on Linux



Support for operating system:  
Red Hat Enterprise Linux RHEL 8 x86-64

**Operating System Updates** Components

Product support for updates, current and future →

Deployment Unit	Component	Bitness	Base	Update 8.1	Update 8.2	Update 8.3	Update 8.4	Update 8.5	Update 8.6	→
Server	Cognos Analytics Server	64-Exploit	✗	✓ (8)	✓ (8)	✓ (8)	✓ (8)	✓ (8)	✓ (8)	✓
	Cognos Software Development Kit	64-Exploit	✗	✓ (8)	✓ (8)	✓ (8)	✓ (8)	✓ (8)	✓ (8)	✓
	Mashup Services	64-Exploit	✗	✓ (8)	✓ (8)	✓ (8)	✓ (8)	✓ (8)	✓ (8)	✓

**Notes:** (8)  
The Transformer UI is available on Windows platforms only.  
Additional packages  
yum install libXtst  
yum install libX11.so.6  
yum install libnsl  
yum install nspr.i686 nspr.x86\_64

6. In **Notes (8)**, you see that you must install additional packages by entering the following commands:

- `yum install libXtst`
- `yum install libX11.so.6`
- `yum install libnsl`
- `yum install nspr.i686 nspr.x86_64`
- `yum install nss.i686 nss.x86_64`
- `yum install motif.i686 motif.x86_64`
- `yum install libnsl.so.1`
- `yum install libstdc++.so.6`

7. Install the additional packages listed above.

## Results

You can now continue completing the tasks outlined in [Chapter 1, “Preparing to install,”](#) on page 1.

## Verify system requirements

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

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

## Hardware requirements

Table 1. Hardware requirements for a single computer installation	
Requirement	Specification
Operating system	Microsoft Windows UNIX Linux®
Processing	Minimum: 4 CPU cores for one user. For each deployment, a sizing exercise is highly recommended.
RAM	Minimum 32 GB. For more information, see <a href="#">“Memory settings” on page 5</a> .
Operating system specifications	File descriptor limit set to 8192 on UNIX and Linux
Disk space	<p>A minimum of 7 GB of free space is required to install the software and 5 GB of free space on the drive that contains the temporary directory used by IBM Cognos components.</p> <p>An environment variable points to the temporary directory. On Windows this variable is TMP. On UNIX and Linux, this variable is IATEMPDIR</p> <p>For all databases, the size will increase over time. Ensure that you have sufficient disk space for future requirements.</p>
Printer	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.
Email server	To email reports, the system requires the ability to use and access an email server.

## Software requirements

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

Table 2. Software requirements for a single computer installation	
Requirement	Specification
Java™ Runtime Environment (JRE)	An IBM JRE is provided as part of the install with IBM Cognos Analytics on all operating systems.

Table 2. Software requirements for a single computer installation (continued)

Requirement	Specification
Database	<p>You must have one of the following databases available to store IBM Cognos data:</p> <ul style="list-style-type: none"><li>• Oracle</li><li>• IBM Db2®</li><li>• Microsoft SQL Server</li><li>• Informix®</li></ul> <p>The Easy (previously Ready to Run!) option installs and configures an Informix database as the content store.</p> <p>TCP/IP connectivity is required for all database types.</p>
Web browser	<p>For all web browsers, the following must be enabled:</p> <ul style="list-style-type: none"><li>• cookies</li><li>• JavaScript</li></ul>

## Requirements for map visualizations

The maps that you create in dashboards and reports use a cloud-based tile map and polygon service. You must have internet access from your workstation so that your web browser can access the service through an HTTPS connection.

Internet access to the service is not required from the Cognos Analytics server. The service provides the base maps and the polygons only. No user data is sent to the cloud service.

## Memory settings

Memory settings depend on many factors, such as the level of activity that is expected on the server, the complexity of the IBM Cognos applications, the number of users and requests, and acceptable response times.

If your environment supports more than 100 named users, is complex, experiences high peak usage periods, or includes any combination of these factors, consider completing a capacity plan.

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

## Finding memory requirements for your release of Cognos Analytics

Each Cognos Analytics release has a unique list of supported software and minimum requirements to help guide you when you are doing capacity planning. To see the memory requirements for your Cognos Analytics 12.0.x release, follow these steps:

1. Go to the [IBM Cognos Analytics on Premises 12.0.x Supported Software Environments page](https://www.ibm.com/support/pages/node/6966712) (https://www.ibm.com/support/pages/node/6966712).
2. Find the table for your release. Then, under **Requirements by type**, click **Hardware**.

A report lists the hardware requirements for each supported platform.

3. In the **Hardware** column for your platform, find the **Memory** row and then read the associated requirement.

### Example for release 12.0.3

If you are running Cognos Analytics 12.0.3 on Windows and follow the previous steps, a hardware compatibility report tells you that the Cognos Analytics server requires a minimum of 32 GB of RAM.

See the following diagram:

## Windows

Filter

Hardware	Components	Requirement	Applicable Operating System
Disk Space	Desktop <ul style="list-style-type: none"> <li>Transformer</li> </ul>	A minimum of 10 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 Analytics components.  Ensure that you have sufficient disk space for future requirements, as by default each user can use 500MB of disk space for uploaded files.	All supported Windows operating systems
	Server <ul style="list-style-type: none"> <li>Cognos Analytics Server</li> </ul>	A minimum of 10 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 Analytics components.  Ensure that you have sufficient disk space for future requirements, as by default each user can use 500MB of disk space for uploaded files.	All supported Windows operating systems
Memory	Server <ul style="list-style-type: none"> <li>Cognos Analytics Server</li> </ul>	We recommend a minimum requirement of 32 GB. For each deployment, a sizing exercise is highly recommended.	All supported Windows operating systems
	Desktop <ul style="list-style-type: none"> <li>Transformer</li> </ul>	We recommend a minimum requirement of 8 GB. For each deployment, a sizing exercise is highly recommended.	All supported Windows operating systems
Network: adapters, drivers, protocols	Server <ul style="list-style-type: none"> <li>Cognos Analytics Server</li> </ul>	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.	All supported Windows operating systems
Processor	Desktop <ul style="list-style-type: none"> <li>Transformer</li> </ul>	We recommend a minimum requirement of 4 CPU cores for one user. For each deployment, a sizing exercise is highly recommended.	All supported Windows operating systems

## Set the ulimit values on UNIX and Linux operating systems

Setting the appropriate ulimit values on your UNIX or Linux operating system can affect how IBM Cognos Analytics performs.

For example, on Linux operating systems, problems that are caused by stack ulimit settings include unusually high memory usage of BIBusTKServerMain or BIBusTKServerMain errors when large reports are processed.

If you are using the report service on Linux operating systems, running reports or idle BIBusTKServerMain processes can use all of your available RAM.

Whereas, on UNIX operating systems, issues can arise if the stack ulimit settings are too low.

Ensuring the correct stack ulimit settings can prevent these problems.

The recommended ulimit settings for a new installation are as follows:

### IBM AIX®

- CPU time (seconds): ulimit -t unlimited
- File size (blocks): ulimit -f unlimited
- Maximum memory size (kbytes): ulimit -m unlimited
- Maximum user processes: ulimit -u unlimited
- Open files: ulimit -n 8192 (minimum value)
- Stack size (kbytes): ulimit -s 8192 (minimum value)
- Virtual memory (kbytes): ulimit -v unlimited

### Linux (x, z, and p)

- CPU time (seconds): ulimit -t unlimited
- File size (blocks): ulimit -f unlimited
- Maximum memory size (kbytes): ulimit -m unlimited
- Maximum user processes: ulimit -u unlimited
- Open files: ulimit -n 8192 (minimum value)
- Stack size (kbytes): ulimit -s unlimited
- Virtual memory (kbytes): ulimit -v unlimited

**Note:** These settings may need to be adjusted for your environment during the lifecycle of the application.

## Configuring a Content Security Policy

If you think that your company may use a Content Security Policy (CSP), you must complete the following procedure.

**Important:** You or someone else in your company is responsible for configuring and maintaining your CSP. Cognos Analytics does not configure CSPs.

### Procedure

1. Determine whether your company uses a CSP.  
**Tip:** If there is no CSP governing the Cognos Analytics environment, Cognos Analytics can run as usual. All of its features are available.
2. Verify that the CSP includes all mandatory CSP directives.
3. Ensure that your CSP includes the correct directives if you plan to use any of the features that require other CSP directives.
4. Check whether your CSP includes these two directives:
  - `script-src 'unsafe-eval' ;`
  - `script-src 'unsafe-inline' ;`**Tip:** If the two directives appear in the CSP, Cognos Analytics can run as usual. All of its features are available.
5. If the directives `script-src 'unsafe-eval' ;` and `script-src 'unsafe-inline' ;` are **not** included in the CSP, do the following:
  - [Disable the predefined set of blocked features.](#)
  - Review the list of [additional feature limitations](#).

### Mandatory CSP directives

If a CSP is running in your environment, it must include the following directives for Cognos Analytics to work.

- `default-src 'self' ;`
- `script-src 'self' ;`
- `connect-src 'self' *.mapbox.com *.ibm.com ;`
- `frame-src 'self' ;`
- `worker-src 'self' blob: ;`
- `style-src 'self' 'unsafe-inline' ;`
- `img-src 'self' data: blob: ;`
- `font-src 'self' data: ;`

### Other CSP directives required by Cognos Analytics features

The following table lists some additional CSP directives that are required for certain features.

CSP directive	Associated Cognos Analytics feature
<code>script-src 'self' d3js.org ;</code>	Allows custom visualizations to be added to a report.

CSP directive	Associated Cognos Analytics feature
<pre>connect-src ws:// Jupyter_server_host:Jupyter_server _port</pre> <p>or, if Jupyter server is secured:</p> <pre>connect-src wss:// Jupyter_server_host:Jupyter_server _port</pre>	<p>Allows Jupyter Notebook Editor to work.</p> <p><b>Note:</b> The host and port must match the Jupyter service location in Cognos Analytics.</p>
<pre>img-src https://avatars.slack- edge.com/ ; https://*.wp.com ;</pre>	<p>Allows user profile pictures and avatars to appear when you are sharing an asset users via Slack.</p>

## Java requirements

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

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

### Cryptographic standards

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

For more information about the supported Java versions for IBM Cognos Analytics, see the [IBM Cognos Analytics on Premises 12.0.x Supported Software Environments](https://www.ibm.com/support/pages/node/6966712) (https://www.ibm.com/support/pages/node/6966712).

For more information about this security standard, see the [IBM SDK, Java Technology Edition Knowledge Center](http://www.ibm.com/support/knowledgecenter/SSYKE2/welcome_javasdk_family.html) (www.ibm.com/support/knowledgecenter/SSYKE2/welcome\_javasdk\_family.html).

### JAVA\_HOME

Set a JAVA\_HOME environment variable if you want to use your own Java.

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

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

To verify that your JRE is supported, see the [IBM Cognos Analytics on Premises 12.0.x Supported Software Environments](https://www.ibm.com/support/pages/node/6966712) (https://www.ibm.com/support/pages/node/6966712).

### Unrestricted JCE Policy File

JREs include a restricted policy file that limits you to certain cryptographic algorithms and cipher suites. If you require a wider range of cryptographic algorithms and cipher suites, unrestricted (unlimited) policy files are now provided by default. They can be found here:

- install location/ibm-jre/jre/lib/security/policy/unlimited/US\_export\_policy.jar
- install location/ibm-jre/jre/lib/security/policy/unlimited/local\_policy.jar

In addition, for Java that is provided by IBM, the unrestricted JCE policy files are also available [here](#).



## Review the default port settings

After installation, you can use the configuration tool to change the default IBM Cognos Analytics settings. The **Easy** installation type selects port settings for you.

**Important:** These ports must be open to inbound and outbound traffic.

### Default port settings for Cognos Analytics components

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

Table 3. Default port settings for Cognos Analytics components		
Setting	Default Value	Description
Content Manager URI	http://localhost:9300/p2pd/servlet	The URI to Content Manager.
Gateway URI	http:// computer_name:port/bi/v1/ disp	The URI to the gateway.
Dispatcher URI (Internal, External)	http://localhost:9300/ p2pd/servlet/dispatch	The URI to the dispatcher.
Dispatcher URI for external applications	http:// localhost:9300/bi/v1/disp	The URI to the dispatcher.
Log server port	9362	The port used by the local log server.
Member synchronization port	4300	The local port used for network communication that transfers and synchronizes configuration information from one server to another.
Member coordination port	5701	The local port used for network communication for group coordination. This port is used to discover and join a group, and to maintain an up to date list of configuration group members.
Dataset Service port	9301	The local port that is used for inter-process communication. This port is assigned when Cognos Analytics is started for the first time. The port number is based on the Cognos Analytics dispatcher port plus 1. For example, 9300 +1 = 9301.

Table 3. Default port settings for Cognos Analytics components (continued)

Setting	Default Value	Description
Compute Service port number	0	The local port that is used by the Compute service. Ensure that you specify a port that is not already in use. The value must be in the range 0 - 65535. If you specify 0, the Compute service assigns the port dynamically. For any other value, the Compute service will use the port number that you specify.
NodeJS Services port range	9303-9323	<p>Specifies the port range used by the nodeJS services. Ensure that you specify a port range that includes at least 10 available ports.</p> <p><b>Note:</b> Some Cognos Analytics components use these dynamically assigned ports for back-end services that use NodeJS. The NodeJS back-end services are located in <i>installation_location\node-services\services</i>. Here are two examples:</p> <ul style="list-style-type: none"> <li><i>installation_location\node-services\services\ca-dataplatform-server</i></li> <li><i>installation_location\node-services\services\mobile-gateway</i></li> </ul>

For more information, see [“Port and URI settings”](#) on page 169.

## Guidelines for creating the content store

The content store is a database that is used 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 a supported enterprise-level database as the content store in a production environment.

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 Analytics product. If you use the Easy (previously Ready to Run!) option, Informix is installed and configured to use as your content store.

If you are using IBM Db2 for your content store, you can generate a DDL to allow your database administrator to create a Db2 database suitable for the content store. For more information, see [“Generating a script file to create a database for an IBM Db2 content store”](#) on page 100.

## Database properties

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

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

Table 4. Character encoding and protocols for the content store database		
Database	Character encoding	Protocol
Db2	UTF-8	TCP/IP
Oracle	AL32UTF8 or AL32UTF16	TCP/IP
Microsoft SQL Server	UTF-8 or UTF-16	TCP/IP
Informix	UTF-8	TCP/IP

## Collation sequence

Cognos Analytics uses a single sort order that specifies the rules used by the database to interpret, collect, compare, and present character data. For example, a sort order defines whether the letter A is less than, equal to, or greater than the letter B; whether the collation is case sensitive; and whether the collation is accent sensitive. For more information about collation and collation sequences, see the [ICU - International Components for Unicode web site](http://site.icu-project.org/) (<http://site.icu-project.org/>), select the User Guide, and search for Collation.

## Suggested settings for creating the content store in IBM Db2 on Linux, Windows, and UNIX operating systems

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

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

## Guidelines for creating the content store

Use the following checklist to help you set up the content store on Db2.

- Set the appropriate environment variables for Db2, which are as shown in the following table.

Table 5. Environment variables for Db2	
Environment variable	Description
DB2PATH	The top-level directory that contains the database client software or the entire database installation.

Table 5. Environment variables for Db2 (continued)

Environment variable	Description
LD_LIBRARY_PATH	<p>The load library path.</p> <p>Add the driver location to the path, and replace the double hash symbol with 64-bit.</p> <p>For Windows: LD_LIBRARY_PATH= \$DB2_location/sql/lib/lib##: \$LD_LIBRARY_PATH</p> <p>For Linux: LD_LIBRARY_PATH= \$DB2DIR/lib/lib##: \$LD_LIBRARY_PATH</p> <p>For AIX: LIBPATH=\$DB2DIR/lib/lib##:\$LIBPATH</p>
DB2INSTANCE	The default database server connection.
DB2CODEPAGE	<p>Setting this optional environment variable to a value of 1208 provides support for multilingual databases.</p> <p>For information about whether to use this environment variable, see the Db2 documentation.</p>

- Use **UTF-8** as the code set value when you create the database.

To check that your database has the correct code set, using the command-line interface, and type the following at the command prompt:

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

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

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

Table 6. Configuration parameters for Db2

Property	Setting
Application heap size (applheapsz)	<p>AUTOMATIC or at least 1024 KB</p> <p>If the application heap size value is too small, out of memory errors may occur when there are many users.</p>
Lock timeout (locktimeout)	<p>240 seconds</p> <p>Do not set this to an infinite timeout value.</p>
Db2 registry variable (DB2_INLIST_TO_NLJN)	<p>YES</p> <p>Setting this variable to YES improves performance.</p>

- Create a buffer pool with a page size of 32 KB, and a second one with a page size of 8 KB.
  - Create a system temporary tablespace using the 32 KB buffer pool you created in the previous step.
  - Create a user temporary tablespace using the 8 KB buffer pool you created.
- Global temporary tables will be created in the user temporary tablespace.
- Grant the following database privileges for the user account IBM Cognos Analytics will use to access the database:

- Connect to database
- Create tables
- Create schemas implicitly

**Tip:** If you want to host more than one content store on your Db2 instance and you use both at the same time, use a different user account for each content store to ensure that each IBM Cognos Analytics 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 Analytics that you will use to access the database, and ensure the user has create, drop, and alter permissions for the schema.
- Create a profile that sources the `sqllib/db2profile` from the Db2 user's home directory. For example, the content of your profile will be similar to the following:

```
if
[ -f /home/db2user/sqllib/db2profile ]; then
./home/db2user/sqllib/db2profile
fi
```

- Your database administrator must back up IBM Cognos Analytics 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 IBM Db2 on z/OS

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

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

Use the following checklist to help you set up the content store in Db2 on z/OS®.

- Log on to the z/OS system as a user with System Administrator (SYSADM) or System Control (SYSCTRL) privileges in Db2 to create the database.
- Create a database instance, storage group, and a user account for the content store.

IBM Cognos Analytics uses the credentials of the user account to communicate with the database server.

- Ensure that you reserve a buffer pool with a page size of 32 KB, and a second one with a page size of 4 KB for the database instance.
- Administrators must run a script to create table spaces to hold Large Objects and other data for the content store and grant user rights to the table spaces. For information about running the script, see [“Creating tablespaces for a content store on IBM Db2 for z/OS ” on page 100](#).
- Your database administrator must back up the content store regularly because it contains the IBM Cognos data application and security information. To ensure the security and integrity of the content store database, protect it from unauthorized or inappropriate access.

## Suggested settings for creating the content store in Oracle

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

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

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

- Ensure that the parameter for the database instance compatibility level of the content store database is set to 9.0.1 or higher.

For example, you can check the COMPATIBLE initialization parameter setting by issuing the following SQL statement:

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

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

- Determine if the database is Unicode.

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

```
select * from NLS_DATABASE_PARAMETERS
```

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

If using the compatible query mode, you might want to specify the COGUDA\_EXTENDEDCHAR\_SUPPORT environment variable with value T or t. This variable replaces substrng expressions with SUBSTRC for Oracle to return correct results when the string contains Unicode supplementary characters.

- Determine which user account is to access the database.

**Tip:** If you want to host more than one content store on your Oracle instance and you will use both at the same time, use a different user account for each content store to ensure that each IBM Cognos Analytics 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 Analytics databases regularly because they contain the Cognos data. To ensure the security and integrity of databases, protect them from unauthorized or inappropriate access.

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

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

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

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

- Ensure that the collation sequence is case-insensitive.

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

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

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

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

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

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

## Suggested settings for creating the content store in IBM Informix database server

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

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

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

- Set the following environment variables:
  - Set **GL\_USEGLU** to 1 to enable International Components for Unicode (ICU) in Informix database server.
  - Set **DB\_LOCALE** to `en_us.utf8` to set the database locale to Unicode.
- 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**.

## Configure a User Account or Network Service Account for IBM Cognos Analytics

---

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

The user or network service account under which IBM Cognos Analytics runs must:

- have access to all required resources, such as printers
- have the rights to log on as a service and act as part of the operating system

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

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

### Configure a User Account

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

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

## 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 systems.

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 Analytics components use default browser configurations. Additional required settings are specific to the browser.

### Browser settings required for Cognos Analytics

The following table shows the settings that must be enabled.

Table 7. Enabled browser settings	
Browser	Setting
All browsers	Allow pop-ups for all Cognos Analytics pages
Firefox	Allow Cookies Enable Java Enable JavaScript Load Images
Edge	Allow Cookies Enable JavaScript Load Images
Safari 5	Enable Java Enable JavaScript Block Cookies: Never
Google Chrome	Cookies: Allow local data to be set Images: Show all images JavaScript: Allow all sites to run JavaScript

### Cookies used by Cognos Analytics components

Cognos Analytics uses the following cookies to store user information.



Table 8. Cookies used by Cognos Analytics components

Cookie	Type	Purpose
AS_TICKET	Session temporary	Created if Cognos Analytics is configured to use an IBM Cognos Series 7 namespace
caf	Session temporary	Contains security state information
Cam_passport	Session temporary	<p>Stores a reference to a user session stored on the Content Manager server.</p> <p>Administrators can set the HTTPOnly attribute to block scripts from reading or manipulating the CAM passport cookie during a user's session with their web browser.</p> <p>For more information, see the <i>IBM Cognos Analytics Administration and Security Guide</i>.</p>
cc_session	Session temporary	Holds session information
cc_state	Session temporary	Holds information during edit operations, such as cut, copy, and paste
CRN	Session temporary	Contains the content and product locale information, and is set for all IBM Cognos Analytics users. This cookie is required by the Cognos Analytics legacy components. The newer up cookie is similar to this cookie.
up	Session temporary	Stores the user preferences associated with the content and locale settings, and removes some outdated preferences. The cookie is set for all IBM Cognos Analytics users. This cookie is almost identical as the CRN cookie. However, both cookies are required by Cognos Analytics.
CRN_RS	Persistent	Stores the choice that the user makes for the view members folder in Reporting

*Table 8. Cookies used by Cognos Analytics components (continued)*

<b>Cookie</b>	<b>Type</b>	<b>Purpose</b>
PAT_CURRENT_FOLDER	Persistent	Stores the current folder path if local file access is used, and is updated after the Open or Save dialog box is used
qs	Persistent	Stores the settings that the user makes for user interface elements such as menus and toolbars
userCapabilities	Session temporary	Contains all capabilities and the signature for the current user
usersessionid	Session temporary	Contains a unique user session identifier, valid for the duration of the browser session.
XSRF (Cross-Site Request Forgery)	Session temporary	<p>XSRF tricks a web browser into executing a malicious action on a trusted site for which the user is currently authenticated. XSRF exploits the trust that a site has in a user's browser.</p> <p>Prevents a web page loaded from domain X from making requests to domain Y, assuming that the user is already authenticated to domain Y.</p> <p>When first authenticated to Cognos Analytics, XSRF cookie is set. From that point on, all requests will require both the XSRF-TOKEN cookie as well as an HTTP header called X-XSRF-TOKEN.</p>

After upgrading or installing new software, restart the web browser and advise users to clear their browser cache.

---

## Chapter 2. Easy Install

This install option is intended to help you get up and running with IBM Cognos Analytics quickly, without any additional configuration, and without the need to install any supporting software. This option is not recommended for production.

Easy Install is available on Windows only. You must change the configuration to use any of the supported databases for content store, auditing and notification in production environments. The bundled and pre-configured Informix database is not considered production feasible.

### Before you begin

Before you run a Cognos Analytics Easy Install, you must run Windows Update to apply the latest updates. Then restart your computer.

### About this task

This install option is intended to help you get up and running with IBM Cognos Analytics in no time, without any additional configuration and without the need to install any supporting software. You can perform only one **Easy Install** on a computer. With this install option, you get the following components with all the configuration already in place:

- A full version of IBM Cognos Analytics software with all the new capabilities for testing.
- Informix 12.10 that is co-installed and configured for use as content store database only.
- A Custom Java Authentication Provider (CJAP) to create and manage users (local server users).
- Cognos Analytics samples (base samples only).

This install option **does not** support:

- Administration or configuration of the deployed Custom Java Authentication Provider (CJAP).
- Administration or configuration of the deployed Informix database.
- Auditing using the deployed Informix database.

**Note:** In order for the Informix user and group to be created locally, the Cognos installer must be run as a **local Administrator**.

### Procedure

1. Download installer executable and repository zip file from <https://www.ibm.com/software/passportadvantage/index.html>.
2. Run installer and follow prompts to begin.
3. The following can be adjusted during the installation process:
  - Install Location
  - Shortcut Name
  - Shortcut Availability

4. Select a User ID and password which we be used to log on.

Password requirement is:

At least one uppercase character, at least one lowercase character, and at least one digit.

At least one special character among (!@#\$), and password length between 15 –20 characters.

**Important:** The minimum password length is 15 characters as per industry standards.

5. Review options and click **Install**.
6. Review messages to ensure installation success.

7. If needed, review logs at `installLocation/uninstall/logs`.
8. Click **Done**.

## **Results**

You can now launch **IBM Cognos Analytics** from the program shortcut.

---

## Chapter 3. Single server installation

A single server installation allows you to run all IBM Cognos Analytics server components on the same machine.

You need administration privileges to install and uninstall IBM Cognos Analytics.

### Before you begin

You must specify fully qualified host names in the values for the following Cognos Configuration fields. Each value you specify must also appear in either the field **Subject Alternative Name > DNS names** or the field **Subject Alternative Name > IP addresses**.

- **Environment**
  - **Gateway URI**
  - **External dispatcher URI**
  - **Internal dispatcher URI**
  - **Dispatcher URI for external applications**
  - **Content Manager URIs**
- **Environment > Configuration Group**
  - **Group contact host**
  - **Member coordination host**
- **Security > Cryptography > Cognos**
  - **Server common name**
  - **Subject Alternative Name > DNS names**
  - **Subject Alternative Name > IP addresses**

### Procedure

1. Sign in to [Passport Advantage](#) and navigate to **Download software and request media**. Follow the instructions on screen to select the installer and repository you want to download.
2. Double click the installer file, and follow the directions in the installation wizard to copy and install the files to your computer.

Installation log files are found here: <installLocation/uninstall/logs>.

3. Once completed, navigate to **Drivers** folder <InstallLocation\drivers> and place appropriate JDBC drivers for **Content Store** and **Audit** databases.
4. Navigate to shortcut location and launch **Cognos Configuration**.
5. If the **Gateway** option was selected, modify the **Gateway URI** to the following format: <http://applicationTierServer:applicationTierPort/bi/v1/disp>.

Use **HTTPS** if SSL is being used. For more information, refer to Chapter 6 of the IBM Cognos Analytics *Configuring Cognos Analytics Guide*.

6. Configure the Audit Database.
  - a. Right click on **Logging > New Resource > Destination**.
  - b. Set the name to **Audit**.
  - c. Set the type to **Database**.
  - d. Right click on **New Resource > Database > Audit**.
  - e. Set the name to **Audit**.

- f. Select the type in **Select your database type**.
  - g. Select the database server and port number.
  - h. Set database user ID and password.
  - i. Set the database name and encryption.
7. Configure the Authentication Provider.
- a. Right click **Authentication Source** > **New Resource** > **Namespace**.
  - b. Set the name.
  - c. Set the Type (Group)
  - d. Set the Type

For more authentication details, please refer to Configuring Cognos Analytics guide, Chapter 7

8. If Content Store is Db2, fill in the following fields:
- a. Database Server and port number.
  - b. User ID and Password for the database.
  - c. Database name and encryption.
9. If Content Store is not Db2, complete the following steps:
- a. Right Click **Content Manager** and select **Delete**. Confirm deletion.
  - b. Right Click **Content Manager** > **New Resource** > **Database**.
  - c. Set the Name.
  - d. Set the Type (Group).
  - e. Set the Database Server and Port number.
  - f. Set the User ID and Password for the database.
  - g. Set the Database name and Encryption.
10. Configure a mail Server.
- a. Click **Notification**.
  - b. Set the SMTP mail server.
  - c. Set account and password, if applicable.
  - d. Set default sender, if applicable.
  - e. Set the SSL encryption enabled value.
11. Configure a notification store.
- a. Click **Notification** > **New Resource** > **Database**.
  - b. Set the name as Notification Store.
  - c. Select your notification store database type in Type.
  - d. Set the database server and port number.
  - e. Set the User ID and password.
  - f. Set the Database name.
  - g. Set the Encryption.
12. Test the configurations to ensure settings are valid. Do this by clicking **Configuration** > **Action Menu** > **Test**.

If you have not set up a **Gateway** you can now access IBM Cognos Analytics here:  
 serverName:9300/bi.

## Required and Optional tasks after installation

The following chart shows required and optional tasks after installing components.

Table 9.

Task	Resources	Required or Optional
<p>You must use one of the supported enterprise-level databases as the content store in a production environment.</p> <p>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.</p>	<p>See <a href="#">“Guidelines for creating the content store” on page 10</a> and <a href="#">“Installing and configuring Content Manager for the content repository” on page 96</a>.</p>	Required
<p>Configure after installing components.</p> <p>These configuration actions are critical to the success of your installation.</p>	<p>For more information, refer to Chapter 1 of the IBM Cognos Analytics <i>Installing Cognos Analytics Guide</i>.</p>	Required
<p>For authenticated logon, you must configure IBM Cognos Analytics components with an appropriate namespace for the type of authentication provider in your environment.</p>		Required
<p>You can create an audit database to store log messages.</p>	<p>For more information, refer to Chapter 3 of the IBM Cognos Analytics <i>Configuring Cognos Analytics Guide</i>.</p>	Optional
<p>Configure your IBM® Cognos® Analytics mail server to send notifications using IBM Cognos Event Studio.</p>	<p>For more information, refer to Chapter 1 of the IBM Cognos Analytics <i>Event Studio User Guide</i>.</p>	Optional
<p>You can use a separate database for notification in situations where you run large volumes of batch reports and email.</p> <p>By default, the notification server uses the same database that Content Manager uses for the content store.</p>	<p>For more information, refer to Chapter 6 of the IBM Cognos Analytics <i>Configuring Cognos Analytics Guide</i>.</p>	Optional

Table 9. (continued)

Task	Resources	Required or Optional
Configure your web server.	<p>You must configure your web server before users can connect to the IBM® Cognos® Analytics portal. For IBM Cognos Analytics 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.</p> <p>For more information, refer to Chapter 4 of the IBM Cognos Analytics <i>Configuring Cognos Analytics Guide</i>.</p> <p>This tool automates the configuration steps based on the IBM Knowledge Center article – Configuring IIS with Cognos Analytics.</p> <p>See <a href="#">Internet Information Services Automated Script</a></p> <p>To view and browse images in the Reporting, configure Web Distributed Authoring and Versioning (WebDAV) on your web server. Report authors can browse for images to include in reports in a way that is similar to browsing a file system. On Microsoft Internet Information Services (IIS) web servers, you must first enable the WebDAV feature, and then configure your web server to access the image location.</p> <p>For more information, refer to Chapter 4 of the IBM Cognos Analytics <i>Configuring Cognos Analytics Guide</i>.</p>	



Table 9. (continued)

Task	Resources	Required or Optional
Configure your web server (continued)	<p>To view and browse images in the Reporting, configure Web Distributed Authoring and Versioning (WebDAV) on your web server. Report authors can browse for images to include in reports in a way that is similar to browsing a file system. On IBM HTTP Server or Apache HTTP Server, you must add directives to your server configuration file, and then configure the directory access.</p> <p>For more information, refer to Chapter 4 of the IBM Cognos Analytics <i>Configuring Cognos Analytics Guide</i>.</p> <p>After you complete this web server procedure, the server can handle requests for static files (such as .js, .html, .css), load balance requests to IBM Cognos Analytics, and route SSO requests through the IBM Cognos Analytics gateway code.</p> <p>For more information, refer to Chapter 4 of the IBM Cognos Analytics <i>Configuring Cognos Analytics Guide</i>.</p>	



---

## Chapter 4. Distributed server installation

A distributed server installation allows you to run IBM Cognos Analytics server components on different machines.

When you install the IBM Cognos Analytics server components, you can specify where to place the application tier, the data tier (Content Manager), and the gateway tier components. Choose this option to maximize performance, availability, capacity, or security based on the processing characteristics of your organization.

You need administration privileges to install and uninstall IBM Cognos Analytics.

### Before you begin

You must specify fully qualified host names in the values for the following Cognos Configuration fields. Each value you specify must also appear in either the field **Subject Alternative Name > DNS names** or the field **Subject Alternative Name > IP addresses**.

- **Environment**
  - **Gateway URI**
  - **External dispatcher URI**
  - **Internal dispatcher URI**
  - **Dispatcher URI for external applications**
  - **Content Manager URIs**
- **Environment > Configuration Group**
  - **Group contact host**
  - **Member coordination host**
- **Security > Cryptography > Cognos**
  - **Server common name**
  - **Subject Alternative Name > DNS names**
  - **Subject Alternative Name > IP addresses**

### Application tier

The application tier contains one or more Cognos Analytics servers. The servers run requests, such as reports, analyses, and queries that are forwarded by the gateway, and renders the interfaces.

To learn how install the application tier component, see [Application Tier Installation](#).

### Data tier: Content Manager

The data tier, also known as Content Manager, manages the storage of application data, including security, configuration data, models, report specifications, and report outputs. Content Manager is needed to publish packages, retrieve and store report specifications, manage scheduling information, and manage the Cognos namespace.

To learn how install the content tier component, see [Content Tier Installation](#).

### Gateway tier

The gateway tier allows you to set up advanced options such as single sign-on with Kerberos security with IIS, or an architecture where the web server is publicly available outside a firewall. IBM Cognos Analytics

uses the web server for load balancing certain requests in addition to hosting and serving static content like icons and image files.

To learn how install the gateway tier component, see [Gateway Tier Installation](#).

## Required and Optional tasks after installation

The following chart shows required and optional tasks after installing components.

Table 10.		
Task	Resources	Required or Optional
<p>You must use one of the supported enterprise-level databases as the content store in a production environment.</p> <p>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.</p>	<p>For more information, refer to Chapter 3 of the IBM Cognos Analytics <i>Configuring Cognos Analytics Guide</i>.</p>	Required
<p>Configure after installing components.</p> <p>These configuration actions are critical to the success of your installation.</p>	<p>For more information, refer to Chapter 1 of the IBM Cognos Analytics <i>Installing Cognos Analytics Guide</i>.</p>	Required
<p>Use a separate database for notification in situations where you run large volumes of batch reports and email.</p> <p>By default, the notification server uses the same database that Content Manager uses for the content store.</p>	<p>For more information, refer to Chapter 6, page 131 of the IBM Cognos Analytics <i>Configuring Cognos Analytics Guide</i>.</p>	Required
<p>For authenticated logon, you must configure IBM Cognos Analytics components with an appropriate namespace for the type of authentication provider in your environment.</p> <p>You can configure multiple namespaces for authentication and then choose, at run time, which namespace you want to use.</p>	<p>For more information, refer to Chapter 7 of the IBM Cognos Analytics <i>Configuring Cognos Analytics Guide</i>.</p>	Required

Table 10. (continued)

Task	Resources	Required or Optional
You can create an audit data base to store log messages.	For more information, refer to Chapter 3 of the IBM Cognos Analytics <i>Configuring Cognos Analytics Guide</i> .	Optional
Configure your IBM® Cognos® Analytics mail server to send notifications using IBM Cognos Event Studio.	For more information, refer to Chapter 1, of the IBM Cognos Analytics <i>Event Studio User Guide</i> .	Optional
Configure your web server.	<p>You must configure your web server before users can connect to the IBM® Cognos® Analytics portal. For IBM Cognos Analytics 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.</p> <p>For more information, refer to Chapter 4 of the IBM Cognos Analytics <i>Configuring Cognos Analytics Guide</i>.</p> <p>This tool automates the configuration steps based on the IBM Knowledge Center article – <a href="#">Configuring IIS with Cognos Analytics</a>.</p> <p>For more information, see <a href="#">Internet Information Server Automated Script</a>.</p> <p>To view and browse images in the Reporting, configure Web Distributed Authoring and Versioning (WebDAV) on your web server. Report authors can browse for images to include in reports in a way that is similar to browsing a file system. On Microsoft Internet Information Services (IIS) web servers, you must first enable the WebDAV feature, and then configure your web server to access the image location.</p> <p>For more information, refer to Chapter 4 of the IBM Cognos Analytics <i>Configuring Cognos Analytics Guide</i>.</p>	Optional

Table 10. (continued)

Task	Resources	Required or Optional
Configure your web server (configure)	<p>To view and browse images in the Reporting, configure Web Distributed Authoring and Versioning (WebDAV) on your web server. Report authors can browse for images to include in reports in a way that is similar to browsing a file system.</p> <p>For more information, refer to Chapter 4 of the IBM Cognos Analytics <i>Configuring Cognos Analytics Guide</i>.</p> <p>After you complete this procedure, the server can handle requests for static files (such as .js, .html, .css), load balance requests to IBM Cognos Analytics, and route SSO requests through the IBM Cognos Analytics gateway code.</p> <p>For more information, refer to Chapter 4 of the IBM Cognos Analytics <i>Configuring Cognos Analytics Guide</i>.</p>	

## Gateway Tier Installation

Procedure to Install the Gateway for IBM Cognos Analytics 11.1.x.

Install the gateway if you plan on setting up advanced options such as single sign-on with Kerberos security with IIS, or an architecture where the web server is publicly available outside a firewall. IBM Cognos Analytics uses the web server for load balancing certain requests in addition to hosting and serving static content like icons and image files.

**Important:** You must specify fully qualified host names in the values for the following Cognos Configuration fields. Each value you specify must also appear in either the field **Subject Alternative Name** > **DNS names** or the field **Subject Alternative Name** > **IP addresses**.

- **Environment**
  - **Gateway URI**
  - **External dispatcher URI**
  - **Internal dispatcher URI**
  - **Dispatcher URI for external applications**
  - **Content Manager URIs**
- **Environment** > **Configuration Group**
  - **Group contact host**
  - **Member coordination host**
- **Security** > **Cryptography** > **Cognos**
  - **Server common name**

- **Subject Alternative Name > DNS names**
- **Subject Alternative Name > IP addresses**

## Procedure

1. Download installer and repository.  
Download from [Passport Advantage](#).
2. Double click installer file and point to repository, when prompted.
3. Select **IBM Cognos Analytics** and desired Install location.
4. Select **Gateway** when prompted and complete installation steps.
5. Navigate to shortcut location and launch **Cognos Configuration**
6. Click **Environment**
7. Under **Gateway Settings** set the Dispatcher URI's for the Gateway to the server/port where the **Application Tier** was installed.  
Example format <http://applicationTierServer:applicationTierPort/bi/v1/disp>
8. Click on **Local Configuration > Action Menu > Test** to test the configuration.
9. **Save** the configuration.
10. Start the **Content Tier**.

## Application Tier Installation

---


Procedure to Install Application Tier of IBM Cognos Analytics 11.1.x

**Important:** You must specify fully qualified host names in the values for the following Cognos Configuration fields. Each value you specify must also appear in either the field **Subject Alternative Name > DNS names** or the field **Subject Alternative Name > IP addresses**.

- **Environment**
  - **Gateway URI**
  - **External dispatcher URI**
  - **Internal dispatcher URI**
  - **Dispatcher URI for external applications**
  - **Content Manager URIs**
- **Environment > Configuration Group**
  - **Group contact host**
  - **Member coordination host**
- **Security > Cryptography > Cognos**
  - **Server common name**
  - **Subject Alternative Name > DNS names**
  - **Subject Alternative Name > IP addresses**

## Procedure

1. Download installer executable and repository zip files.  
Download from [Passport Advantage](#).
2. Double-click installer file.
3. Select **IBM Cognos Analytics** and install location.
4. If you want shortcut available to all users, click **Check box**.
5. Select **Installation Type** as **Custom** and click **Next**.

6. Check **Application Tier**.
7. Review installation options and click **Install**.
8. Review any error messages.
9. Installation log files are found here: <installLocation/uninstall/logs>
10. Click **Done**.
11. In your **Drivers** folder <InstallLocation\drivers>, place appropriate JDBC drivers for **Content Store** and **Audit** databases.
12. Launch **Cognos Configuration**.
13. Click **Environment**
14. Change **HTTP** to **HTTPS** if SSL is being used.  
Refer to For more information, refer to Chapter 6 of the IBM Cognos Analytics *Configuring Cognos Analytics Guide*.
15. If a gateway is to be installed, modify the **Gateway URI** using the following format:  
<webserverName:webserverPort/alias/bi/v1/disp>
16. Under **Other URI Settings** click the  next to **Content Manager URI's** and add the server and port for the **Content Tier** that was previously installed.
17. If the Application server is installed on the same server as another instance of **IBM Cognos Analytics** and that instance was not running at the time the Application Tier was installed, follow these steps:
  - a) Ensure that the following ports are adjusted to open ports:
    - External Dispatcher URI
    - Internal Dispatcher URI
    - Dataset Service Port Number
    - Dispatcher URI for External Applications
  - b) Right click **Environment** > **Configuration Group** > **Retrieve**, and enter the following information that is configured in the Content Tier Installation.
    - **User ID**: User id of an admin user in the namespace
    - **Password**: Password of the above user
    - **Namespace ID**: ID of the namespace
    - **Cognos Analytics URL**: Content manager URL (content\_tier\_server:port\_number:bi)
  - c) Click **OK**.
18. Right click **Configuration Group** > **Retrieve**
  - Set the UserID, password, namespace and URL as configured by the **Content Tier**
  - Set the **Member Synchronization port** and **Member Coordination port**.
19. Click **Logging** and adjust the local log server port number.
20. Configure the Audit Database.
  - a) Right click on **Logging** > **New Resource** > **Destination**.
  - b) Set the name to **Audit**.
  - c) Set the type to **Database**.
  - d) Right click on **New Resource** > **Database** > **Audit**.
  - e) Set the name **Audit**.
  - f) Select the type **Select your database type**.
  - g) Select the database server and port number from **Content Tier** set up.
  - h) Set database user ID and password from **Content Tier** set up.
  - i) Set the database name and encryption from **Content Tier** set up.
21. Configure a Mail Server.



- a) Click **Notification**.
  - b) Set the SMTP mail server.
  - c) Set the account and password, if applicable.
  - d) Set the default sender, if needed.
  - e) Set the SSL encryption enabled value.
22. Configure a Notification store.
- a) Right Click **Notification** > **New Resource** > **Database**. Fill out the following:
    - Set the name **Notification Store**
    - Type - select your notification store database type
    - Database server and port number.
    - User ID and password.
    - Database name.
    - Encryption.
23. **Test** configuration to ensure settings are valid.
- a) Click on **Configuration** > **Action Menu** > **Test**  
 The mail server connection test will fail if mail server is not configured.
24. **Start** the **Application Tier**.
25. You can now access Cognos Analytics at <applicationtierserver:portnumber/bi>

## Content Tier Installation

---

Procedure to Install Content Tier of IBM Cognos Analytics 11.1.x

**Important:** You must specify fully qualified host names in the values for the following Cognos Configuration fields. Each value you specify must also appear in either the field **Subject Alternative Name** > **DNS names** or the field **Subject Alternative Name** > **IP addresses**.

- **Environment**
  - **Gateway URI**
  - **External dispatcher URI**
  - **Internal dispatcher URI**
  - **Dispatcher URI for external applications**
  - **Content Manager URIs**
- **Environment > Configuration Group**
  - **Group contact host**
  - **Member coordination host**
- **Security > Cryptography > Cognos**
  - **Server common name**
  - **Subject Alternative Name > DNS names**
  - **Subject Alternative Name > IP addresses**

### Procedure

1. Download installer executable and repository zip files.  
 Download from [Passport Advantage](#).
2. Double click installer file.
3. Select **IBM Cognos Analytics** and desired install location.
4. Check box if you want shortcut available to all users.

5. Select **Installation Type** as **Custom** and click **Next**.
6. Check **Content Tier**.
7. Review installation options and click **Install**.
8. Review any post installation messages.
9. Installation log files are found here: <installLocation/uninstall/logs>
10. Click **Done**.
11. Navigate to **Drivers** folder <InstallLocation\drivers> and place appropriate JDBC drivers for **Content Store** and **Audit** databases.
12. If SSL is being implemented, import SSL certs. Refer to .
13. Navigate to shortcut location and launch **Cognos Configuration**.
  - a) Click on **Environment**
  - b) Under **Other URI Settings** set the **Dispatcher URI for External Applications** to the server and port where the Application Tier will be installed.  
Format of URI is <http://applicationTierServer:applicationTierPort/bi/v1/disp>
  - c) Use **HTTPS** if SSL is being used.
14. Configure the Audit Database.
  - a) Right click on **Logging** > **New Resource** > **Destination**.
  - b) Set the name to **Audit**.
  - c) Set the type to **Database**.
  - d) Right click on **New Resource** > **Database** > **Audit**.
  - e) Set the name **Audit**.
  - f) Select the type **Select your database type**.
  - g) Select the database server and port number.
  - h) Set database user ID and password.
  - i) Set the database name and encryption.
15. Configure the Authentication Provider.
  - a) Right click **Authentication** > **New Resource** > **Namespace**. Set the following:
    - Name
    - Type (Group)
    - Type
  - b) Select **Security** > **Authentication** > **Cognos** > **Allow anonymous access?**  
Select **False** as its value.
16. If Content Store is DB2, fill in the following fields:
  - a) Database Server and port number.
  - b) User ID and Password for the database.
  - c) Database name and encryption.
17. If Content Store is not DB2, complete the following steps:
  - a) Right Click **Content Manager** and select **Delete**. Confirm deletion.
  - b) Right Click **Content Manager** > **New Resource** > **Database**. Set the following:
    - Name
    - Type (Group)
    - Database Server and port number
    - User ID and Password for the database
    - Database name and encryption

18. Configure a Mail Server.

a) Click **Notification**.

- Set the SMTP mail server.
- Set Account and password, if applicable.
- Set Default sender, if needed.
- Set the SSL encryption enabled value.

19. Configure a Notification store.

a) Right Click **Notification** > **New Resource** > **Database**. Fill out the following:

- Set the name **Notification Store**
- Type - select your notification store database type
- Database server and port number.
- User ID and password.
- Database name.
- Encryption

20. **Test** configuration to ensure settings are valid.

a) Click on **Configuration** > **Action Menu** > **Test**

The mail server connection test will fail if mail server is not configured.

21. **Start** the Content Tier.

Refer to Configuring Cognos Analytics Guide for more details.



---

## Chapter 5. Silent installation, uninstallation, and configuration

Use a silent installation, uninstallation, and configuration to do the following:

- install an identical configuration across several computers on your network
- automate the installation and configuration process by specifying options and settings for users
- install and configure components in a UNIX or Linux environment that does not have XWindows
- uninstall IBM Cognos Analytics.

Before you set up a silent 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 need administration privileges to install and uninstall IBM Cognos Analytics.

---

### Use a silent installation

Use the silent installation to duplicate an installation from one computer to another without being prompted for information.

#### Procedure

1. Ensure that your **DISPLAY** environment variable is unset.
2. Either “Use a response file template” on [page 39](#), or run the installation wizard from a command line with a parameter to save a response file.

For example:

Windows: analytics-installer-3.0.<build>-win.exe -DREPO=<RepoZipPath> -r “C:\ResponseFile\ResponseFile.properties”.

UNIX or Linux: analytics-installer-<build>-<platform>.bin -DREPO=<RepoZipPath> -r “./ResponseFile/ResponseFile.properties”

#### Note:

- The directory, for example C:\ResponseFile, must exist before running the installation wizard.
- <RepoZipPath> refers to the location of the repository.zip file. When upgrading Cognos Analytics, ensure that the path points to the version of this file that is downloaded for the new version of the product.
- Additional command line options can be found here: [Command line options \(https://helpnet.flexerasoftware.com/installanywhere2017/Content/helplibrary/ia\\_ref\\_command\\_line\\_install\\_uninstall.htm\)](https://helpnet.flexerasoftware.com/installanywhere2017/Content/helplibrary/ia_ref_command_line_install_uninstall.htm)

You do not need to run a full install to create a response file. You can launch the install with the -r option and run it until the summary panel, then cancel out of the install. The response properties file will be created once the install exits.

3. After the installation is completed, modify the response file as needed.

The response file contains values that correspond to the values used when the install wizard was run to create the response file. The password entered during the installation is encrypted in the response file.

4. On the computer where you plan to install the software, do one of the following:
  - Insert the appropriate product installation disk, and copy the contents of the disk to your computer.
  - Copy the product installation files you downloaded to your computer.

5. In a command or terminal window, go to the operating system directory where you copied the installation files and type the following command:

- On Windows, where *location* is the directory where you created or copied the *response filename* file:

```
analytics-installer-3.0.<build>-win.exe -DREPO=<RepoZipPath> -f
location\response_filename -i silent
```

**Tip:**

Launch the unattended install response file from a batch file. This makes the install process wait for the install to be completely finished before it returns. Also, add an %errorlevel% echo command at the end of your batch file to know the exit code of the install batch file entries. For example, *install\_location\analytics-installer-3.0.<build>-win.exe -DREPO=<RepoZipPath> -i silent -f location\response\_filename echo %errorlevel%*

If an error occurs during the install, the install's command prompt window may quickly display some important information. The exit code displayed by should be 0 (zero) for success. If the exit code is not 0, there are two options.

- a. View the installation log located under  
*install\_location\logs\IBM\_Cognos\_Analytics\_Install\_<timestamp>.log*
  - b. View an additional output log under the user's temp folder %TEMPDIR%\install\_output\_log\_cognos\_analytics.txt. This log file displays a list of possible exit codes and their descriptions. You can also search for the phrase *Install Error:* for additional details.
- On UNIX or Linux:
- ```
analytics-installer-<build>-<platform>.bin -DREPO=<RepoZipPath> -f
location/response_filename -i silent
```
- To install in a supported language, use the -l <lang\_code> option.

For example, to install in french and create a response file:

Windows: *analytics-installer-3.0.<build>-win.exe -DREPO=<RepoZipPath> -l <lang\_code> -r location\response\_filename.*

UNIX or Linux: *analytics-installer-<build>-<platform>.bin -DREPO=<RepoZipPath> -l <lang\_code> -r location/response\_filename*

To use the response file and install in French, for example in Windows:

```
analytics-installer-3.0.<build>-win.exe -DREPO=<RepoZipPath> -l fr -i
silent -f c:\response\location\responsefile.properties echo %errorlevel%
```

| Table 11. Supported language codes |                      |
|------------------------------------|----------------------|
| Code                               | Language             |
| en                                 | English              |
| es                                 | Spanish              |
| fr                                 | French               |
| it                                 | Italian              |
| ja                                 | Japanese             |
| ko                                 | Korean               |
| pt_BR                              | Portuguese Brazilian |
| zh_CN                              | Chinese simplified   |

| Table 11. Supported language codes (continued) |                     |
|------------------------------------------------|---------------------|
| Code                                           | Language            |
| zh_TW                                          | Chinese traditional |

- Windows PowerShell:

When passing Java properties to the installer with the -D option in Windows PowerShell, you must enclose the -D option and the Java properties within quotation marks ("). You must also enclose other options and arguments within quotation marks:

For example, to generate a silent response file:

```
analytics-installer-3.0.<build>-win.exe "-DREPO=<RepoZipPath>" "-r"
"C:\ResponseFile\ResponseFile.properties"
```

To perform a silent installation:

```
analytics-installer-3.0.<build>-win.exe "-DREPO=<RepoZipPath>" "-f"
"location\response_filename" "-i" "silent"
```

If you specify the -D option at the end of the command, you do not have to enclose the other options and arguments within quotation marks.

For example, to generate a silent response file with the -D option at the end:

```
analytics-installer-3.0.<build>-win.exe -r
"C:\ResponseFile\ResponseFile.properties" "-DREPO=<RepoZipPath>"
```

To perform a silent installation with the -D option at the end:

```
analytics-installer-3.0.<build>-win.exe -f "location\response_filename" -i
silent "-DREPO=<RepoZipPath>"
```

## Results

If a return status other than zero (0) is returned, check the log files for error messages. Errors are recorded in the *install\_location\logs* 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*.

After all errors are resolved, you can [set up an silent configuration](#).

## Use a response file template

You can use a template to create a response file instead of running an installation to generate the response file.

This topic includes three response file templates for the following types of installations: custom install, Easy Install, and client install.

## Procedure

1. Cut and paste from this topic to create the response file you want to use, either for a custom installation or for an Easy Install.
2. Make changes to the response file that you created by following the guidelines in the file.

### Custom install response file template

```
#Template of Response file for IBM Cognos Analytic Software Silent installation
#Note: This template has some old properties to keep it backward compatible with older 11.x
versions
```

```

#If you wish to create a new response file instead you can refer to 'Use a silent
installation' documentation.
#
#This template is for a "Custom" install. If you want to do an "Easy" install
#please use other template, located below.
#
#(C) Copyright IBM(R) Corp. 2016. All rights reserved.

#Remember to make a copy of this file before editing it.

#Do not change this variable value, as this is a CA install
#-----
BISRVR_CA_INSTALL=1

#Do not change this, as this response file is not for tools
#----
BISRVR_CA_TOOLS_INSTALL=0

#Please DO NOT change the following variable since this is a "Custom" install
BISRVR_INSTALLTYPE_CUSTOM=1

#Required - Install type for "Custom" install
#-----
#You must select one of the following install types
# If you want to perform "Custom/First Install",
#   set BISRVR_CUSTOM_FIRST to be 1, set the other to be 0
# If you want to perform "Custom/Connect and install",
#   set BISRVR_CUSTOM_EXPAND to be 1, set the other to be 0
#-----
BISRVR_CUSTOM_FIRST=
BISRVR_CUSTOM_EXPAND=

#Required - Features
#-----
#For "Custom/First install", feature DATATIER must be selected.
#   Other features can be selected at the same time too.
#For Custom Expand Install, you must select at least one of the features.
#
#BISRVR_FEATURE_DATATIER is called "Content repository" in GUI install.
#BISRVR_FEATURE_APPTIER is called "Application services" in GUI install.
#BISRVR_FEATURE_GATEWAY is called "Optional Gateway" in GUI install.
#CASVR_VIDAImageComponent is called "Image service" in GUI install.(Note: This feature is
available in 11.2.4 and above)
#-----
REPO=<RepoZipPath>
BISRVR_FEATURE_DATATIER=
BISRVR_FEATURE_APPTIER=
BISRVR_FEATURE_GATEWAY=
CASVR_VIDAImageComponent=

#Required - Install Location
#-----
#The installation location
#It is called "Install location" in GUI
# DEFAULT:
#   on UNIX, and Linux
#   /opt/ibm/cognos/analytics
#   on Windows
#   C:\\Program Files\\ibm\\cognos\\analytics
#-----
USER_INSTALL_DIR=

#Optional - Options for Windows Install
#-----
#The following two entries are for Windows only
#BISRVR_SHORTCUT is called "Program folder" in GUI install
#BISRVR_ALLUSERS is called "Make shortcut visible to all users in the Start menu"
#   in GUI install. Set to 1 if you want the shortcut visible.
#-----
BISRVR_SHORTCUT=
BISRVR_ALLUSERS=

#End of Custom install template
#-----

```

## Easy Install response file template

```

#Template of Response file for IBM Cognos Analytic Software Silent installation
#

```



```

#This template is for an "Easy" install. If you want to do a "Custom" install
#please use other template, located above.
#
#(C) Copyright IBM(R) Corp. 2016. All rights reserved.

#Remember to make a copy of this file before editing it.

#Required - Install type for "Easy Install"
#-----
#You must select one of the following install types
# If you want to perform "Easy Install/First Install",
#   set BISVRV_INSTALLTYPE_READY to be 1, set the other to be 0
# If you want to perform "Easy Install/Connect and Install",
#   set BISVRV_INSTALLTYPE_EXPAND to be 1, set the other to be 0
#-----
REPO=<RepoZipPath>
BISVRV_INSTALLTYPE_READY=
BISVRV_INSTALLTYPE_EXPAND=

#Required - Install Location
#-----
#The installation location
#It is called "Install location" in GUI
# DEFAULT:
#   on UNIX, and Linux
#       /opt/ibm/cognos/analytics
#   on Windows
#   C:\\Program Files\\ibm\\cognos\\analytics
#-----
USER_INSTALL_DIR=

#Required - Input Required for "Easy Install"
#-----
#Cognos administrator credentials are required for "Easy Install".
#BISVRV_COGNOSUSER is called "Cognos administrator user ID" in GUI install.
#BISVRV_COGNOSUSER_PASSWORD is called "Password" in GUI install.
# The password must be encrypted. It can be obtained by recording a GUI install.
#-----
BISVRV_COGNOSUSER=
BISVRV_COGNOSUSER_PASSWORD=

#Optional - Options for Windows Install
#-----
#The following two entries are for Windows only
#BISVRV_SHORTCUT is called "Program folder" in GUI install
#BISVRV_ALLUSERS is called "Make shortcut visible to all users in the Start menu"
#   in GUI install. Set to 1 if you want the shortcut visible.
#-----
#BISVRV_SHORTCUT=
#BISVRV_ALLUSERS=

#End of Easy Install template
#-----

```

## Client install response file template

The client applications include: Framework Manager (CA\_FM), Cognos Cube Designer (CA\_DCUBEMODEL), and Dynamic Query Analyzer (CA\_DQA).

```

#Template of Response file for IBM Cognos Analytic Software Silent installation#
#This template is for installing client tools.#
#(C) Copyright IBM(R) Corp. 2016. All rights reserved.

#Remember to make a copy of this file before editing it.

#Do not change this variable value, as this is not a CA install
#-----
BISVRV_CA_INSTALL=0

#Do not change this, as this response file is for tools
#-----
BISVRV_CA_TOOLS_INSTALL=1

#Set only one client tool you need to install to 1
#-----
CA_FM=
CA_DCUBEMODEL=
CA_DQA=

```

```
#manifest
#-----
#Examples:
#FM Example: MANIFEST=fm-manifest-11.2.0-2105060408-winx64h.json
#DCM Example: MANIFEST=dcubemodel-manifest-11.2.0-2105060408-winx64h.json
#DQA Example: MANIFEST=dqa-manifest-11.2.0-2105060408-winx64h.json
MANIFEST=<product_name>-manifest-<product_version>-winx64h.json

#Set the installation location
USER_INSTALL_DIR=

#repo zip file full path
REPO=
```

**Note:** Running a silent installation might result in errors if the repo zip file that you specified in the **REPO** parameter contains multiple manifests. If you get an error message stating that there are multiple manifests in the repo, generate your own response file by running the installation wizard from a command line with a parameter to save a response file. For more details on using the installation wizard to save a response file, refer to [“Use a silent installation” on page 37](#).

## What to do next

Run your response file according to the instructions in the topic [“Use a silent installation” on page 37](#).

## Use a silent configuration

To use a silent configuration, you must export a configuration from an existing installation that has the same IBM Cognos Analytics components installed. You can then run IBM Cognos Configuration in silent mode.

The exported configuration contains the properties of the IBM Cognos Analytics components that you installed on one computer.

## Before you begin

Ensure that the configuration settings on the computer where you are exporting the configuration are appropriate to use on another computer with the same installed components. For example, if you changed the host name portion of the Gateway URI property from localhost to an IP address or computer name, ensure this setting is appropriate for the new computer's configuration.

## Procedure

1. In IBM Cognos Configuration, from the **File** menu, click **Export as**.
2. When prompted about exporting decrypted content, click **Yes**.
3. If you want to export the current configuration to a different folder, in the **Look in** box, locate and open the folder.
4. In the **File name** box, type a name for the configuration file.
5. Click **Save**.
6. Copy the exported configuration file to the *install\_location*/configuration directory on the computer where you plan to use the unattended configuration.
7. Rename the file to cogstartup.xml.
8. Go to *install\_location*/bin or *install\_location*/bin64 directory.
9. Type the following command:
  - On UNIX or Linux, type  
./cogconfig.sh -s
  - On Windows, type  
cogconfig.bat -s

**Tip:** To view log messages that were generated during an unattended configuration, see the `cogconfig_response.csv` file in the `install_location/uninstall/logs` directory.

You can check if the unattended configuration was successful by checking the return status. A value of zero (0) indicates success and all other values indicate that an error occurred.

## Results

IBM Cognos Configuration applies the configuration settings specified in the `cogstartup.xml` file, encrypts credentials, generates digital certificates, and if applicable, starts IBM Cognos service or process.

## Use a silent uninstallation

---

Use a silent uninstallation to automate the removal of components on several computers that have the same components or remove components on a UNIX or Linux environment that does not have XWindows.

**Tip:** If monitoring tools such as Process explorer, MMC (Microsoft Management Console) are running during the uninstall, they will interfere with the deletion of the services. This applies to all services in general. For example, after uninstalling Cognos Analytics, product services such as ApacheDS, IBM Cognos, and Informix will not be fully removed, but instead they will show in the services panel as stopped and disabled. To avoid this, do not have any monitoring tools running while running the uninstall. Shutting down these monitoring tools after the uninstall will also complete the removal of the services.

## Procedure

Run the uninstallation wizard from a command line with parameters as follows:

Windows: `install_location/uninstall/Uninstall_IBM_Cognos_Analytics.exe -i silent`.

UNIX or Linux: `./install_location/uninstall/Uninstall_IBM_Cognos_Analytics -i silent`



## Chapter 6. Installing IBM Cognos Analytics for Jupyter Notebook Server

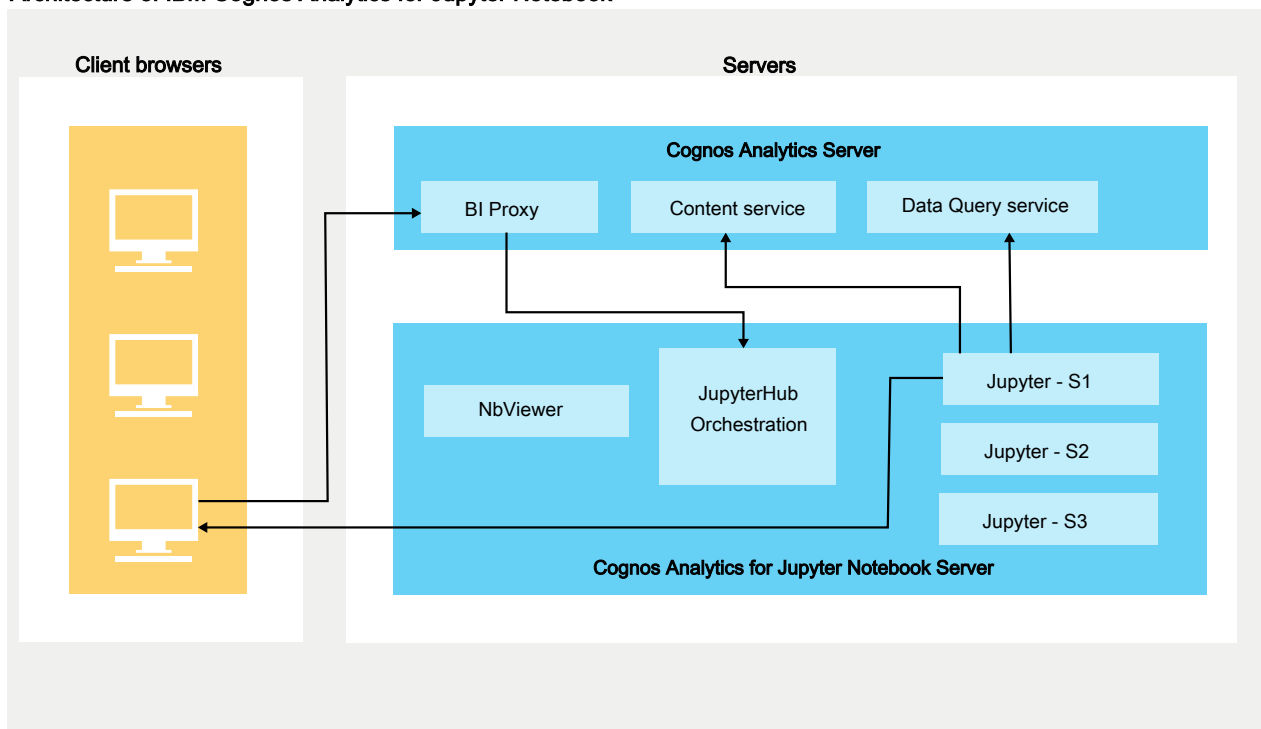
IBM Cognos Analytics includes a version of Jupyter Notebook that is available as a separate installer.

After you install Jupyter Notebook Server, Cognos Analytics users can create and edit Jupyter Notebook in Cognos Analytics.

The two main components of Jupyter Notebook Server are JupyterHub and the Notebook viewer (NbViewer). JupyterHub is the orchestrator that manages multiple server instances.

IBM Cognos Analytics for Jupyter Notebook Server can be installed on the same computer as IBM Cognos Analytics Server or on a different computer. The following diagram shows the server architecture.

**Architecture of IBM Cognos Analytics for Jupyter Notebook**



Before you install Cognos Analytics for Jupyter Server, determine your [hardware requirements](#).

After you install and configure IBM Cognos Analytics for Jupyter Notebook Server, the administrator must perform these tasks:

- Assign the Notebook capability to the appropriate users. For more information, see *Managing IBM Cognos Analytics*.
- Enable IBM Cognos Analytics for Jupyter Notebook. For more information, see *Managing IBM Cognos Analytics*.

### Hardware requirements for Jupyter Notebook Server

The hardware requirements of a Cognos Analytics for Jupyter Server installation depend on the number of concurrent Notebook users and the complexity of their work.

To determine the sizing requirements of your Cognos Analytics Jupyter Server installation, consider these two factors:

- the number of active Notebook sessions that will run concurrently

- the complexity of the operations being performed in Notebook

This section provides some rough estimates of sizing examples.

**Note:** In the following sizing examples, the first three are for a single Cognos Analytics Jupyter Server. However, you can also deploy a clustered architecture behind a reverse-proxy, as described in this [high-failover example](https://community.ibm.com/community/user/businessanalytics/blogs/antonio-marziano/2019/06/18/setup-failover-jupyter-using-nginx-reverse-proxy) (<https://community.ibm.com/community/user/businessanalytics/blogs/antonio-marziano/2019/06/18/setup-failover-jupyter-using-nginx-reverse-proxy>).

### Sizing example 1

- **Usage pattern:** For 10-20 data scientist users with approximately five concurrent Notebook edit/run/schedule sessions.
- **Sizing requirements:** Minimal.

**Note:** Notebook consumers, such as widgets in reports/dashboards, or users who view notebooks in read-only (nbViewer) mode do not contribute significantly to the resource requirements. Only Notebook users who edit, run, and schedule notebooks concurrently require increased resources.

### Sizing example 2

- **Usage pattern:** For small-complexity usage patterns, such as data cleansing and visualizations.
- **Sizing requirements:**
  - Number of CPU Cores: 4
  - RAM: 16 Gb

### Sizing example 3

- **Usage pattern:** For medium-complexity usage patterns, such as profile data quality, random forest classifier, KNN classification and decision trees.
- **Sizing requirements:**
  - Number of CPU Cores: 16
  - RAM: 64 Gb

### Sizing example 4

- **Usage pattern:** For higher-complexity usage patterns, such as deep learning models or neural nets with pyTorch/Tensor Flow.
- **Sizing requirements:**
  - high complexity usage patterns have a different resource profile
  - For example, here are the minimum requirements for a [four-node IBM DSX-Local installation](https://www.ibm.com/support/knowledgecenter/SSAS34_1.2.1/local/requirements.html?view=kc#requirements__5node) ([https://www.ibm.com/support/knowledgecenter/SSAS34\\_1.2.1/local/requirements.html?view=kc#requirements\\_\\_5node](https://www.ibm.com/support/knowledgecenter/SSAS34_1.2.1/local/requirements.html?view=kc#requirements__5node)).

## Installing Jupyter Notebook Server on Linux

---

You can install IBM Cognos Analytics for Jupyter Notebook Server either on the same computer or on a different computer from where Cognos Analytics is installed.

The Jupyter Notebook Server supports Linux and Windows 10 platforms and requires Docker to be installed.

**Note:** Docker CE (Community Edition), Docker Engine, and Docker Desktop (CE) are supported at this time.

When you download and run the installer script, you load and start Docker containers. These containers allow Cognos Analytics users to create and edit Jupyter Notebook. By default, Cognos Analytics for

Jupyter Server is configured with many of the most common data science/analytic Python packages. In Cognos Analytics on Premises 11.1.2, Jupyter Server includes packages from PixieDust.

**Tip:** You can later [upgrade the Python packages](#) in your existing installation.

## Before you begin

Before you install Jupyter Notebook Server, follow these steps:

1. Install Docker or Podman (on RHEL 8 or RHEL 9) as the container engine for Jupyter Notebook.

### To install Docker:

Follow the procedures for one of these Linux distributions:

- [Installing Docker CE for CentOS](#)
- [Installing Docker CE for Ubuntu](#)
- [Installing Docker Engine for Red Hat Enterprise Linux](#)

You must be added to the Docker group for any Docker command to run without root privileges.

### To install Podman on RHEL8 or RHEL9:

Follow the installation and configuration steps at [Podman](#).

**Note:** Throughout the Podman documentation, you will see Podman commands which correspond to particular topics where Docker commands were available.

One of Podman's greatest advantages is its complete CLI compatibility with Docker. When building Podman, Docker users can adapt without any significant changes. For example, you can use the alias command to create a docker alias for Podman:

```
yum install podman-docker
```

**Important:** To enable advanced networking features in Jupyter Server, you must also install the package podman-plugins. Type the following:

```
yum install -y podman-plugins
```

For more information on Podman, see this [Podman developer blog](#).

2. Set the fully qualified domain in Cognos Configuration.
  - a. In IBM Cognos Configuration, in the **Explorer** window, click **Environment**.
  - b. Under the **Dispatcher URI for external applications** set the fully qualified domain name (FQDN) for the IBM Cognos Analytics server.
  - c. Under the **Gateway URI** set the fully qualified domain name (FQDN) for the IBM Cognos Analytics server.
  - d. Click **File > Save**.
  - e. Restart the Cognos Analytics service.

## About this task

For a demonstration of how to install Jupyter Notebook Server, [watch this video](#).

## Procedure

1. Download the IBM Cognos Analytics for Jupyter Notebook Server installer and Server repository from [Passport Advantage](#).

**Tip:** The Jupyter Server installer and Server repository are found only in the Linux eAssemblies.

2. Double click the installer file.
3. Follow the directions in the installation wizard to copy and install the files to your computer.

**Tip:** You can install on top of an older version of Jupyter Server.

The folder `jupyter_installation_location/dist` folder contains two subfolders:

- `dist/images`
- `dist/scripts`

**Tip:** The folder `dist/scripts/unix` contains all the scripts that you need to run.

| Script                    | Purpose                                                                    |
|---------------------------|----------------------------------------------------------------------------|
| <code>build.sh</code>     | Run this to rebuild the images.                                            |
| <code>config.conf</code>  | Edit this <a href="#">configuration file</a> to change Jupyter parameters. |
| <code>install.sh</code>   | Run this to load and start the Docker containers.                          |
| <code>prune.sh</code>     | Run this to remove old Docker images.                                      |
| <code>start.sh</code>     | Run this to start the Jupyter server.                                      |
| <code>stop.sh</code>      | Run this to stop the Jupyter server.                                       |
| <code>uninstall.sh</code> | Run this to uninstall Jupyter server.                                      |

4. Ensure that you have execute permissions for each script:

Type `chmod -R u+x dist/scripts/unix`

5. Navigate to the `dist/scripts/unix` directory.

6. Type `./install.sh`

The install script runs.

## Results

All of the Jupyter Server Docker images are loaded from the `jupyter_installation_location/dist/images` directory and the Docker containers are started.

## What to do next

After installing IBM Cognos Analytics for Jupyter Notebook Server, the following tasks can be performed:

- If you want to change some default settings, you can [configure the Jupyter Notebook Server](#).
- The administrator must assign the Notebook capability to the appropriate users. For more information, see *Managing IBM Cognos Analytics*.
- The administrator must enable IBM Cognos Analytics for Jupyter Notebook. For more information, see *Managing IBM Cognos Analytics*.

## Uninstalling Jupyter Notebook Server

To uninstall Jupyter Notebook Server, navigate to the `dist/scripts/unix` directory and then type `./uninstall.sh`

## Installing Jupyter Notebook Server on Microsoft Windows 10

You can now install IBM Cognos Analytics for Jupyter Notebook Server for Microsoft Windows 10 either on the same computer or on a different computer from where Cognos Analytics is installed.

The Jupyter Notebook Server supports Linux and Microsoft Windows 10 platforms and requires Docker to be installed.

**Note:** Docker CE (Community Edition), Docker Engine, and Docker Desktop (CE) are supported at this time.



When you download and run the installer script, you load and start Docker containers. These containers allow Cognos Analytics users to create and edit Jupyter Notebook. By default, Cognos Analytics for Jupyter Server is configured with many of the most common data science/analytic Python packages. In Cognos Analytics on Premises 11.1.2+, Jupyter Server includes packages from versions of PixieDust.

**Tip:** You can later upgrade the Python packages in your existing installation.

## Before you begin

Before you install Jupyter Notebook Server, follow these steps:

1. Verify that the **Hyper-V Platform** is running so that Linux containers can run on a windows host.
  - a. Open the **Control Panel**.
  - b. Click **Programs**.
  - c. Click **Turn Windows Features on or off**.
  - d. Find and expand the **Hyper-V** option.
  - e. Ensure that the **Hyper-V Platform** is checked.
2. Install Docker as the container engine for Jupyter Notebook.

Follow the Microsoft Windows 10 procedures at [Installing Docker Desktop for Windows](#)

**Important:** The Jupyter server requires that Docker use Linux containers. If your Docker Desktop installation was configured to use Windows containers, do one of the following tasks:

- Right-click the Docker icon in the bottom-right corner of the window and then select the option to switch to Linux containers.
- Re-install Docker Desktop, ensuring that you do not select the option to use Windows containers instead of Linux containers.

You must be added to the Docker group for any Docker command to run without root privileges.

3. Set the fully qualified domain in Cognos Configuration.
  - a. In IBM Cognos Configuration, in the **Explorer** window, click **Environment**.
  - b. Under the **Dispatcher URI for external applications** set the fully qualified domain name (FQDN) for the IBM Cognos Analytics server.
  - c. Under the **Gateway URI** set the fully qualified domain name (FQDN) for the IBM Cognos Analytics server.
  - d. Click **File > Save**.
  - e. Restart the Cognos Analytics service.

## Procedure

1. Download the IBM Cognos Analytics for Jupyter Notebook Server installer and Server repository from [Passport Advantage](#).

**Tip:** See the Cognos Analytics 11.1.5 [Download Document](#) to find out which part number to download.

2. Double click the installer file.
3. Follow the directions in the installation wizard to copy and install the files to your computer.

**Tip:** You can install on top of an older version of Jupyter Server.

The folder `jupyter_installation_location/dist` folder contains two subfolders:

- `dist/images`
- `dist/scripts`

**Tip:** The folder `dist/scripts/windows` contains all the scripts and configuration files for windows installations.

| Script        | Purpose                                                                    |
|---------------|----------------------------------------------------------------------------|
| build.bat     | Run this to rebuild the images.                                            |
| config.conf   | Edit this <a href="#">configuration file</a> to change Jupyter parameters. |
| install.bat   | Run this to load and start the Docker containers.                          |
| prune.bat     | Run this to remove old Docker images.                                      |
| startup.bat   | Run this to start the Jupyter server.                                      |
| stop.bat      | Run this to stop the Jupyter server.                                       |
| uninstall.bat | Run this to uninstall Jupyter server.                                      |

4. Open a command prompt window with administrator privileges.
5. Navigate to the `dist/scripts/windows` directory.
6. Type `./install.bat`

The install script runs.

## Results

All of the Jupyter Server Docker images are loaded from the `jupyter_installation_location/dist/images` directory and the Docker containers are started.

## What to do next

After installing IBM Cognos Analytics for Jupyter Notebook Server, the following tasks can be performed:

- If you want to change some default settings, you can [configure the Jupyter Notebook Server](#).
- The administrator must assign the Notebook capability to the appropriate users. For more information, see *Managing IBM Cognos Analytics*.
- The administrator must enable IBM Cognos Analytics for Jupyter Notebook. For more information, see *Managing IBM Cognos Analytics*.

## Uninstalling Jupyter Notebook Server

To uninstall Jupyter Notebook Server, open a command prompt window with administrator privileges and navigate to the `dist/scripts/windows` directory and then type `./uninstall.bat`

## Installing a pip package in an offline Linux environment

Install Jupyter Notebook Server, including the additional pip package, without internet access.

### About this task

When installing Jupyter Notebook Server, you need to install the PixieDust package `additional_pip_packages.txt`. This task requires internet access, which in some cases might not be available. So you need to download the package before installing Jupyter.

### Procedure

1. Locate the `tar.gz` file for your specific package online, and download it.

The Python Package Index (PyPI) [pypi.org](https://pypi.org) (<https://pypi.org>) website can be used to download most pip packages from the source.

2. Navigate to the `/opt/ibm/cognos/jupyter/dist/scripts/` directory, and create a new directory named `tmp`.

3. Place all of the tar.gz packages that you downloaded into the tmp directory.
4. Open the file /opt/ibm/cognos/jupyter/dist/scripts/Dockerfile\_server\_instance for editing.
5. Modify the file in the following way:
  - a) Under the line:

```
COPY additional_pip_packages.txt /home/ca_user
```

Add the following new line:

```
COPY tmp/ /tmp/
```

This line instructs Docker to take your packages and place them into the Docker container during the build.

- b) Comment out the following section:

```
#COPY additional_conda_packages.txt .
#RUN if [ -s additional_conda_packages.txt ]; then \
# conda install --yes --file additional_conda_packages.txt; \
# fi \
#&& rm additional_conda_packages.txt
```

6. Save the Dockerfile\_server\_instance file ensuring that it's saved without a file extension.
7. Open the file /opt/ibm/cognos/jupyter/dist/scripts/additional\_pip\_packages.txt for editing.
8. Modify the file in the following way:
  - a) Remove the line pixiedust==1.1.17
  - b) Add the following new line /tmp/<package-name>.tar.gz. Ensure that the path matches the exact name of your tar.gz file.
  - c) Add a new line for every package that you want to install this way.
9. Save the additional\_pip\_packages.txt file.
10. Run the Linux installation script by using the following command: /opt/ibm/cognos/jupyter/dist/scripts/unix/install.sh.

## Installing a pip package in an offline Windows environment

Install Jupyter Notebook Server, including the additional pip package, without internet access.

### About this task

When installing Jupyter Notebook Server, you need to install the PixieDust package additional\_pip\_packages.txt. This task requires internet access, which in some cases might not be available. So you need to download the package before installing Jupyter.

### Procedure

1. Locate the tar.gz file for your specific package online, and download it.  
The Python Package Index (PyPI) [pypi.org](https://pypi.org) (<https://pypi.org>) website can be used to download most pip packages from the source.
2. Navigate to the C:\Program Files\ibm\cognos\jupyter\dist\scripts directory, and create a new directory named tmp.
3. Place all of the tar.gz packages that you downloaded into the tmp directory.
4. Open the file C:\Program Files\ibm\cognos\jupyter\dist\scripts\Dockerfile\_server\_instance for editing.
5. Modify the file in the following way:

a) Under the line

```
COPY additional_pip_packages.txt /home/ca_user
```

add the following new line

```
COPY tmp/ /tmp/
```

This line instructs Docker to take your packages, and place them into the Docker container during the build.

b) Comment out the following section:

```
#COPY additional_conda_packages.txt .
#RUN if [ -s additional_conda_packages.txt ]; then \
# conda install --yes --file additional_conda_packages.txt; \
# fi \
#&& rm additional_conda_packages.txt
```

6. Save the `Dockerfile_server_instance` file ensuring that it's saved without a file extension.
7. Open the file `C:\Program Files\ibm\cognos\jupyter\dist\scripts\additional_pip_packages.txt` for editing.
8. Modify the file in the following way:
  - a) Remove the line `pixiedust==1.1.17`
  - b) Add the following new line `/tmp/<package-name>.tar.gz`. Ensure that the path matches the exact name of your `tar.gz` file.
  - c) Add a new line for every package that you want to install this way.
9. Save the `additional_pip_packages.txt` file.
10. Run the Windows installation script by using the following command: `C:\Program Files\ibm\cognos\jupyter\dist\scripts\windows\install.bat`.

## Configuring Jupyter Notebook Server

You can change the default settings in IBM Cognos Analytics for Jupyter Notebook Server by editing the `config.conf` file and by updating Cognos Configuration.

### Procedure

1. Edit the `config.conf` file.
  - a) In a text editor, open the file `jupyter_installation_location/dist/scripts/unix/config.conf` file for Linux or the `jupyter_installation_location/dist/scripts/windows/config.conf` for Microsoft Windows 10.
  - b) Specify values, as required, for the parameters listed in the following table:

| Parameter                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CERTIFICATES_DIRECTORY_PATH     | <p>If you are securing Jupyter Notebook Server using SSL, enter the path to the directory that contains certificates for trusted SSL hosts.</p> <p><b>Tip:</b> We recommend that the directory containing the certificates be located <i>outside</i> the <i>jupyter_installation_location</i> directory. As a result, the certificate files won't need to be moved after subsequent installations and the <code>config.conf</code> file can continue to point to the certificates.</p> <p>For example:</p> <pre>CERTIFICATES_DIRECTORY_PATH=// myjupyterserver.mycompany.com/ certificates</pre> |
| PROXY_CERTIFICATE_FILE_PATH     | <p>If using SSL, enter the path, in Privacy Enhanced Mail (PEM) format, to the certificate file for the Jupyter Server.</p> <p>For example:</p> <pre>PROXY_CERTIFICATE_FILE_PATH=// myjupyterserver.mycompany.com/ certificates/ myjupyterserver.chained.pem</pre>                                                                                                                                                                                                                                                                                                                               |
| PROXY_KEY_FILE_PATH             | <p>If using SSL, enter the path, in Privacy Enhanced Mail (PEM) format, to the certificate private key file for the Jupyter Server.</p> <p>For example:</p> <pre>PROXY_KEY_FILE_PATH=// myjupyterserver.mycompany.com/ certificates/myjupyterserver.my company.com.rsa.key</pre>                                                                                                                                                                                                                                                                                                                 |
| DOCKER_IMAGES_PATH=../../images | <p>If the location of your Docker images changes, update the path to the new location.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| HOST_NAME=\$(hostname)          | <p>You should not need to edit the hostname value. It is resolved automatically if the hostname is set correctly. To check this, type <code>hostname</code> on a command line. The fully qualified name of the computer should be returned. If it is incorrect, you can edit the <code>HOST_NAME</code> value and add the fully qualified name.</p> <p>For example, type the following:</p> <pre>HOST_NAME=myjupyterserver.mycompany .com</pre>                                                                                                                                                  |
| HOST_PORT=8000                  | <p>The port number of the Jupyter Notebook hub.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Parameter      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| COGNOS_HOST    | <p>COGNOS_HOST is an optional parameter that points the Jupyter server to the Cognos Analytics host. By default, the Jupyter server uses the <b>Dispatcher URI for External Applications</b> environment parameter from Cognos Configuration. However, if required, it can be overwritten here.</p> <p>Valid examples: <code>https://cognos.domain.com:9300</code>, <code>http://9.23.132.233:9300</code>, or <code>http://another-cognos-host.com</code></p> <p><b>Note:</b> localhost or 127.0.0.1 cannot be used.</p> |
| SERVER_LIMIT=0 | Specifies the maximum number of users that can be connected at one time. When set to 0 (the default value), no limit is enforced.                                                                                                                                                                                                                                                                                                                                                                                        |
| MEM_LIMIT=     | <p>Specifies the memory limit for each user's container.</p> <p>The value can either be an integer (bytes) or a string with a K, M, G or T prefix.</p> <p>Examples:</p> <p><code>MEM_LIMIT=150M</code></p> <p><code>MEM_LIMIT=2G</code></p> <p>When there is no value (the default), the user container is allocated the memory that it requires.</p>                                                                                                                                                                    |
| CULL_TIMEOUT   | Specifies the idle time of each container, after which the cull service will remove them (default is 3600 seconds).                                                                                                                                                                                                                                                                                                                                                                                                      |
| LOG_INTERVAL   | Specifies, for each container, the time interval between log entries in <code>jupyter_installation_location/dist/logs/timestamp_folder/performance.txt</code> (default is 300 seconds).                                                                                                                                                                                                                                                                                                                                  |

**Important:** After you make any changes to the `config.conf` file, you must follow these steps:

- i) Run the `dist/scripts/unix/build.sh` for Linux or the `dist/scripts/windows/build.bat` for Windows script to apply your changes.
  - ii) Run the `dist/scripts/unix/startup.sh` for Linux or the `dist/scripts/windows/startup.bat` for Windows script to see your changes.
2. Update Cognos Configuration as follows:
- a) Start Cognos Configuration.
  - b) Click **Environment** and set the value for the **Dispatcher URI for External Applications** property.

**Tip:** If you set the `COGNOS_HOST` parameter in the `config.conf` file, you do not need to also set the **Dispatcher URI for External Applications** property in Cognos Configuration.

c) Set the value for the **Gateway URI** property.

**Tip:** You must set this value even if you have not explicitly configured an IIS or Apache gateway.

#### Examples

If no IIS or Apache gateway is configured in front of Cognos Analytics, the **Gateway URI** value is typically the URL to the Cognos server, for example, `https://cognos-host:9300/bi/v1/dispatch`

If another gateway is in place, the **Gateway URI** value must match it, for example, `https://gateway-host:443/ibmcognos/bi/v1/dispatch`

## Configuring the Cognos Analytics gateway for Jupyter Notebook Server

If you installed the Cognos Analytics gateway and you want to integrate Cognos Analytics for Jupyter Notebook Server, you must edit the existing gateway configuration.

### About this task

WebSocket communication is used between the Jupyter Notebook Server and the browser client.

The proxy layer in the Cognos Analytics service manages the dispatching of `http://` and `https://` traffic to the Jupyter server. However, it cannot broker WebSocket requests. Therefore, Notebook WebSocket requests must bypass the Cognos Analytics services layer and connect directly with the Jupyter service behind the Cognos Analytics service.

When Cognos Analytics is using a gateway, you can configure the bypassing of WebSocket traffic by adding a Rewrite Rule to the proxy specification. For more information, see "Configuring the gateway" in the *IBM Cognos Analytics Installation and Configuration Guide*.

### Procedure

1. If you are using an Apache gateway, complete step 5 in the section "Configuring Apache HTTP Server or IBM HTTP Server with Cognos Analytics" in the *IBM Cognos Analytics Installation and Configuration Guide*.
2. If you are using an IIS gateway, proceed as follows:
  - a) Install WebSocket Protocol support in IIS. For more information, see [WebSocket <websocket>](https://docs.microsoft.com/en-us/iis/configuration/system.webserver/websocket) ([https://docs.microsoft.com/en-us/iis/configuration/system.webserver/web socket](https://docs.microsoft.com/en-us/iis/configuration/system.webserver/websocket)).
  - b) Complete step 6d in the topic "Configuring IIS in Cognos Analytics".
3. Restart the Cognos Analytics service.

## Notebook performance logs

Jupyter Notebook performance logs contain information such as memory usage and CPU usage for each Docker container. This is useful if you want to view the usage of notebooks or notebook schedules, as each one uses a separate Docker container.

The performance logs are created in `jupyter_installation_location/dist/logs/timestamp_folder/performance.txt`

Here is an example of log entries in the file `performance.txt`:

```
[2023-03-30 20:51:44]
[1] Container name: ca_jupyter_hub, CPU Usage: 0.00%, Memory Usage: 272.84MiB
[2] Container name: ca_jupyter_viewer, CPU Usage: 0.00%, Memory Usage: 79.75MiB
Total CPU Usage: 0.00%, Total Memory Usage: 352.60MiB

[2023-03-30 20:56:44]
[1] Container name: ca_jupyter_hub, CPU Usage: 0.00%, Memory Usage: 272.87MiB
[2] Container name: ca_jupyter_viewer, CPU Usage: 0.00%, Memory Usage: 79.75MiB
Total CPU Usage: 0.00%, Total Memory Usage: 352.62MiB

[2023-03-30 21:01:44]
[1] Container name: ca_jupyter_hub, CPU Usage: 0.00%, Memory Usage: 272.91MiB
[2] Container name: ca_jupyter_viewer, CPU Usage: 0.00%, Memory Usage: 79.75MiB
Total CPU Usage: 0.00%, Total Memory Usage: 352.66MiB
```

Performance logs are always enabled. By default, the logs are gathered every 5 minutes. You can change this time interval in the `config.conf` file by updating the variable `LOG_INTERVAL`.

The logs capture memory and CPU usage of the Docker containers that the server is running in.

A summary line is added to the bottom of every log that shows the total memory and CPU usage of all active containers in the Jupyter server. This is important to know, because every notebook and schedule creates a new Docker container with its own memory and CPU footprint.

## Troubleshooting

If the performance logs are not always created at equal intervals, there might be excessive load on the system that is impacting the logging service. Read the performance logs to see if memory or CPU usage may be nearing its capacity.

If you change the `LOG_INTERVAL` value in the `config.conf` file, but the new interval isn't applied to the logs, you may have forgotten to re-run the `install.sh` script to apply the changes. Re-running `stop.sh` and `startup.sh` will not apply your change.

## Securing Jupyter Notebook Server

You can secure your Jupyter Notebook Server installation with SSL encryption using SSL certificates.

**Note:** If the Cognos Analytics server is secured with SSL, then the Jupyter Notebook server must also be secured with SSL. Similarly, if the Cognos Analytics server is **not** secured with SSL, the Jupyter Notebook server must also **not** be secured with SSL.

### About this task

For a demonstration of how to secure Jupyter Notebook Server, [watch this video](#).

### Procedure

1. Update the `config.conf` file for SSL encryption.
  - a) Set the value for `CERTIFICATES_DIRECTORY_PATH` with the path to the directory containing the authority certificates for the Jupyter server.
  - b) Set the value for `PROXY_CERTIFICATE_FILE_PATH` with the path to the certificate file for the Jupyter server.
  - c) Set the value for `PROXY_KEY_FILE_PATH` with the path to the private key file for the Jupyter server.

**Tip:** For more information see “Configuring Jupyter Notebook Server” on page 52.

2. Ensure that the administrator specifies `https`, rather than `http`, when they enable IBM Cognos Analytics for Jupyter Notebook. For more information, see *Managing IBM Cognos Analytics*.



3. Register the Jupyter server with the Cognos Analytics server as a trusted third party host.

Regardless if Cognos Analytics server is set up for SSL, you must still register the Jupyter server in the Cognos Analytics trusted service store. Cognos Analytics will not forward a request to an https target without first verifying (by certificate) that the target is trusted and genuine.

This involves importing a copy of the certificate for the secured Jupyter server to the Cognos Analytics trusted service store using the `ThirdPartyCertificateTool` utility provided with Cognos Analytics, in the `installation_location/bin` directory. For more information, see "ThirdPartyCertificateTool commands and examples" in the *IBM Cognos Analytics Installation and Configuration Guide*.

For example, to import a certificate, type the following on a command line at the computer where Cognos Analytics is installed:

```
ThirdPartyCertificateTool -i -T -p NoPassWordSet -r  
fully_qualified_pathname_of_jupyter_certificate_file_in_pem_format
```

4. **Only** if the Cognos Analytics server is also set up for SSL, register the Cognos Analytics server with the Jupyter server as a trusted third party host.
  - a) On the computer where Jupyter Server is installed, create a directory where the certificates will be stored.
  - b) Edit the file `config.conf` and set the `CERTIFICATES_DIRECTORY_PATH` parameter to point to the directory that you just created.
  - c) For each instance of Cognos Analytics that will connect to the Jupyter Server, copy the certificate in Privacy Enhanced Mail (PEM) format for the Cognos Analytics server into the certificates directory that you configured in step "4.b" on page 57.

**Important:** Even though the certificates must be in PEM format, they must have `.crt` file extensions.

- d) Rebuild the image:

In Linux, run `jupyter_installation_location/dist/scripts/unix/build.sh`

In Windows, run `jupyter_installation_location/dist/scripts/windows/build.bat`

- e) Restart the server:

In Linux, run `jupyter_installation_location/dist/scripts/unix/start.sh`

In Windows, run `jupyter_installation_location/dist/scripts/windows/startup.bat`

## Results

The Jupyter Notebook Server is secured with SSL encryption.

## Upgrading IBM Cognos Analytics for Jupyter Notebook Server

You can upgrade IBM Cognos Analytics for Jupyter Notebook Server to a newer version. Alternatively, you can update the Python packages in your existing installation of IBM Cognos Analytics for Jupyter Notebook Server.

**Important:** If the IBM Cognos Analytics for Jupyter Notebook server and its associated libraries are customized by users, support will be provided on a "best effort" basis only.

## Upgrading your installation for Linux

You can install a newer version of IBM Cognos Analytics for Jupyter Notebook Server without manually uninstalling your current version.

**Note:** This task involves specifying a **different location** as your installation directory.

## About this task

For a demonstration of how to upgrade your Jupyter Server installation, [watch this video](#).

## Procedure

1. Follow steps “1” on page 47 to “4” on page 48 in “Installing Jupyter Notebook Server on Linux” on [page 46](#), specifying a different installation location when prompted.
2. If you are upgrading from Cognos Analytics version 11.1.6 or later, copy the files `additional_pip_packages.txt` and `additional_conda_packages.txt` from `current_jupyter_installation_location/dist/scripts/` and paste them into the corresponding folder in your new location: `new_jupyter_installation_location/dist/scripts/`.
3. If you are upgrading from Cognos Analytics version 11.1.5 or earlier, copy the contents of the file `additional_packages.txt` from `current_jupyter_installation_location/dist/scripts/` and paste it into one or both of the following files, as required:
  - `new_jupyter_installation_location/dist/scripts/additional_pip_packages.txt`
  - `new_jupyter_installation_location/dist/scripts/additional_conda_packages.txt`
4. Copy the file `current_jupyter_installation_location/dist/scripts/unix/config.conf` and paste it into the corresponding folder in your new location: `new_jupyter_installation_location/dist/scripts/unix/`.
5. Navigate to the `new_jupyter_installation_location/dist/scripts/unix` directory.
6. Type `./install.sh`

## Results

Your current installation is uninstalled. Then all of the Jupyter Server Docker images are loaded from the `new_jupyter_installation_location/dist/images` directory and the Docker containers are started.

## Upgrading your installation for Microsoft Windows

You can install a newer version of IBM Cognos Analytics for Jupyter Notebook Server without manually uninstalling your current version.

**Note:** This task involves specifying a **different location** as your installation directory.

## About this task

For a demonstration of how to upgrade your Jupyter Server installation, [watch this video](#).

## Procedure

1. Follow steps 1 to 4 in [Installing Jupyter Notebook server on Microsoft Windows 10](#), specifying a different installation location when prompted.
2. If you are upgrading from Cognos Analytics version 11.1.6 or later, copy the files `additional_pip_packages.txt` and `additional_conda_packages.txt` from `current_jupyter_installation_location/dist/scripts/` and paste them into the corresponding folder in your new location: `new_jupyter_installation_location/dist/scripts/`.
3. If you are upgrading from Cognos Analytics version 11.1.5 or earlier, copy the contents of the file `additional_packages.txt` from `current_jupyter_installation_location/dist/scripts/` and paste it into one or both of the following files, as required:
  - `new_jupyter_installation_location/dist/scripts/additional_pip_packages.txt`

- `new_jupyter_installation_location/dist/scripts/additional_conda_packages.txt`
4. Copy the file `current_jupyter_installation_location/dist/scripts/windows/config.conf` and paste it into the corresponding folder in your new location: `new_jupyter_installation_location/dist/scripts/windows/`.
  5. Open a command prompt window with administrator privileges.
  6. Navigate to the `new_jupyter_installation_location/dist/scripts/windows` directory.
  7. Type `./install.bat`

## Results

Your current installation is uninstalled. Then all of the Jupyter Server Docker images are loaded from the `new_jupyter_installation_location/dist/images` directory and the Docker containers are started.

## Upgrading Python packages and R packages

You can add other Python packages or R packages. You can also update the versions of existing Python packages and R packages in your IBM Cognos Analytics for Jupyter Notebook Server installation.

To accomplish this task, you edit the files `additional_pip_packages.txt` and `additional_conda_packages.txt`.

**Note:** The files `additional_pip_packages.txt` and `additional_conda_packages.txt` follow the standard `requirements.txt` file format that is used in Python, as specified in the [PyPA Reference Guide](https://pip.pypa.io/en/stable/reference/pip_install/#requirements-file-format) ([https://pip.pypa.io/en/stable/reference/pip\\_install/#requirements-file-format](https://pip.pypa.io/en/stable/reference/pip_install/#requirements-file-format)).

## Before you begin

Decide whether you need to upgrade. Check to see which versions of Python packages are in your current installation.

**Tip:** To see what is in the modules available in the Notebook environment, type the following in a notebook cell:

```
`!pip list --isolated`
```

You can also, for most Python packages, load a module at runtime for the specific Notebook with the `pip` command. For example, type the following in a Notebook cell:

```
!pip install --user prettyplotlib`
```

## About this task

For a demonstration of how to upgrade Python packages, [watch this video](#).

## Procedure

1. Edit the file `jupyter_installation_location/dist/scripts/additional_pip_packages.txt`

**Tip:** You can add Python packages by specifying them in the `additional_pip_packages.txt` file.

2. Stop the server:

For Linux, run `jupyter_installation_location/dist/scripts/unix/stop.sh`

For Windows, run `jupyter_installation_location/dist/scripts/windows/stop.bat`

3. Rebuild the image:

For Linux, run `jupyter_installation_location/dist/scripts/unix/build.sh`

For Windows, run `jupyter_installation_location/dist/scripts/windows/build.bat`

4. Restart the server:

For Linux, run `jupyter_installation_location/dist/scripts/unix/start.sh`

For Windows, run `jupyter_installation_location/dist/scripts/windows/startup.bat`

5. Edit the file `jupyter_installation_location/dist/scripts/additional_conda_packages.txt` and repeat steps 2-4.

**Tip:** You can add both Python packages and R packages by specifying them in the `additional_conda_packages.txt` file.

## Adding additional Ubuntu operating system packages

You can add operating system packages into your Jupyter notebook server.

To do this, edit the `install_dir>/dist/scripts/additional_os_packages.txt`.

**Note:** Each package name must be written on a new line.

### Procedure

1. Locate the `install_dir>/dist/scripts/additional_os_packages.txt`.
2. Add desired package on a new line.
3. Save the file.
4. Run the server `install.sh` script for Linux or the `install.bat` script for Microsoft Windows.

## Troubleshooting IBM Cognos Analytics for Jupyter Notebook Server

---

To troubleshoot issues with Jupyter Notebook Server, you can use this Docker command: `docker logs container_id`

JupyterHub can provide useful information to help you diagnose a problem. For IBM Cognos Analytics for Jupyter Notebook Server, type the following:

```
docker logs ca_jupyter_hub
```

For more information, see [Troubleshooting](https://jupyterhub.readthedocs.io/en/latest/troubleshooting.html) (<https://jupyterhub.readthedocs.io/en/latest/troubleshooting.html>) on the JupyterHub web site.

### No space left on device when installing Jupyter Server error message

Refer to official [Docker documentation](#) on how to free up space.

#### Note:

Docker stores all of its content (containers, images, and volumes) within `/var/lib/docker` by default.

The default storage location can be changed by adding the "data-root" key to the `daemon.json` file.

More information can be found on the docker daemon configuration file here:

<https://docs.docker.com/engine/reference/commandline/dockerd/#daemon-configuration-file>

<https://docs.docker.com/engine/reference/commandline/dockerd/#daemon-configuration-file>

---

## Chapter 7. Distribution options

Before implementing IBM Cognos Analytics, decide how to install it in your environment. You can install all server components on one computer, or distribute them across a network. The best distribution option depends on your reporting requirements, resources, and preferences. Configuration requirements are different when you install all components on one computer, and when you distribute the components across multiple computers.

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

Cognos Analytics cannot be installed to the same location as other Cognos products, such as Cognos Framework Manager, Cognos Transformer, Cognos PowerPlay, and so on.

---

### Cognos Analytics components

IBM Cognos Analytics is a web-based business intelligence solution with integrated reporting, dashboarding, analysis, event management, and more features. Cognos Analytics includes server and modeling components.

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

**Tip:** When Cognos Analytics is installed using the **Easy Install** option, you do not need to configure a content store database or a security provider. The product is preconfigured and ready to use.

IBM Cognos Analytics runs WebSphere® Application Server Liberty Profile as the application server.

### Server components

The server components for IBM Cognos Analytics are separated into three tiers: data, application, and an optional gateway.

The server components provide the user interfaces for reporting, dashboarding, analysis, event management, and so on, as well as the functionality for routing and processing user requests.

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

- [“Content Tier” on page 61](#)
- [“Application tier: components” on page 62](#)
- [“Gateway tier: web communication” on page 63](#)

**Tip:** The optional gateway is needed for Kerberos only.

As an optional server component, you can also install Cognos Analytics samples. Using data from a fictitious company, the Sample Outdoors Company, the samples illustrate product features and technical and business best practices. You can use the samples for experimenting with and sharing report design techniques, and for troubleshooting. For more information, see the *Samples for IBM Cognos Analytics Guide*.

### Content Tier

Content Manager is the IBM Cognos Analytics service that manages the storage of application data, including security, configuration data, models, report specifications, report outputs, and so on.

Content Manager is needed to publish packages, retrieve and store report specifications, manage scheduling information, and manage the Cognos namespace.

Content Manager stores information in a content store database.

## Application tier: components

The IBM Cognos Analytics applications tier contains one or more Cognos Analytics servers. The servers run requests, such as reports, analyses, and queries that are forwarded by the gateway, and renders the interfaces.

## Configuring and managing the product - IBM Cognos Configuration

IBM Cognos Configuration is used to configure Cognos Analytics, and to start and stop its services.

## Publishing, managing, and viewing content - Cognos Analytics portal

Cognos Analytics portal provides 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 Cognos Analytics applications through the portal. Other applications, and web addresses to other applications, can be integrated with the portal.

## Professional reporting

Using the Reporting tool, report authors create, edit, and distribute a wide range of professional reports.

## Dashboarding

Cognos Analytics provides dashboards to communicate your insights and analysis. You can assemble a view that contains visualizations such as a graph, chart, plot, table, map, or any other visual representation of data.

A dashboard is a type of view that helps you to monitor events or activities at a glance. It provides key insights and analysis about your data on one or more pages or screens.

## Central administration - Manage and Administration Console

Cognos Analytics has a **Manage** function that you can use to perform common administration tasks day to day. An option from the **Manage** menu opens the **Administration Console**, a central management interface that contains the administrative tasks for IBM Cognos Analytics. It provides easy access to the overall management of the IBM Cognos environment. Access to the administration functions depends on user's permissions.

## Monitoring data for exceptional conditions - Event Studio

In Event Studio, you set up agents to monitor your data and perform tasks when business events or exceptional conditions occur in your data that must be dealt with. When an event occurs, people are alerted to take action. Agents can publish details to the portal, deliver alerts by email, run and distribute reports based on events, and monitor the status of events. For example, a support call from a key customer or the cancellation of a large order may trigger an event, sending an e-mail to the appropriate people.

## Microsoft Office compatibility - IBM Cognos for Microsoft Office

Using IBM Cognos for Microsoft Office, Microsoft Office users can access data and visualizations from IBM Cognos reports within Microsoft Office applications, such as Excel, PowerPoint, and Word.

Cognos for Microsoft Office components are included with Cognos Analytics and must be installed separately.

## Gateway tier: web communication

Gateways are often CGI programs, but they can follow other standards, such as Internet Server Application Program Interface (ISAPI) or Apache Modules (apache\_mod). IBM Cognos Analytics uses only CGI, ISAPI or Apache module for Kerberos. Otherwise, you do not need to configure a gateway.

In IBM Cognos Analytics the application tier provides the functions of a gateway.

## Modeling components

Modeling components model data within data sources to structure and present data in a way that is meaningful to users. Modeling components include the following tools:

### IBM Cognos Analytics web modeling

IBM® Cognos® Analytics has a simple-to-use, zero-footprint modeling tool that you can use to quickly create data modules from various data sources. You can use data sources, such as data servers, uploaded files, and previously saved data modules to create data modules. Cognos Analytics data modeling uses intent-driven modeling to generate a module by using terms that you define. For details on all the available features, see the *IBM Cognos Analytics Data Modeling Guide*.

Cognos Analytics data modeling does not replace the more complex modeling capabilities of IBM Cognos Framework Manager or IBM Cognos Cube Designer. These tools are still available in Cognos Analytics.

### Creating a business view of your data - Framework Manager

IBM Cognos Framework Manager is the modeling tool for creating and managing business-related metadata for use in IBM Cognos Analytics. Metadata is published for use by reporting tools as a package, providing a single, integrated business view of any number of heterogeneous data sources.

Framework Manager must be installed to a different location than Cognos Analytics.

### ROLAP modeling - Cube Designer

IBM® Cognos® Cube Designer is the modeling tool provided with IBM Cognos Dynamic Cubes. You use it to build dynamic cubes and publish them for use in IBM Cognos Analytics.

To get started, you import metadata from a relational database. Using the metadata, you model dynamic cubes and save the cube definitions in a project. After you publish the cubes, they are listed as data sources in Content Manager and their related packages are available to report authors.

Cube Designer must be installed to a different location than Cognos Analytics.

### Multidimensional modeling - IBM Cognos Transformer

IBM Cognos Transformer is the IBM Cognos Analytics modeling tool used to create PowerCubes for use in IBM Cognos Analytics. Secured IBM Cognos Analytics PowerCubes are not compatible with IBM Cognos Series 7.

Transformer must be installed to a different location than Cognos Analytics.

**Tip:** For information about installing and configuring versions of Transformer that are earlier than 8.4, see the documentation provided with your edition of Transformer.

## Required database components

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

### Content store

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

When setting up your Cognos Analytics environment, set up the content store to use a supported database that can be secured and tuned for performance and stability. For more information, see the topic about deploying the entire content store in the *IBM Cognos Analytics Administration and Security Guide*.

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

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

### Data sources

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

## Distributing components

---

When you install IBM Cognos Analytics server components, you specify where to place the application tier, the data tier (Content Manager), and the optional gateway tier components.

You can use the following installation scenarios:

- Install all components on one computer.

This option is typically used for departmental deployments, as a demonstration system, or in a proof of concept environment.

- 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.

- Install the optional gateway on a separate computer.

In this option, the gateway and web server are on one computer, and the remaining Cognos components are on other computers. You can choose this option if you have existing web servers that are available to handle Cognos Analytics components requests.

- Consolidate multiple servers by installing on System z®

IBM Cognos Analytics is supported for Linux on System z operating system. This type of installation is suitable when you are setting up or customizing an installation in your environment to suit IT and infrastructure requirements.

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

In addition to installing the data tier (Content Manager), application tier, and optional gateway tier components, you can also install Cognos Framework Manager, the metadata modeling tool, and Cognos Transformer, the modeling tool for creating PowerCubes. No matter which IBM Cognos installation scenario you follow, install the modeling components in separate locations.



## Application Tier Components and Content Managers on separate computers

Application Tier Components balance loads, access data, perform queries, schedule jobs, and render reports. Content Manager stores all report specifications, results, packages, folders, and jobs in the content store.

You can install the Application Tier Components and Content Manager on the same computer, or on different computers. Installing on different computers can improve performance, availability, and capacity.

### More than one Content Manager

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

### Install multiple Content Managers

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

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

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

In the following diagram, the gateway passes the request to the dispatcher (not shown), which passes it to the default active Content Manager computer. Because the computer has failed, the request is redirected to the standby Content Manager computer, which became active when the default active Content Manager computer failed.

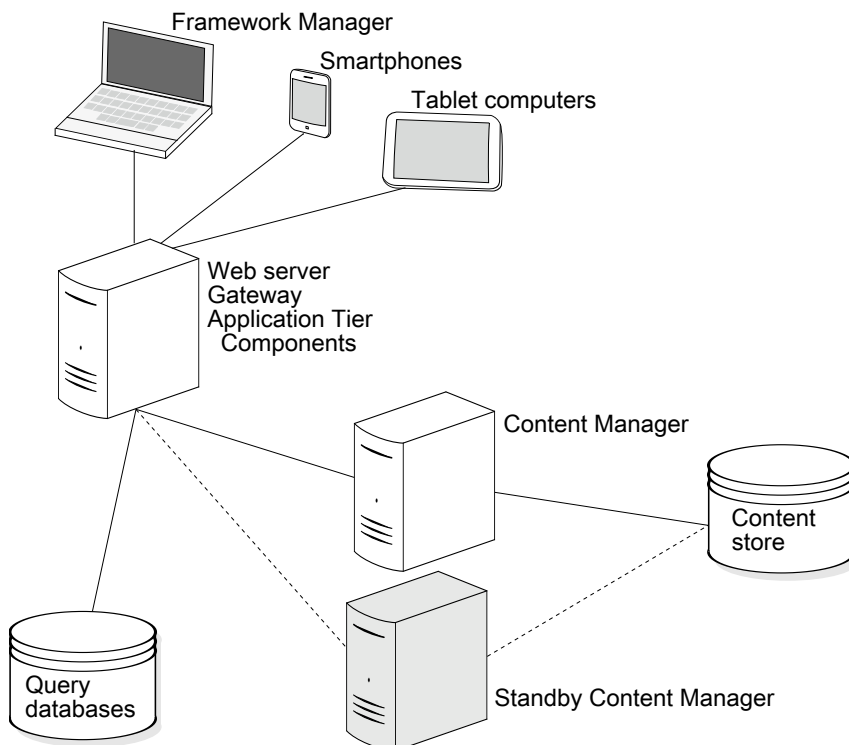


Figure 1. Installation with an active and a standby Content Manager

## 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 server (if you want to email reports or send notifications)

## More than one Application Tier Components computer

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

## Configuration requirements

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

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

## Consolidate servers for Linux on System z

Linux on System z operating system is a native implementation of the Linux operating system. Hosting options include running Linux in one or more logical partitions (LPAR).

## Integrated facility for Linux (IFL)

IFLs are System z processors dedicated to running Linux operating system workloads either natively, or under virtualization software, depending on your needs. IFLs enable you to consolidate and centrally manage Linux resources on System z.

## Logical partition (LPAR) mode

Linux operating system can run in LPARs and communicate with other Linux partitions using TCP/IP connections.

The horizontal scalability in a large Linux environment is limited by the number of LPARs that can be created. Running Linux in LPARs may be best if you are running a small number of Linux images, and those images will each be using a large amount of processing power, or will require a very large amount of dedicated memory. This ensures that the images will not have underutilized resources allocated to them.

## Installation for optional modeling components

---

You install the modeling tools, such as Framework Manager and Transformer on Microsoft Windows operating system computers.

To publish packages so that they are available to users, you must configure the optional modeling tools to use a dispatcher, either directly or through a gateway. If the portal is secured, you must have privileges to create data sources and publish packages in the portal

## Firewall considerations

When the modeling tool is outside a network firewall that protects the Application Tier Components, communication issues with the dispatcher can occur. For security reasons, the default IBM Cognos Analytics configuration prevents the dispatcher from accepting requests from the modeling tool when it is outside the network firewall.

A modeling tool that is outside a network firewall, for example Framework Manager, cannot send requests across a network firewall to the dispatcher on the IBM Cognos Analytics application server. To avoid communication issues when communicating across a network firewall, install the modeling tool in the same architectural tier as the Application Tier Components. The following diagram shows the Framework Manager computer inside the network firewall, successfully communicating with the dispatcher on the IBM Cognos Analytics application server.

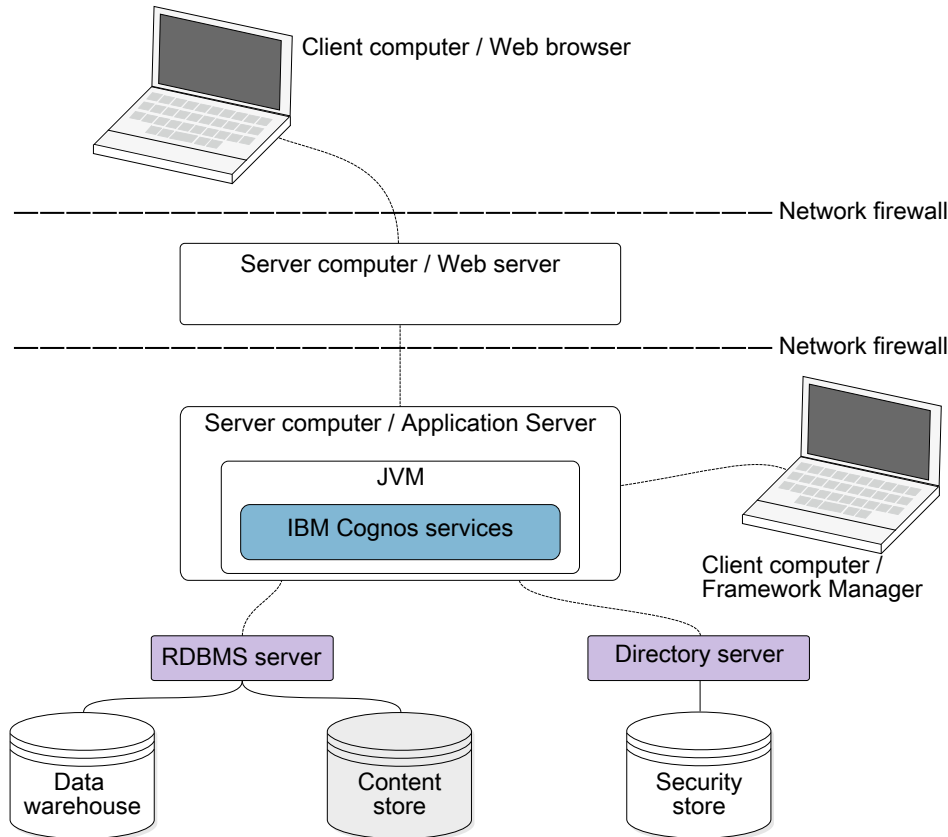


Figure 2. Client computer outside of firewall

Alternatively, you can install an additional gateway that is dedicated to communication with the modeling tool as shown in the following diagram. You then configure the modeling tool and its gateway such that the dispatcher accepts requests from the modeling tool.

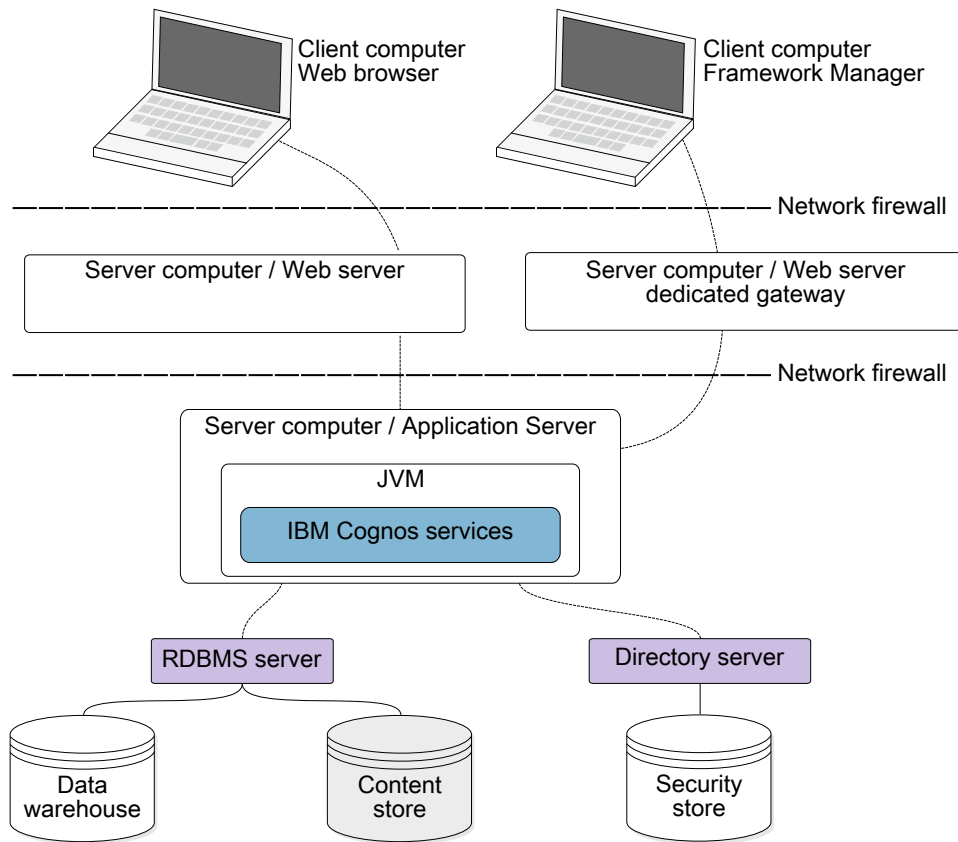


Figure 3. Client computer outside of firewall

## Distributing Framework Manager components

Framework Manager communicates with the Application Tier Components, which can be installed on one or more application servers. To publish packages, you must configure Framework Manager to communicate with the dispatcher, either directly or through a dedicated gateway.

### Configuration requirements

On the computer where Framework Manager is installed, configure the following environment properties:

- **Gateway URI**
- **Dispatcher URI for external applications**

If the modeling tool is using a dedicated gateway instead of communicating directly with the dispatcher, you must also configure the **Dispatcher URIs for gateway** property on the dedicated gateway computer.

## Distributing Transformer components

Transformer can be installed on a computer that contains other IBM Cognos Analytics components or on a computer that is separate from other IBM Cognos Analytics components. When installed separately, Transformer can be used as a standalone product or it can be configured to communicate with other IBM Cognos Analytics components.

Transformer consists of the following components. You may have one or both, depending on your environment.

- Transformer on Windows

This is the modeling tool for Microsoft Windows operating system for designing PowerCubes that are used in IBM Cognos Analytics. It can also be used to build and publish PowerCubes.

- Transformer on UNIX or Linux

This is a command line utility for building PowerCubes on UNIX and Linux operating systems. You first design the models using Transformer Windows or MDL scripting, and then use the models to build the PowerCubes.

You install Transformer PowerCube building components for Linux on System z.

## Supported features

When you use Transformer as a standalone product, you can use data sources that are external to IBM Cognos Analytics and you cannot create secured views with dimensional filtering. When you use Transformer with other IBM Cognos Analytics components, you can use the following features provided by IBM Cognos Analytics:

- IBM Cognos Analytics authentication providers
- IBM Cognos Analytics data sources, such as published packages, Query Studio reports, and Reporting reports

You cannot use flat files as data sources.

- the portal for publishing the PowerCube data source and package
- building PowerCubes

## Role-based server considerations

You may want to set up dedicated Transformer servers for optimal cube build performance and accessibility to the IBM Cognos Analytics users. In this scenario, consider the following requirements:

- Database client software is installed on any computer where Transformer will be used to build PowerCubes or test data sources.
- For data source connectivity, set appropriate environment variables for UNIX and Linux servers.
- IBM Cognos Analytics servers have access to the location where PowerCubes are stored so that the report server can access the PowerCubes.

Building and updating production PowerCubes can be scripted and run remotely when sufficient access and user privileges are set up. For more information about building and updating production PowerCubes, see the Transformer *User Guide*.

## Business analysts or specialists

You may have specialized business or power users who want to build PowerCubes that are modeled on a combination of corporate and personal data sources. These users may want to do their own analysis of the data for their line of business or a small group of users. You can enable such users to be self-sufficient within the IT and security infrastructure of the organization by meeting the following requirements:

- Database client software is installed, or available for modelers to install, on the Transformer computers that are used to access IBM Cognos Analytics data sources.
- Modelers must have privileges to create a data source in IBM Cognos Administration.

Modelers do not need direct access to IBM Cognos Administration. They can create and update data sources by using Transformer or command line tools. You can provide modelers with a secured folder in the portal in which to publish PowerCube packages.

- Modelers must have access to a location in which to store the PowerCube after building it.

This location must also be accessible to the IBM Cognos service and can be a secured share on a LAN.

- To build PowerCubes on a specific Transformer server, modelers should have FTP privileges to transfer models and execute privileges to build cubes on that server.

Modelers can transfer models and execute cube builds using scripts. Modelers can also use automated methods to build PowerCubes. For more information, see the *Administration and Security Guide*.

## Configuration requirements

To publish PowerCube packages, you must configure Transformer to communicate with the dispatcher, either directly or through a dedicated gateway. If IBM Cognos Connection is secured, you must have privileges to create data sources and publish packages in the portal.

On the computer where Transformer is installed, configure the following environment properties:

- **Gateway URI**
- **Dispatcher URI for external applications**

If the modeling tool is using a dedicated gateway instead of communicating directly with the dispatcher, you must also configure the **Dispatcher URIs for gateway** property on the dedicated gateway computer.

## IBM Cognos Analytics with other IBM Cognos products

---

You can install IBM Cognos Analytics in an environment that includes other IBM Cognos products.

The installation wizard for IBM Cognos Analytics can recognize compatible directories and shows a warning when conflicts occur. After IBM Cognos Analytics is installed, you can access objects that are created in another IBM Cognos product in IBM Cognos Analytics. The requirements for access depend on how you choose to run the two products.

### Duplicated Services if Using Multiple Products

Many IBM Cognos products use similar services, such as the report service and the presentation service. If you are using multiple products, such as IBM Cognos Analytics with IBM Cognos PowerPlay®, you must disable some of the duplicated services to ensure your products work properly.

For example, you have IBM Cognos Analytics and IBM Cognos PowerPlay installed. Both products have a reports service and a presentation service. If both products are accessed through the same gateway, reports that must be run on the IBM Cognos Analytics services could be routed to the IBM Cognos PowerPlay services. The result may be that your reports will display an error.

## IBM Cognos products that interoperate with IBM Cognos Analytics

Some IBM Cognos products provide functionality that is not available in IBM Cognos Analytics. You can use these products in the same environment as IBM Cognos Analytics. With some products, you can access the different types of cubes or reports in the IBM Cognos Analytics portal. With other products, you can access unique features in the IBM Cognos Analytics portal.

### Cognos Planning - Analyst

You can access published plan data in IBM Cognos Analytics 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 Analytics server, you must ensure that both products are the same version.

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

### Cognos Planning - Contributor

You can access unpublished (real-time) Contributor cubes in IBM Cognos Analytics by custom installing the IBM Cognos Analytics - 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 Analytics 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 Analytics server, you must ensure that both products are the same version. You cannot install IBM Cognos Planning in the same path as 64-bit IBM Cognos Analytics.

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

## **Cognos Controller**

You can access IBM Cognos Analytics 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.

## **Cognos Transformer**

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

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

Before you load the model, the IBM Cognos Series 7 namespace must be configured in IBM Cognos Analytics and the name ID that is used to configure it in IBM Cognos Analytics 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 Analytics Transformer User Guide*.

For IBM Cognos Series 7 PowerCubes to be used in IBM Cognos Analytics, optimize the cubes for use in IBM Cognos Analytics by using the pcoptimizer utility, which is supplied with IBM Cognos Analytics. Otherwise, PowerCubes that were created with previous versions of Transformer may take too long to open in the IBM Cognos Analytics 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 Analytics portal. You can publish single PowerCube data sources and packages to the portal 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 the portal can publish PowerCubes in the portal as well. The MDC file must be in a secured location that the IBM Cognos Analytics 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 Analytics 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.

## Planning Analytics

IBM Planning Analytics integrates business planning, performance measurement and operational data to enable companies to optimize business effectiveness and customer interaction regardless of geography or structure. Planning Analytics provides immediate visibility into data, accountability within a collaborative process, and a consistent view of information, allowing managers to quickly stabilize operational fluctuations and take advantage of new opportunities.

For more information, see the *IBM Planning Analytics* documentation.



---

## Chapter 8. Upgrading Cognos Analytics

When upgrading IBM Cognos Analytics, you need to back up the content store, upgrade your data, understand the implications of the upgrade on other components in a distributed environment, ensure that files that must be preserved are not overwritten, and possibly perform other upgrade tasks.

### Important:

Do not upgrade your 11.2.4 FP3 content to version 12.0.0, 12.0.1, or 12.0.2. If you do so, you may need to run specialized scripts before you can do another upgrade to version 12.0.3 or later. If you want to upgrade 11.2.4 FP3 content to version 12.0.x, you must wait until 12.0.3 or later to do so.

### Reason:

Schema changes are made in the content store of 11.2.4 FP3 (and future releases) to support faster processing of content retention rules. Therefore, when you upgrade from 11.2.4 FP3 (or later), you must upgrade to a release with the same content store enhancements, for example, 12.0.3 (or later).

You can still upgrade any 11.2.x content **other than** 11.2.4 FP3 to any version of 12.0.x.

### Over-the-top installations are supported

You can upgrade your version of IBM Cognos Analytics by performing an over-the-top installation. This is the default upgrade method, and the simplest and easiest way to upgrade. All components are upgraded to a newer version using the same configuration details, ports, themes and extensions as your previous installation.

The over-the-top upgrade procedure takes advantage of the Cognos Analytics continuous delivery model, and deploys new features quickly and easily.

---

## Data upgrade tasks for Cognos Analytics

To support the optimized user experience in dashboards, explorations, and other components, and to improve query performance on uploaded files and data sets, you must upgrade your data from previous versions of IBM Cognos Analytics.

The upgrade process includes the following two tasks: retrieving some deeper data characteristics from data servers, packages, uploaded files, and data sets, and upgrading the Parquet file format in uploaded files and data sets.

### Retrieve deeper data characteristics from data servers, packages, uploaded files, and data sets

The deeper data characteristics support the product functions that are behind the optimized user experience in dashboards, explorations, and other components. These characteristics are captured from samplings of data from the underlying sources.

Cognos Analytics captures the deeper data characteristics for the following reasons:

- To intelligently set the default column properties, such as **Usage** and **Aggregate**.
- To provide recommendations for visualizations in dashboards, stories, and explorations.
- To determine the subset of fields that are the best candidates to show in the relationship diagram in **Explore**.
- To enable **Assistant** to be more successful in understanding the user's intent.
- To provide other forms of automated assistance.

To retrieve the deeper data characteristics, you need to re-upload your data from previous Cognos Analytics versions using the following methods:

- For data server connections, reload the schemas metadata.

Use the **Load options** option. Ensure that the following check boxes are selected: **Retrieve the primary and foreign keys**, **Retrieve sample data**, **Retrieve statistics** (version 11.1.4 and earlier).

For more information, see the topic about preloading metadata from a data server connection in the *IBM Cognos Analytics Managing Guide*.

- For packages, use the **Enrich package** action.

Use the automatic enrichment option, and ensure that the check boxes **Retrieve sample data** and **Retrieve statistics** (version 11.1.4 and earlier) are selected on the **Load options** tab.

For more information, see the topic about enriching packages in the *IBM Cognos Analytics Managing Guide*.

- For uploaded files and data sets, either run the ParquetUpgrade utility with option **m** or refresh the individual files and data sets manually.

The ParquetUpgrade utility with option **m** retrieves the deeper data characteristics from all uploaded files and data sets in the content store. When running this utility, you will upgrade the Parquet format in the affected files and data sets at the same time. For more information, see [“Running the ParquetMigrate utility”](#) on page 74.

For individual uploaded files, use the **Append file** and **Replace file** options. For individual data sets, use the **Refresh** option.

## Upgrade the Parquet format in uploaded files and data sets

The Parquet file format that is used to store uploaded files and data sets enables faster query processing on uploaded files and data sets.

You can implement this upgrade in the following ways:

- Use the ParquetUpgrade utility to upgrade the Parquet format in all uploaded files and data sets in the content store.

Run this utility before users start running the reports, dashboards, or explorations. This ensures that all workloads immediately benefit from the performance gains associated with the new format. For more information, see [“Running the ParquetMigrate utility”](#) on page 74.

- Manually refresh data in the individual uploaded files and data sets.

Use the **Append file** and **Replace file** options on uploaded files. Use the **Refresh** option on data sets.

- Do not upgrade at all.

When a query uses data that wasn't upgraded, the query service internally initiates the upgrade, and users experience a one-time performance degradation when they run the dashboards, stories, reports, or explorations in your current Cognos Analytics version. Subsequent queries use the upgraded data.

The Parquet format is used automatically when new files are uploaded, new data sets are created, and when deployment archives that contain uploaded files and data sets are imported.

## Running the ParquetMigrate utility

Use the ParquetMigrate utility to apply the new Parquet format to uploaded files and data sets from IBM Cognos Analytics 11.0.x. When used with its option **m**, this utility also retrieves the deeper data characteristics from uploaded files and data sets.

The Parquet format that is used to store data in uploaded files and data sets has changed between Cognos Analytics versions 11.0.x and 11.1. Run the ParquetUpgrade command before users start running dashboards and reports. This ensures that all workloads immediately benefit from performance gains of the new format. If a query uses data that wasn't upgraded, the query service internally initiates the upgrade and the users experience a one-time performance degradation when they run the dashboards, stories, reports, or explorations in Cognos Analytics 11.1. Subsequent queries use the upgraded data.

The ParquetMigrate command supports the following parameters:

**-h URL**

The URL to an active Cognos Analytics server. When you don't specify the URL, the URL that is configured in Cognos Configuration on the computer from which the command is run is used.

**-n Namespace**

The namespace to authenticate into when connecting to the Cognos Analytics server.

**-u User name**

The user name to authenticate with when connecting to the Cognos Analytics server.

**-p Password**

The password to use for authentication to the Cognos Analytics server.

**-d**

Displays information about the uploaded files and data sets in the content store. No objects are upgraded.

**-k**

Ignores the SSL certificate validation. You can use this parameter when running the script in Cognos Analytics with SSL configured. However, you might not need this parameter if the SSL certificate is imported into the keystore of the Java that is used when you run the ParquetMigrate utility. For information about importing certificates, see [“Import the certificate authority \(CA\) certificates” on page 202](#).

**-l**

Applies only to the last used files.

**-t**

Filters displayed results by task ID. Use this parameter only with the -d parameter.

**-s**

Specifies the store ID. The command is applied to the hierarchy, starting with the provided content store ID.

**-m**

Retrieves the deeper data characteristics in Cognos Analytics. For more information, see [“Data upgrade tasks for Cognos Analytics” on page 73](#)

**-a**

Smarts version upgrade only.

## Procedure

1. Open the command line utility, and navigate to the *cognos\_analytics\_location\bin64* directory.
2. Run the ParquetMigrate.bat (Windows) or ParquetMigrate.sh (Unix) utility. The following examples are the commands that you can run:

To display information about uploaded files or data sets, use the following command:

```
ParquetMigrate -d -n namespace -u user_name -p password
```

Or

```
ParquetMigrate -d -h http://cognos_analytics_host:9300 -n namespace -u user_name -p password
```

To upgrade files or data sets, use the following command:

```
ParquetMigrate -n namespace -u user_name -p password
```

To upgrade files and data sets, and at the same time retrieve the deeper data characteristics, use the following command:

```
ParquetMigrate -m -n namespace -u user_name -p password
```

3. Run the command.

## Results

When the command completes, the number of upgraded objects is displayed. A value of 0 indicates that no objects requiring upgrade were found.

## Converting multiple queries and analyses to reports

Bulk Converter can be used to convert a group of objects of type **query** (Query Studio report) or **analysis** (Analysis Studio report) to objects of type **report**. This supports the deprecation of Query Studio and Analysis Studio and allows you to migrate your analysis and query content to Cognos Analytics Reporting.

You can also convert individual query or analysis objects to reports. For more information, see [Open a Report in IBM Cognos Analytics - Reporting](#).

### Before you begin

Bulk Converter is a Java-based graphical user interface (GUI) application, and it is not a console application or command-line program.

You must have the necessary permissions to locate and convert analyses and queries to reports.

#### Notes:

- Anonymous user access is not supported.
- You cannot convert objects in **My content**.
- Schedules of analyses and queries will not be transferred to the converted reports.
- Computers that use UNIX operation system must have X-Window software installed to support GUI applications.

### Converting a group of query and analysis objects to report objects

You can use Bulk Converter to convert multiple query and analysis objects to report objects at once. The Bulk Converter is installed in the *<installation\_location>/sdk/bulkconverter* folder as part of the Application Tier components.

1. On a command line, go to the *<installation\_location>/sdk /bulkconverter* folder.
2. On Windows, type

```
RunBulkConverter.bat
```

OR

On UNIX, type

```
./RunBulkConverter.sh
```

3. Enter the value of **Internal dispatcher URI** from **Cognos Configuration** and log in to the namespace as an authenticated user.
4. Locate and select one or more analyses, queries, and folders containing analyses or queries in the tree pane that shows all the contents in **Team content**.
5. Select **Queries to Reports** from the **Convert** menu to convert the selected query objects to reports.

6. Select **Analyses to Reports** from the **Convert** menu to convert the selected analysis objects to reports.

The results are displayed in the output pane. To see the newly created reports in the tree pane, select **Refresh Tree** from the tree pane or from the **File** menu.

If the conversion is successful, the converted reports are saved with the same names as the originals in the **Converted Analyses** or **Converted Queries** folder located in the same folder as the selected analyses or queries.

**Tip:** If the conversion fails with an analysis or a query, try converting the analysis or query individually and view the error log. For more information, see [Open a Report in IBM Cognos Analytics - Reporting](#).

## Changed modification time property on objects after an upgrade

The modification time property is changed for objects that are affected by the upgrade. The new property value is set to the date and time of the first **Cognos Analytics** service startup after the upgrade.

**Tip:** The modification time is shown in the **Last Accessed** column of the **Content** page, and as the **Modified** property value in the **Details** panel.

The modification time is changed when the object properties are changed between releases, and the object needs to be upgraded in the new release.

These types of upgrades are not done for all releases of Cognos Analytics. An example of such upgrade can be found in version 11.2.4. In this release, folders and packages which had the object capabilities explicitly defined in previous versions of the product needed an upgrade because new object capabilities were added in the release. For more information, see "Changed modification time on folders and packages after an upgrade" in the *IBM Cognos Analytics What's new* guide.

## Preserved files and folders when upgrading Cognos Analytics

You can install a new version of IBM Cognos Analytics over your current, running version of the product without overwriting configuration settings from the previous version.

Files to be preserved by default during an upgrade are listed in the `install_location\configuration\preserve\.ca_base_preserve.txt` file. Do not edit this file.

If you want to remove or preserve other files or directories when upgrading Cognos Analytics, edit the `install_location\configuration\preserve\preserve.txt.template` file. Instructions about using `preserve.txt.template` are included in the file itself. Then, rename the `preserve.txt.template` file to `preserve.txt`.

**Tip:** Hard or soft links that are created by customers within the Cognos Analytics file structure are not supported.

### Files and folders preserved by default

By default, the following folders and files, as specified in the `install_location\configuration\preserve\.ca_base_preserve.txt` file, are preserved in the installation directory when upgrading Cognos Analytics:

```
#####
#
# IBM Confidential
#
# IBM Cognos Products: Preserve Files by the Install
#
# (C) Copyright IBM Corp. 2017, 2021
#
# DO NOT EDIT THIS FILE.
#
# Please use the file <installdir>/configuration/preserve/preserve.txt
# to list files/folders to be preserved during an upgrade installation.
#
#####
```

```
#exclude section must be done first
exclude:deployment/Samples_for_Install.zip
exclude:deployment/Templates.zip
exclude:webcontent/bi/images/cahome_icons.svg
exclude:webcontent/bi/images/authoring_icons.svg
exclude:webcontent/bi/images/admin_icons.svg
exclude:webcontent/bi/images/JupyterNotebook.svg

# Various folders
configuration/certs
configuration/csk
configuration/data
configuration/caSerial
configuration/preserve/preserve.txt
data/cmstorage
data/search
deployment
drivers
ldapschema
informix
war/AuditExt
webcontent/bi/images
webapps/p2pd/WEB-INF/AAA/lib
templates/ps/async/system.xml

# Miscellaneous files.
uninstall/cognos_ex.ldif
uninstall/logs/pre_upgrade.log
webapps/p2pd/WEB-INF/web.xml
wlp/usr/servers/cognosserver/bootstrap.properties
wlp/usr/servers/cognosserver/jvm.options
wlp/usr/servers/cognosserver/server.xml
wlp/usr/servers/dataset-service/bootstrap.properties
wlp/usr/servers/dataset-service/jvm.options
wlp/usr/servers/dataset-service/server.xml
wlpdropins/AuditExt.war
cgi-bin/web.config

# Configuration files
configuration/cogconfig.prefs
configuration/cogconfig_reg.txt
configuration/coglocale.xml
configuration/cogstartup.xml
configuration/c11AuditExtension.keystore
configuration/dispatcher.properties
configuration/install_gatewayurl.xml
configuration/installData.properties
configuration/ipfclientconfig.xml
configuration/configuration/caSerial
configuration/xqe.config.custom.xml
configuration/xqe.diagnosticslogging.xml
configuration/local-server.xml
configuration/Series7Namespaces.xml
configuration/Launch IBM Cognos Analytics.url
configuration/cjap_directory.json

# webcontent files
webcontent/web.config
webcontent/bi/web.config
```



### Attention:

If you are running version 12.0.0, 12.0.1, or 12.0.2, the file `.ca_base_preserve.text` is missing some references to other files. You must fix this issue. However, you cannot edit the file `.ca_base_preserve.txt`. Instead, you create (or modify if it exists) a file named `preserve.text`.

Follow these steps:

1. Go to the folder `install_location/configuration/preserve`.
2. In a text editor, do one of the following:
  - Open the file `preserve.txt`, if it already exists.
  - or
  - Open the file `preserve.txt.template`.

3. Add the following lines:

```
#TM1 files
templates/ps/portal/variables_TM1.xml
templates/ps/portal/variables_plan.xml
templates/ps/portal/icon_active_application.gif
webcontent/planning.html
webcontent/PMHub.html
webcontent/tm1/web/tm1web.html

#CA files
templates/ps/system.xml
templates/ps/portal/system.xml
```

4. Save the file as `preserve.txt`.

For more information, see [The file `.ca\_base\_preserve.txt` is missing references to some files \(existing issue\)](#).

You might need to manually migrate these files and folders under the following circumstances:

- You are installing the new version in a new directory.
- You are uninstalling the current version, and then installing the new version.

Uninstalling the current version completely deletes the *install\_location* directory.

### Preserving other files and folders in Cognos Analytics 11.2.1

In addition to the files and folders that are preserved by default, you can preserve other files in the Cognos Analytics installation directory when upgrading the product to a new version.

Use the *install\_location*\configuration\preserve\preserve.txt.template file to specify the files that you want to preserve. For example, if you want to preserve the samples deployment *install\_location*\deployment\IBM\_Cognos\_Mobile\_Samples.zip, add deployment\IBM\_Cognos\_Mobile\_Samples.zip to the list of preserved files in the preserve.txt.template file. Then, rename preserve.txt.template to preserve.txt.

When you upgrade Cognos Analytics, you can choose to preserve or overwrite the files that are specified in the preserve.txt file. Depending on your decision, the installation proceeds in one of the following ways:

- You choose to preserve files.

New versions of files that are specified in the preserve.txt file are copied to the *install\_location*\configuration\preserved-by-manifest\manifest\_version directory. The .new extension is added to each file in this directory. For example, *install\_location*\configuration\preserved-by-manifest\11.2.1-2108230833\IBM\_Cognos\_Mobile\_Samples.zip.new.

- You choose to not preserve files.

Old versions of files that are specified in the preserve.txt file are copied to the *install\_location*\configuration\preserved-by-manifest\manifest\_version directory. The .old extension is added to each file in this directory. For example, *install\_location*\configuration\preserved-by-manifest\11.2.1-2108230833\IBM\_Cognos\_Mobile\_Samples.zip.old.

### Preserving other files and folders in Cognos Analytics 11.2.0

In addition to the files and folders that are preserved by default, you can preserve other files in the Cognos Analytics installation directory when upgrading the product to a new version.

Use the *install\_location*\configuration\preserve\preserve.txt.template file to specify the files that you want to preserve. For example, if you want to preserve the samples deployment *install\_location*\deployment\IBM\_Cognos\_Mobile\_Samples.zip,

add deployment\IBM\_Cognos\_Mobile\_Samples.zip to the list of preserved files in the preserve.txt.template file. Then, rename preserve.txt.template to preserve.txt.

When Cognos Analytics is upgraded, the files that you chose to preserve are not overwritten. If the new product version contains new versions of the preserved files, the new file versions are saved to the same directory under the name *filename\_manifestversion.new*. Using the samples example, the *install\_location*\deployment directory would contain the following files after the upgrade:

- IBM\_Cognos\_Mobile\_Samples.zip

This is the preserved samples deployment.

- IBM\_Cognos\_Mobile\_Samples.zip\_manifestversion.new

This is the new, Cognos Analytics 11.2 version of the samples deployment.

For example, if the installer uses the manifest casrv -

manifest-11.2.0-2104060200-linux138664h.json, the file name is

IBM\_Cognos\_Mobile\_Samples.zip\_11.2.0\_2104060200.new.

## Standard upgrade process

---

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

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

When planning your upgrade, perform the following tasks:

- Gather the necessary information, such as the required inputs and expected outputs for each phase.
- Assess the applications in your reporting environment and group similar reports together.
- Install the new software in a test environment and deploy the content to the test environment.
- Test the upgraded applications to ensure that your reports run as expected.

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

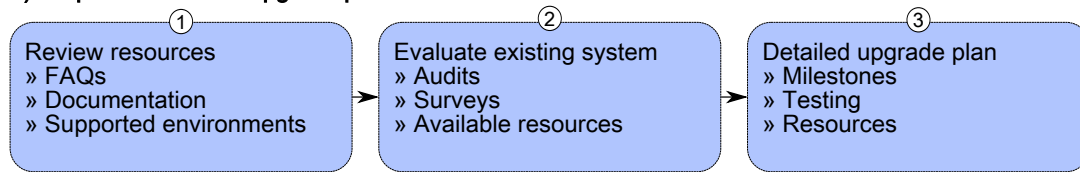
The following diagram shows a general upgrade workflow and the stages in the upgrade process. The process includes the following stages:

- Creating an upgrade plan, which includes the following activities:
  - Reviewing resources, such as the documentation, the [Upgrade Central Website \(www.ibm.com/support/docview.wss?uid=swg22011664\)](http://www.ibm.com/support/docview.wss?uid=swg22011664), and the following upgrade steps: <http://www.ibm.com/support/docview.wss?uid=swg21994915>
  - Verifying the supported environments to ensure compatibility with your other software by going to the [IBM Cognos Analytics on Premises 12.0.x Supported Software Environments \(https://www.ibm.com/support/pages/node/6966712\)](https://www.ibm.com/support/pages/node/6966712). You may also want to check this page if you are thinking of upgrading your operating system.
  - Evaluating your existing system to determine what you want to move to your new version of the product.
  - Creating a detailed plan to implement your upgrade strategy.
- Creating a development or test system with the new version of the product.

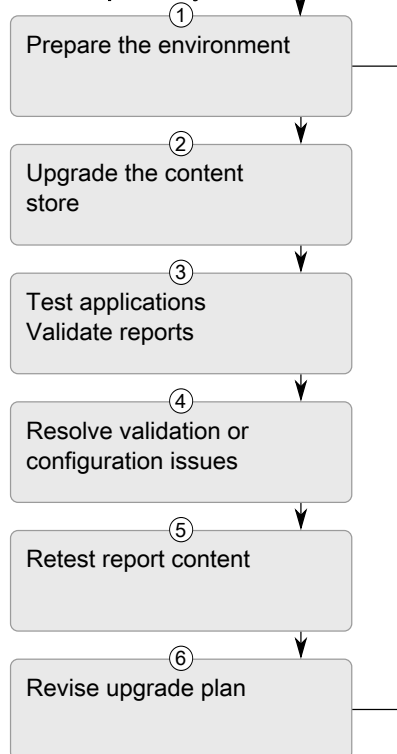


- Using the information learned from the development or test system and applying it as you create your QA or production systems.

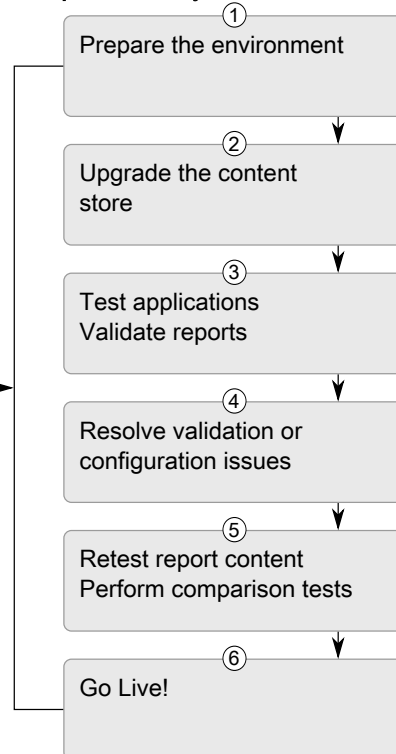
#### A) Prepare: Create an upgrade plan



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



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



Apply lessons learned  
as you create a QA or  
production system

#### D) Leverage: Adopt new features



Figure 4. Upgrade process

## Reviewing the documentation

Documentation is provided to help you achieve a successful upgrade.

All the documentation is available online at [IBM Cognos Knowledge Center](http://www.ibm.com/support/knowledgecenter/SSEP7J_11.2.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html) ([http://www.ibm.com/support/knowledgecenter/SSEP7J\\_11.2.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html](http://www.ibm.com/support/knowledgecenter/SSEP7J_11.2.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html)).

## Assess applications in your environment before you upgrade

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

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

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

An audit of your existing applications can include the following tasks:

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

To review an up-to-date list of environments that are supported by IBM Cognos Analytics products, including information on operating systems, patches, browsers, web servers, directory servers, database servers, and application servers, see [IBM Cognos Analytics on Premises 12.0.x Supported Software Environments](https://www.ibm.com/support/pages/node/6966712) (<https://www.ibm.com/support/pages/node/6966712>).

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

- Configuration settings that you enabled in IBM Cognos Configuration

Installing the new version of the product in a different location than the existing version lets you compare the settings between the two version. To run the two versions you must ensure that you use unique port numbers, web server aliases, and unique content store databases.

- Changes to other configuration files

You must manually change other configuration files during the upgrade. If you changed other configuration files, you must assess the changes that you want to preserve in the upgraded environment. This might include .xml, .txt, and .css files in the configuration, templates, webapps, and webcontent directories.

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

- Back up your content store database.

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

## Guidelines when upgrading your operating system

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

- Check the IBM Cognos Analytics on Premises 12.0.x Supported Software Environments (<https://www.ibm.com/support/pages/node/6966712>) to ensure that the IBM Cognos Analytics version supports the version of the operating system you are thinking of moving to.
- Ensure that the third-party software that is used by IBM Cognos Analytics is supported on the proposed operating system version. Third-party software would include components, such as database and database drivers, application servers, web servers, and browsers.
- Determine whether you must recompile IBM Cognos Analytics SDK applications.
- Determine whether you must re-create web deployments, which include web archive (.war) files and enterprise archive (.ear) files.

## Install and configure a new version of the product

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

Installing to a new location allows you to maintain your existing version of the product and run it in addition to the new version of the product. This can help you test your new version without affecting

your existing version. You can compare the configuration settings between version and compare the appearance and functionality of the reports in both environments to ensure equivalency.

## **Running multiple versions or instances of IBM Cognos Analytics on the same computer**

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

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

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

#### **Ports and URI settings**

If you are using the default application server, you must use different port numbers than 9300 to avoid port conflicts. IBM Cognos Analytics reserves a range of port number, so you must ensure that you use an offset of at least 100 for the port number. For example, if you are using the default port number, 9300, for one instance of IBM Cognos Analytics. For a second installation on the same computer, you must change the port number to at least 9400. Do not use the same port numbers for both installations.

Change the following ports.

- Dispatcher URIs for gateway
- External dispatcher URI
- Internal dispatcher URI
- Dispatcher URI for external applications
- Content Manager URIs
- Local log server port number

If you are installing the product on an application server other than the one provided with IBM Cognos Analytics, ensure that you install the new version to a new application server profile or a separate instance than your existing version.

#### **Content store**

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

#### **Optional web server virtual directories**

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

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

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

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

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

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

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

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

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

## Customized configuration files

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

The IBM Cognos Analytics 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 you upgrade. By replacing the `system.xml` files with files from your earlier version of the product, the files can be upgraded by the new version of the product. The automatic upgrade is applied when you start the IBM Cognos service.

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

- `install_location/templates/ps`
- `install_location/templates/ps/portal`
- `install_location/templates/ps/qs`

## Configuring a second instance of IBM Cognos Analytics on one computer

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

## Before you begin

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

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

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

## Procedure

1. For the new instance of IBM Cognos Analytics, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. Ensure that the port numbers for the following settings do not conflict with your other instance or version of IBM Cognos Analytics:
  - **Dispatcher URIs for gateway**
  - **External dispatcher URI**
  - **Internal dispatcher URI**
  - **Dispatcher URI for external applications**
  - **Content Manager URIs**
4. Ensure that the **Gateway URI** uses a different virtual directory or alias than your other instance or version of IBM Cognos Analytics.

5. Click **Logging**, and ensure that the **Local log server port number** is unique.
6. If you are using Portal Services, update the `applications.xml` file location:
  - In the **Explorer** window, click **Environment > Portal Services**.
  - In the **Properties** window, ensure that the port number for the **Location of applications.xml** property matches the port number for the other URI properties.
7. In the **Explorer** window, under **Data Access > Content Manager**, ensure that you do not use the same content store that is used for your other instance or version of IBM Cognos Analytics.
8. Save the configuration, and start IBM Cognos Analytics.

## Move your content to the new version of the product

There are two methods for moving your content. You can move the entire content store, or you can move content by creating deployment archives.

### Move your entire content store

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

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

When configuring security, ensure that you set the unique identifier to the same value as it was in the release that you are upgrading from, otherwise the security settings will be lost.

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

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

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

### Move content by creating deployment archives

You can move content by creating deployment archives.

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

If you are changing content store database vendors, you must create deployments to move your content. For example, if you are changing your contents store from Microsoft SQL Server to IBM Db2, you must do so with deployment archives.

### Considerations for both methods

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

## Upgrade your content store

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

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

1. Make a backup of your existing content store database.
2. Create a database from the backup.
3. Connect the new version of the product to the content store that you created from the backup in IBM Cognos Configuration.
4. Start your services.

The content store is upgraded during the startup process.

**Tip:** When restarting services manually, (if applicable) the **ApacheDS - cognos** service must be started before the **IBM Cognos** service.

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

Later, you can upgrade your reports with IBM Cognos Administration. Additionally, if you have Software Development Kit applications that create, modify, or save report specifications, do not select the option to upgrade your report specifications.

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

## Unregister previous version dispatchers from your content store

If you use a backup of your existing content store with a new version of the product, you must unregister the dispatchers from your previous version.

### Procedure

1. From **Manage > Administration console**, open IBM Cognos Administration.
2. Click **Configuration**, and then click **Dispatchers and Services**.
3. Click **More** for the dispatchers belonging to your previous version.
4. Click **Unregister**, and then click **OK**.

The dispatcher information is removed from the content store.

## Moving your content with a deployment archive

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

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

Moving your content with deployment archives involves the following steps:



1. Creating the archive.
2. Copying the archive to the new version of the product.
3. Importing the content.

## Creating a deployment archive

Use the following task to create a deployment archive.

### Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Content Administration**.
2. On the toolbar, click the **New Export** icon .

3. Enter **Name** for the archive.
4. Select the content you want to include in the archive:
  - To export specific folders and directory content, click **Select public folders and directory content**.
  - To export the entire content store, click **Select the entire content store**. If you select the entire content store, you can also select **Include user account information**.
5. Click **Next**.
6. If you clicked **Select the entire content store**, enter a password to be used when you import the content, and then click **OK**.
7. If you clicked **Select public folders and directory content**:
  - a) On the **Select the Public folders content** panel, click **Add**.
  - b) On the **Select entries** panel, in the **Available Entries** box, select the packages or folders that you want to export.  
 You can browse the Public Folders hierarchy and choose the packages and folders that you want.  
 Click the **Add** icon  to move the selected items to the **Selected entries** box, and click **OK**.
  - c) For each package and folder that you export, do the following, and then click **Next**:
    - If you want to make any changes to the package or folder in the target environment, click the **Edit** icon , make your changes, and click **OK**.
    - To restrict access to the package or folder and its entries, select the check box in the **Disable after import** column. This is useful when you want to test the reports before you make them available in the target environment.
    - Under **Options**, select whether you want to include the report output versions, run history, and schedules and what to do with entries when there is a conflict.
  - d) On the **Select the directory content** panel, select the options that you want, and click **Next**.
  - e) On the **Specify the general options** panel, select the options that you want, and click **Next**.
  - f) On the **Specify a deployment archive** panel, select an existing deployment archive from the list, or create one.  
 If you are typing a new name for the deployment archive, do not use spaces in the name. If the name of the new deployment specification matches the name of an existing deployment archive, the existing deployment archive is overwritten.
8. Review the summary information and click **Next**.
9. Under **Actions**, select **Save and run once**.
10. On the **Run with options** panel, select **Now** and click **Run**.

## Results

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

## Copying the deployment archive to your new version

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

## Procedure

Copy the deployment archives you created from the *old\_version\_install\_location/deployment* directory to the *new\_version\_install\_location/deployment* directory.

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

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

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

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

### Procedure

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

## Importing a deployment archive

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

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

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

**Note:** To deploy reports or dashboards that reference custom palettes, you must be a member of one of these Cognos roles: Report Administrators, Server Administrators, PowerPlay Administrators, or Directory Administrators.

### Before you begin

Ensure that you have copied the deployment archive to the *install\_location/deployment* directory for your new version of the product.

**Important:** If you try to import any reports or other objects with a description of more than 1024 characters, you will see an error message such as the following:


```
CM-REQ-4192 The property "description" (for an object of class "Report")
is incorrect. CM-REQ-4217 The value length XXXX is longer than the maximum
allowable length of 1024 for the property "description."
```


We recommend that you do not increase the description length to more than 1024 characters. Otherwise, the column size may be exceeded in some databases.



For more information, see [defaultDescription](#).

## Procedure

1. For your new version of the product, in **IBM Cognos Administration**, on the **Configuration** tab, click **Content Administration**.
2. On the toolbar, click the new import icon. 
3. In the **Deployment archive** box, select the deployment archive that you want to import, and click **Next**.
4. If your deployment archive is of your entire content store, type the password entered during the export, and click **OK**.
5. Type a name for the import and select the folder where you want to save it, and then click **Next**.
6. Select the content that you want to include in the import, select the options, and click **Next**.

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

7. On the **Specify the general options** panel, select the options that you want, and click **Next**.
8. Review the summary information, and click **Next**.
9. Under **Actions**, select **Save and run once**, and click **Finish**.
10. On the **Run with options** panel, do the following:
  - a) Select **Upgrade all report specifications to the latest version** if you want to upgrade the report specifications during the import. You can also perform this task after you import the content.
  - b) Click **Run**.

## Upgrade your report specifications

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

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


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

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

### Before you begin

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

## Procedure

1. Open **IBM Cognos Administration**.
2. On the **Configuration** tab, click **Content Administration**.
3. Click the arrow on the new content maintenance button  on the toolbar, and then click **New Report Upgrade**

4. Type a name for the upgrade task and, if you want, a description and screen tip. Click **Next**.
5. Select the packages and locations for the report specification you want to upgrade. Click **Next**.

If you upgrade report specifications by package, all reports in the content store that are based on the model in the package will be upgraded. If you upgrade report specifications by folder, all reports in the folder will be upgraded.

6. Choose one of the following:

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

---

## Chapter 9. Configuring server components

You can install all IBM Cognos Analytics components on one computer, on multiple servers for a distributed installation, or you can expand an existing single computer installation to another server to improve performance.

The following options are available when installing IBM Cognos Analytics from the installation wizard.

- Use the **Easy Install** option to help you get up and running with IBM Cognos Analytics in no time, without any additional configuration and without the need to install any supporting software.

**Important: Easy Install** is available for Windows OS only. If you are upgrading an **Easy Install** (that is, installing over the top of an existing installation), shut down all services manually first, including Informix and Custom Java Authentication Provider (CJAP) services.

With this install option, you get the following with all the configuration already in place:

- A full version of IBM Cognos Analytics software with all the new capabilities.
- Informix 12.10 installed and configured for use as content store database.
- Custom Java Authentication Provider (CJAP) to create and manage users.
- Use the **Custom** option for full flexibility to pick and choose the IBM Cognos Analytics components that you want to install. Maybe you want to customize or integrate IBM Cognos Analytics with third-party software? This is the option you would want to select.

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

When performing a custom install, the server components are collected into the following tiers:

- [Content repository](#) (Content Manager)
- [Application services](#)
- [Gateway tier](#)

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

### Stopping services sequence

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

It is important to also stop the following:

- Applications that are related to the IBM Cognos service, such as Framework Manager, Cognos Transformer, or IBM Cognos Administration.
- Any Software Development Kit applications that are running.

### Upgrading your installation

If you are upgrading from a previous release of IBM Cognos products, see [Chapter 8, “Upgrading Cognos Analytics,”](#) on page 73.

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

## 64-bit installations

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

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

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

## Windows installations

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

## UNIX installations

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

Also, IBM Cognos Analytics uses 755 permissions. This affects only the installation directories. It does not affect the file permissions within the directories.

## 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.

## Uninstallation

For uninstallation instructions, see [Chapter 16, “Uninstalling IBM Cognos Analytics,” on page 291](#).

## 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.

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.

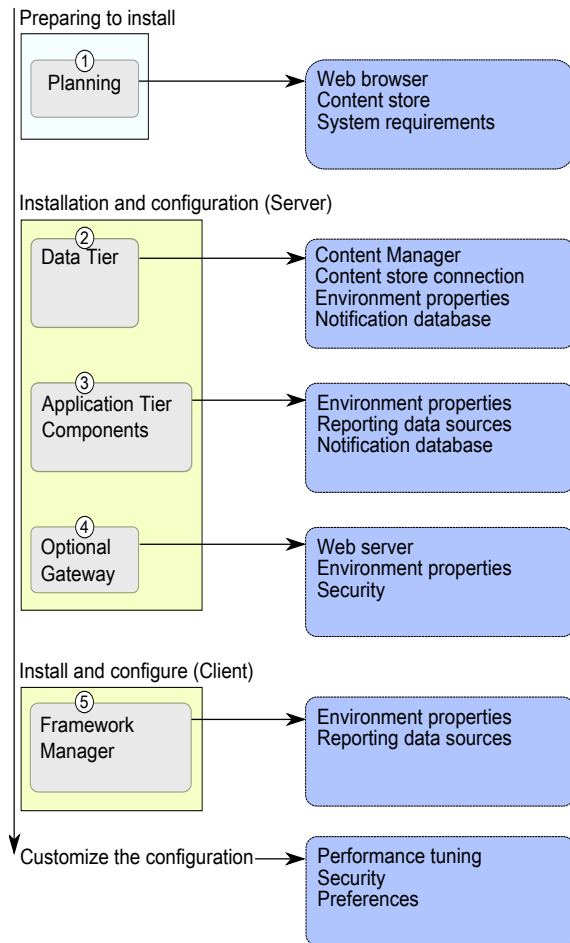


Figure 5. Distributed installation process workflow

## 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 Analytics 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: data tier (Content Manager), application tier components, and gateway tier. Perform only the required configuration tasks, such as configuring distributed components to communicate with each other, to get your distributed environment running before you customize your settings.

Later, you can add optional components and customize your configuration settings to better suit your business intelligence needs.

The sequence in which you configure computers is important. You must configure and then start the services on at least one computer where you installed Content Manager before you configure other server components or Framework Manager. For more information, see [“Installation sequence for server components”](#) on page 92.

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

## Installation modes

---

For a complete installation, you must install components on your server and then configure them to work in your environment.

### Interactive mode

Typically, you run the IBM Cognos installation and configuration programs in interactive mode. This means that the install wizard prompts you to provide information, and the configuration tool enables you to change default settings. The install wizard is `ca_srv_<platform>_<build>.exe` (Windows), or `ca_srv_<platform>_<build>.bin` (UNIX, Linux).

### Silent mode

You can automate the installation of components using response files and running the installation program in silent mode.

You can automate the configuration of components by exporting the configuration settings from one computer to another as long as the installed components are the same. Run IBM Cognos Configuration in interactive mode the first time.

The other option is to edit the `cogstartup.xml` file, using settings that apply to your environment, and then running the configuration tool in silent mode.

### Interactive mode on UNIX systems

Unless you intend to complete a silent-mode installation, install the software from an X Window System workstation, an X terminal, or a PC or other system with X server software installed.

To run an interactive-mode installation, the console attached to your computer must support a Java-based graphical user interface.

## Installing server components on UNIX or Linux operating systems

---

Use the installation wizard to select the server components that you want to install, and the location on your computer where you want to install them.

### Before you begin

Go to the [IBM Cognos Analytics on Premises 12.0.x Supported Software Environments](https://www.ibm.com/support/pages/node/6966712) (<https://www.ibm.com/support/pages/node/6966712>) to verify that the required patches are installed on your computer.

### Procedure

1. Set the `JAVA_HOME` environment variable to point to the installation location of your Java Runtime Environment (JRE), such as `/directory/java/java_version/jre`.

IBM Cognos Analytics requires a JVM, such as the one that is provided by IBM, to run on Linux operating system.

2. Go to the location where the installation files were downloaded and extracted.

**Tip:** Use new versions of file compression software to extract the files. Older versions of such software might not extract the files.

3. To start the installation wizard, go to the operating system directory, and type the following command:

```
./ca_instl_<platform>_<build>.bin
```

Where *<build>* is the build number, and *<platform>* is win (Windows), i386 (Linux i386), ppcle (Linux ppcle), ppc (Linux Power PC), s390x (Linux z), aix (AIX), and zos (z/OS).

**Tip:** When you use the `./ca_instl_<platform>_<build>.bin` command with XWindows, Japanese characters in messages and log files might 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), and then start the installation wizard.

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

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

Install to 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.

5. In the **Finish** page of the installation wizard, you can click **View** to access the log files. Do not configure IBM Cognos Analytics immediately because you must do other tasks first to ensure that your environment is properly set up.

## What to do next

You can configure IBM Cognos Analytics by using IBM Cognos Configuration. Type `cogconfig.sh` in the `install_location/bin64` directory to start Cognos Configuration.

## Installing server components on Windows operating systems

Use the installation wizard to select the server components that you want to install, and the location on your computer where you want to install them.

For Windows computers, the default installation location uses the **Program Files** directory. If you install to this location, ensure that you run IBM Cognos Configuration as an administrator. Alternatively, you can install the product to a directory outside of **Program Files**, such as `C:\IBM\cognos\analytics`.

The installation requires at least 5 GB in the temporary directory. The temporary directory is set with the environment variable `TMP`.

## Procedure

1. Go to the location where the installation files were downloaded and extracted, and double-click `ca_srv_<platform>_<build>.exe`.

**Tip:** Use new versions of file compression software to extract the files. Older versions of such software might not extract the files.

2. 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.

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

You can use one of the following installation options:

- Use the **Easy Install** option to install components to a single computer, install an instance of Informix database for the content store, and configure the system.

**Important:** If you are upgrading (that is, installing over the top of an existing installation) an **Easy Install**, manually shut down all services first, including Informix and ApacheDS services.

- Use the **Custom** option for a distributed installation to install components on multiple servers.

Install IBM Cognos Analytics 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.

## Installing and configuring Content Manager for the content repository

---

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

### Rules for configuring

In an installation where you have more than one Content Manager components, or where Content Manager is located in a separate location, at least one of the one Content Manager must be configured, running and accessible before you configure other components in your environment. This ensures that the certificate authority service, which is installed with Content Manager, is available to issue certificates to other IBM Cognos computers.

For information about the sequence of the installation process for distributed components, see [“Installation sequence for server components” on page 92](#).

### 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” on page 97](#).

In installations with multiple Content Managers, configure IBM Cognos Analytics to use compiled gateways instead of the default CGI gateway. For example, use Apache Module for Apache Server or for IBM HTTP Server, or use ISAPI for IIS. Otherwise, performance may be affected after failover.



## Upgrading

If you are upgrading from ReportNet or an earlier version of IBM Cognos Business Intelligence, you can use the existing configuration data. However, some features in IBM Cognos Analytics are new and may require configuration.

## PowerCubes

If you plan to install IBM Cognos Transformer and you will be using PowerCubes that are secured against an IBM Cognos Series 7 namespace, you must install Content Manager on a computer that supports IBM Cognos Series 7.

## Active and Standby Content Manager Components

You can install any number of installations of Content Manager, although only one is active at any time. The other installations each act as a standby Content Manager.

The standby Content Manager components are for failover protection. If the active Content Manager is not available because of a software or hardware failure, a standby Content Manager becomes active and requests are directed to it.

When the active Content Manager fails, unsaved session data is lost. When another Content Manager becomes active, users may be prompted to log on.

By default, the first Content Manager installed with IBM Cognos Analytics is the active one. An IBM Cognos Analytics server administrator can change the default Content Manager and the active Content Manager at any time. When IBM Cognos Analytics 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.

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.

## Installing Content Manager on UNIX or Linux operating systems

Use the following procedure to install Content Manager on a UNIX or Linux operating system.

### Before you begin

Go to the [IBM Cognos Analytics on Premises 12.0.x Supported Software Environments](https://www.ibm.com/support/pages/node/6966712) (<https://www.ibm.com/support/pages/node/6966712>) to verify that the required patches are installed on your computer.

### Procedure

1. Set the JAVA\_HOME environment variable to point to the installation location of your Java Runtime Environment (JRE), such as `/directory/java/java_version/jre`.

IBM Cognos Analytics requires a JVM, such as the one that is provided by IBM, to run on Linux operating system.

2. Go to the location where the installation files were downloaded and extracted.

**Tip:** Use new versions of file compression software to extract the files. Older versions of such software might not extract the files.

3. To start the installation wizard, go to the operating system directory, and type `./ca_srv_<platform>_<build>.bin`

**Tip:** When you use the `ca_srv_<platform>_<build>.bin` 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), and then start the installation wizard.

If you do not use XWindows, run an unattended installation. For more information, see [Chapter 5, “Silent installation, uninstallation, and configuration,”](#) on page 37.

4. Follow the directions in the installation wizard to copy the files to your computer and implement a basic configuration.

- 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 Analytics on a computer that has an earlier version of IBM Cognos Analytics and you want to keep the earlier version, you must install the new version in a different directory.

- When selecting components, clear all components except for **Content repository**.

5. Click **Finish**.

## What to do next

Do not configure IBM Cognos Analytics immediately because you must do other tasks first to ensure that your environment is properly set up.

You can later configure IBM Cognos Analytics using IBM Cognos Configuration by typing `cogconfig.sh` in the `install_location/bin64` directory.

## Installing Content Manager on Windows operating systems

Use the following procedure to install Content Manager on a Microsoft Windows operating system.

For Windows computers, the default installation location uses the **Program Files** directory. If you install to this location, ensure that you run IBM Cognos Configuration as an administrator. Alternatively, you can install the product to a directory outside of **Program Files**, such as `C:\IBM\cognos\analytics`.

The installation requires at least 5 GB in the temporary directory. The temporary directory is set with the environment variable `TMP`.

## Before you begin

Go to the [IBM Cognos Analytics on Premises 12.0.x Supported Software Environments](https://www.ibm.com/support/pages/node/6966712) (<https://www.ibm.com/support/pages/node/6966712>) to verify that the required patches are installed on your computer.

## Procedure

1. Go to the location where the installation files were downloaded and extracted, and double-click `ca_srv_<platform>_<build>.exe`.

**Tip:** Use new versions of file compression software to extract the files. Older versions of such software might not extract the files.

2. 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.

3. Select the **Custom** installation option, and follow the directions in the installation wizard to copy the files to your computer.

- When selecting the directory, consider the following:

Install Content Manager in a directory that contains only ASCII characters in the path name. Some Microsoft Windows operating system Web servers do not support non-ASCII characters in directory names.

If you are installing IBM Cognos Analytics on a computer that has an earlier version of IBM Cognos Analytics and you want to keep the earlier version, you must install IBM Cognos Analytics in a different directory.

- When selecting components, clear all components except **Content repository** from the **Custom** install option.

4. Click **Finish**.

## What to do next

If you start IBM Cognos Configuration from the installation wizard, ensure that you follow the additional tasks in this section to ensure that your environment is properly set up before you start the services.

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

## Set up database connectivity for the content store database

You may have to install database client software, or Java Database Connectivity (JDBC) drivers, or both, on each computer where you install Content Manager. Doing this allows Content Manager to access the content store database.

### Set up database connectivity for a Microsoft SQL Server content store

You must download, from the Microsoft website, a driver that is supported for your Cognos Analytics release and copy it to the *install\_location/drivers* folder.

For a list of drivers that were tested with your Cognos Analytics release, see [DQM testing of vendor-supported client driver versions for each Cognos Analytics 12.0.x release](https://www.ibm.com/support/pages/node/6989513) (<https://www.ibm.com/support/pages/node/6989513>).

**Important:** For single sign-on (SSO) and Windows authentication, you need to put `sqljdbc_auth.dll` in the `bin64` directory. Windows authentication is a single sign-on setup. The selection in Configuration Manager for the Content Manager is called **Microsoft SQL Server database (Windows Authentication)**.

### Set up database connectivity for an IBM Db2 content store

This procedure describes how to set up database connectivity for a Db2 content store. You must perform this procedure on each computer where you install Content Manager.

You must use a type 4 Java Database Connectivity (JDBC) driver to connect to your content store.

The type 4 driver is considered an independent product. It does not require the Db2 client to be installed.

## Procedure

Copy the following files from *DB2\_installation\sqllib\java* directory to the *install\_location/drivers* directory:

- The universal driver file, `db2jcc4.jar`
- The license file:

For Db2 on Linux, UNIX, or Windows operating systems, use `db2jcc_license_cu.jar`.

For Db2 on z/OS, use `db2jcc_license_cisuz.jar`.

If you are connecting to Db2 on z/OS, use the driver version from Linux, UNIX, or Windows version 9.1 fix pack 5 or version 9.5 fix pack 2.

**Tip:** To check the driver version, run the following command:

```
java -cp path\db2jcc4.jar com.ibm.db2.jcc.DB2Jcc -version
```

### ***Generating a script file to create a database for an IBM Db2 content store***

You can generate a script file to automatically create the content store in Db2 on all platforms. The script file is a DDL file.

### **Procedure**

1. Start **IBM Cognos Configuration**.
2. In the **Explorer** window, under **Data Access > Content Manager**, click **Content Store**.  
The default configuration is for an Db2 database. Ensure that the **Type** is **DB2 database**.
3. In the **Database server and port number** field, enter the name of your computer and port number on which Db2 is running.  
For example, localhost:50000. Where, 50000 is the default port number that is used by Db2. If you are using a different port number, ensure you use that value.
4. Click the **Value** field next to the **User ID and password** property and then click the edit icon. Type the appropriate values and click **OK**.
5. In the **Properties** window, for the **Database name** property, type the name for your content store database.  
**Important:** Do not use a name longer than eight characters and use only letters, numbers, underscores, and hyphens in the name.
6. Right-click **Content Store**, and click **Generate DDL**.
7. Click **Details** to record the location of the generated DDL file.

The DDL file named createDB.sql is created. The script is created in the `install_location\configuration\schemas\content\db2` directory.

### **What to do next**

Use this script to create a database in Db2. For more information about using a DDL file, see your Db2 documentation.

If you use the Db2 command-line interface, you can run the script by entering the following command:

```
db2 -tvf createDB.sql
```

### ***Creating tablespaces for a content store on IBM Db2 for z/OS***

A database administrator must run scripts to create a set of tablespaces required for the content store database. Modify the scripts to replace the placeholder parameters with ones that are appropriate for your environment. By default, the content store is used for notifications, human tasks, and annotations. You can create separate databases for each.

### **About this task**

Ensure that you use the naming conventions for Db2 on z/OS. For example, all names of parameters must start with a letter and the length must not exceed eight characters. There are two exceptions to the character length limit:

- CMScript\_CS\_ID is no more than 2 characters.
- CMScript\_TABLESPACE is no more than 6 characters.

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

For more information, see the [IBM Db2 for z/OS Knowledge Center](http://www.ibm.com/support/knowledgecenter/SSEPEK/db2z_prodhome.html) ([http://www.ibm.com/support/knowledgecenter/SSEPEK/db2z\\_prodhome.html](http://www.ibm.com/support/knowledgecenter/SSEPEK/db2z_prodhome.html)).

## Procedure

1. Connect to the database as a user that has privileges to create and drop tablespaces and to allow execution of SQL statements.
2. Go to the directory that contains the scripts:  
`install_location/configuration/schemas/content/db2z0S`
3. Make a backup copy of the `tablespace_db2z0S.sql` script file and save the file to another location.
4. Open the original `tablespace_db2z0S.sql` script file.
  - a) Add a connection statement to the beginning of the script.

For example,

```
connect to databasename;
```

- b) Use the following table to help you to replace the generic parameters with ones appropriate for your environment.

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

| Table 12. Parameter names and description for the content store tablespace script |                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter name                                                                    | Description                                                                                                                                                                                                                                         |
| <b>CMSCRIPT_STOGROUP</b>                                                          | Specifies the name of the storage group.                                                                                                                                                                                                            |
| <b>CMSCRIPT_DATABASE</b>                                                          | Specifies the name of the content store database.                                                                                                                                                                                                   |
| <b>CMSCRIPT_CS_ID</b>                                                             | Specifies the subsystem identification for the content store database.<br><br>The ID must not be longer than 2 characters.                                                                                                                          |
| <b>CMSCRIPT_TABLESPACE</b>                                                        | Specifies the name of the tablespace that contains all of the base tables in the content store.<br><br>Auxiliary tables are not included.<br><br>The name cannot be longer than 6 characters.                                                       |
| <b>CMSCRIPT_LARGE_BP</b>                                                          | Specifies the name of the large buffer pool allocated for especially large objects.<br><br>This bufferpool is the 32 KB buffer pool that was created when the database administrator created the content store database on the z/OS system.         |
| <b>CMSCRIPT_REGULAR_BP</b>                                                        | Specifies the name of the regular size buffer pool allocated for regular and large objects.<br><br>This bufferpool is the 16 KB buffer pool that was created when the database administrator created the content store database on the z/OS system. |

| Table 12. Parameter names and description for the content store tablespace script (continued) |                                                                      |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| Parameter name                                                                                | Description                                                          |
| <b>CMScript_USERNAME</b>                                                                      | Specifies the user account that accesses the content store database. |

5. Save and run the script.

For example, if you set up your `clp.properties` file and your Db2 alias in your profile or `tcshrc` script file, type the following command to run the script:

```
db2 -tvf tablespace_db2z0S.sql
```

6. Grant the IBM Cognos user rights to the tablespaces that were created when you ran the `tablespace_db2z0S.sql` file script:
  - a) Make a copy of the `rightsGrant_db2z0S.sql` script file and store it in another location.
  - b) In the remote access tool, open the original `rightsGrant_db2z0S.sql` script file and replace the placeholder parameters with values that are appropriate for your environment.  
 Ensure that you use the same values that you used when you allocated resources to the buffer pools and user account  
 .

- c) Add a connection statement to the beginning of the script.

For example,

```
connect to databasename user username using password;
```

- d) Save and then run the script.

For example,

```
db2 -tvf rightsGrant_db2z0S.sql
```

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

| Table 13. Tablespace parameter names and descriptions for the Db2 notification database on z/OS |                                                  |
|-------------------------------------------------------------------------------------------------|--------------------------------------------------|
| Parameter Name                                                                                  | Description                                      |
| NCCOG                                                                                           | Specifies the name of the notification database. |
| DSN8G810                                                                                        | Specifies the name of the storage group.         |
| BP32K                                                                                           | Specifies the name of the buffer pool.           |

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

- c) Save and run the script.

For example,

```
db2 -tvf NC_TABLESPACES.sql
```

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

e) Save the script.

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

## Set up database connectivity for an Oracle content store

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

### Procedure

1. On the computer where the Oracle client is installed, go to the *ORACLE\_HOME*/jdbc/lib directory.
2. Copy the correct library file for your version of the Oracle client to the *install\_location*\drivers directory on the computer where Content Manager is installed and where notification is sent to an Oracle database.

If you are using Oracle version 12c Release 2, you must have the *ojdbc8.jar*.

If you are using Oracle version 12c Release 1, you must have the *ojdbc7.jar*.

If you are using Oracle version 11g Release 2, you must have the *ojdbc6.jar*.

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

## Creating a content store using an Oracle database with Kerberos security

You can create an Oracle content store that uses Kerberos authentication.

### About this task

To create a content store that uses an Oracle database with Kerberos security, you must configure Cognos Analytics to use the Oracle JRE instead of the IBM JRE. The IBM JRE is not compatible with Oracle when it uses Kerberos authentication.

#### Tips:

To debug Kerberos, you can make one or both of these changes:

- Edit the file *Cognos\_Analytics\_installation\_location*/wlp/usr/servers/cognosserver/bootstrap.properties and add this line:

```
sun.security.krb5.debug=true
```

- Edit the JAAS login configuration file and add this line to the entry that is used for creating a content store:

```
debug=true
```

In both cases, debugging messages will appear in the file *Cognos\_Analytics\_installation\_location*/logs/cognosserver.log.

### Procedure

1. Install the Oracle JRE.
  - a) Check the [Supported environments page](https://www.ibm.com/support/pages/node/735235) (<https://www.ibm.com/support/pages/node/735235>) to see which versions of Oracle JRE are supported by your version of Cognos Analytics.
  - b) Install a supported version of Oracle JRE.

For more information, see the [Oracle JRE Download page](https://java.com/en/download/) (<https://java.com/en/download/>).

2. Set the following environment variables to point to the Oracle JRE that you installed:

```
set JAVA_HOME=Oracle_JRE_installation_location
set path=%JAVA_HOME%\bin;%path%
```

3. Configure Cognos Analytics to use the Oracle JRE version that you just installed.

For more information, see [“Changing the version of Java used by IBM Cognos Analytics components” on page 168](#).

4. Ask your Kerberos administrator to give you the `krb5.conf` and `.keytab` files.
5. Add the `krb5.conf` file to the `JRE_installation_location/lib/security` folder.
6. If you plan to use credential caching, create ticket cache files from the `.keytab` files.

For example, follow these steps:

- a) Navigate to the `JRE_installation_location/bin` directory.
- b) Run this command:

```
klist -k -t -K -e absolute_path_to_keytab_file
```

**Tip:** Note the value of *principal*.

- c) Run this command:

```
kinit -c cache_file -k -t absolute_path_to_keytab_file principal
```

7. Create a JAAS login configuration file called, for example, `jaas.conf`.

**Tip:** See the sample file, `installation_location/configuration/jaas-oracle.config.sample`

8. Define an entry in the `jaas.conf` file as shown in these example entries:

Example entry for credential cache:

```
com.cognos.biserver.security.cm
{
    com.sun.security.auth.module.Krb5LoginModule required
    debug=true
    useTicketCache=true
    ticketCache="absolute_path_to_ticket_cache_file"
    renewTGT=true
    doNotPrompt=true
    principal="service_principal_value";
};
```

Example entry for key tab:

```
com.cognos.biserver.security.cm
{
    com.sun.security.auth.module.Krb5LoginModule required
    debug=true
    doNotPrompt=true
    useKeyTab=true
    refreshKrb5Config=true
    keyTab="absolute_path_to_keytab_file"
    principal="service_principal_value";
};
```

Example entry for both the credential cache and the key tab:

**Note:**

In the following example entry, the ticket cache is checked first. If a ticket-granting ticket (TGT) cannot be found, then the keytab is used to log on. However, if the TGT is found but is expired, the system will throw an exception, instead of using the keytab.

```
com.cognos.biserver.security.cm
{
    com.sun.security.auth.module.Krb5LoginModule required
    debug=true
    useTicketCache=true
```



```

ticketCache="absolute_path_to_ticket_cache_file"
renewTGT=true
doNotPrompt=true
useKeyTab=true
refreshKrb5Config=true
keyTab="absolute_path_to_keytab_file"
principal="service_principal_value";
};

```

9. Add the following line to the file *installation\_location/wlp/usr/servers/cognosserver/bootstrap.properties*:

```
java.security.auth.login.config="absolute_path_to_jaas.conf"
```

10. Add the following line to the file *JRE\_installation\_location/lib/security/java.security*:


```
login.config.url.n=file:absolute_path_to_jaas.conf
```

where *n* is a sequence, starting at 1.

11. Copy the Oracle JDBC Thin driver, for example *ojdbc8.jar*, to the *installation\_location/drivers* directory.
12. Start Cognos Configuration and create an Oracle content store that uses Kerberos authentication.

**Tip:** When you configure a new content store in Cognos Configuration, the default name is `com.cognos.biserver.security.cm`. However, you can change this name if you want.

For more information, see [“Configure JDBC data source connections for single sign-on using Kerberos”](#) on page 214.

13. When you start the IBM Cognos service, if "Connection failure" error messages appear in Cognos Configuration, try adjusting the settings that control connection attempts:
  - a) In Cognos Configuration, select **Data Access > Content Manager > Content Store**.
  - b) Click in the **Advanced properties** field and then click the pencil icon .
  - c) Add the following Name-Value pair:
 

**Name:** `max.connection.attempts`

**Value:** 15
  - d) Add the following Name-Value pair:
 

**Name:** `seconds.between.retries`

**Value:** 2
  - e) Save the configuration and start the IBM Cognos service.
  - f) When the service starts, if connection error messages still appear, adjust the parameter values that you set in steps **c** and **d**, then again save the configuration.
14. If the error message `java.sql.SQLException: Oracle Error ORA-12631` appears, follow these steps:
  - a) Open the file `krb5.conf` in a text editor.
  - b) Remove the line `forwardable=true`.
  - c) Save the file.

## Set up database connectivity for an Informix content store

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

### Procedure

1. On the computer where Informix is installed, go to the *Informix\_location/sqlllib/java* directory.
2. Copy the following files to the *install\_location\drivers* directory on every computer where Content Manager is installed.
  - the universal driver file, *db2jcc4.jar*
  - the license file, *db2jcc4\_license\_cisuz.jar*

## Start IBM Cognos Configuration

Use IBM Cognos Configuration to configure IBM Cognos Analytics components and to start and stop IBM Cognos services.

### Before you begin

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

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

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

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

Read [“Critical configuration actions to take first!”](#) on page 167.

### Procedure

1. On Microsoft Windows, click **Start > IBM Cognos Configuration**.

If you are using a Windows computer, and have installed the product to the Program Files (x86) directory, start IBM Cognos Configuration as an Administrator.
2. On UNIX or Linux operating systems, go to the *install\_location/bin64* directory and then type the following command:

```
./cogconfig.sh
```

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

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

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

## Set Database Connection Properties for the Content Store

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

store. After you set the database connection properties, you can test the connection between Content Manager and the content store.

## Content store configuration after an upgrade

If you are upgrading from IBM Cognos Business Intelligence or an earlier release of IBM Cognos Analytics, configure IBM Cognos Analytics 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 IBM Cognos Analytics or the earlier version running with the original data.

## Advanced properties

In Cognos Configuration, you can associate a database resource with each of the following services:

- Content Manager
- Mobile
- Notification
- Logging

Cognos Configuration provides connection editors for each of the supported databases. At runtime, services use the information entered in the connection editors to connect to the database using the vendor's JDBC driver. Each connection editor has an **Advanced properties** box in which you can specify vendor-specific name-value pairs that are supported by the JDBC driver.

The configuration requirements of the database system that you use determine whether you must enter any name-value pairs in the **Advanced properties** box.

For information about the description and purpose of name-value pairs supported by a database, see the JDBC driver documentation of the applicable database vendor.

## Examples

Following are two examples of name-value pairs entered in the **Advanced properties** box:

### Example 1

A SQL Server JDBC driver requires a connection that includes this name-value pair:

```
trustServerCertificate true
```

### Example 2

An ORACLE JDBC driver requires a connection that includes multiple name-value pairs:

```
oracle.net.ssl_server_dn_match true
javax.net.ssl.trustStorePassword mysecret
javax.net.ssl.trustStore C:/myfolder/truststore.jks
javax.net.ssl.keyStore C:/myfolder/keystore.jks
javax.net.ssl.keyStorePassword mysecret
```

## Setting database connection properties for a IBM Db2 content store

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

## Procedure

1. In the location where you installed Content Manager, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Data Access, Content Manager**, click **Content Store**.

3. In the **Properties** window, for the **Database name** property, type the name of the database or the database alias.
4. Change the logon credentials to specify a valid user ID and password:
  - Click the **Value** box next to the **User ID and password** property and then click the edit button when it appears.
  - Type the appropriate values and click **OK**.
5. In the **Database server and port number** field, enter the name of your computer and port number on which Db2 is running. For example, `localhost:50000`. 50000 is the default port number used by Db2. If you are using a different port number, ensure you use that value.
6. From the **File** menu, click **Save**.
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.

## Setting database connection properties for a content store on IBM Db2 for z/OS

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

### Procedure

1. In the location where you installed Content Manager, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Data Access > Content Manager**, click **Content Store**.
3. In the **Properties** window, for the **Database name** property, type the name of the database or the database alias.
4. Change the logon credentials to specify a valid user ID and password:
  - Click the **Value** box next to the **User ID and password** property and then click the edit icon 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. For the **Database server and port number** property, type the database information as `hostname:port`.
6. In the **Explorer** window, click **Local Configuration**.
7. Click inside the **Value** box for **Advanced properties**, and then click the edit icon.

The **Value - Advanced properties** dialog box appears.

8. Click **Add** to add the parameters for the database connection.

The values in the table are examples, ensure that you enter the correct values for your environment.

| Table 14. Content store connection parameters for Db2 for z/OS |               |
|----------------------------------------------------------------|---------------|
| Parameter name                                                 | Example value |
| CMSCRIPT_CREATE_IN                                             | COGUCS.T1TSCS |
| CMSCRIPT_STOGROUP                                              | DBOIUSR       |
| CMSCRIPT_DATABASE                                              | COGUCS        |
| CMSCRIPT_CS_ID                                                 | T1            |
| CMSCRIPT_TABLESPACE                                            | TSCS          |

| Table 14. Content store connection parameters for Db2 for z/OS (continued) |               |
|----------------------------------------------------------------------------|---------------|
| Parameter name                                                             | Example value |
| CMSCRIPT_LARGE_BP                                                          | BP32K         |
| CMSCRIPT_REGULAR_BP                                                        | BP16K0        |

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

## Setting database connection properties for a Microsoft SQL Server, Oracle, Informix 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.

### Before you begin

If you are using Oracle wallets for mutual TLS, copy the corresponding .jar files into the *install\_location/drivers* directory before you start the configuration tool. You must also make sure that the *install\_location/drivers* directory has all the optional .jar files that Oracle requires when using wallets. For more information on the required files, see the [Oracle JDBC documentation \(https://docs.oracle.com/en/cloud/paas/autonomous-database/adbsa/connect-jdbc-thin-wallet.html#GUID-1640CC02-BF3E-48C2-8FFE-A596614A6A40\)](https://docs.oracle.com/en/cloud/paas/autonomous-database/adbsa/connect-jdbc-thin-wallet.html#GUID-1640CC02-BF3E-48C2-8FFE-A596614A6A40).

### Procedure

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 step deletes the connection to the default resource. Content Manager can access only one content store.

3. Right-click **Content Manager**, and then click **New resource, Database**.
4. In the **Name** box, type a name for the resource.
5. In the **Type** box, select the type of database and click **OK**.

**Tip:** If you want to use an Oracle PDB, Oracle RAC functionality, or Oracle wallets for mutual TLS, select **Oracle database (Advanced)**.

6. In the **Properties** window, provide the values for your database type:
  - If you use a Microsoft SQL Server database, type the appropriate values for the **Database server with port number or instance name** and **Database name** properties.

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

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

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

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

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

- If you use an Oracle database, type the appropriate values for the **Database server and port number** and **SID** properties.
- If you use an Oracle PDB, for the **Database specifier** property, type `//<server>/<servicename>`. For example, `//corpserv1:1522/PDB1`
- If you use an advanced Oracle Net 8 database, for the **Database specifier** property, type the Oracle Net8 keyword-value pair for the connection.

Here is an Oracle Net8 keyword-value pair example:

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

When you select the advanced Oracle database, IBM Cognos Analytics 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 are using Oracle wallets for mutual TLS, for the **Database specifier** property, add the parameters as keyword-value pairs.

The following example includes the TNS\_ADMIN parameter:

```
dbhostA1000?TNS_ADMIN=D:/temp/Wallet_DBA1000
```

- If you use an Informix database, type the appropriate values for the **Database server and port number** and **Database name** properties.
7. To configure logon credentials, specify a user ID and password:
    - Click the **Value** box next to the **User ID and password** property and then click the edit icon when it appears.
    - Type the appropriate values and click **OK**.
  8. If you host more than one content store database on an Informix instance, create the advanced property CMSCRIPT\_CS\_ID and specify the account under which the instance runs:
    - In the **Explorer** window, click **Local Configuration**.
    - In the **Properties** window, click the **Value** column for **Advanced properties** and then click the edit icon.
    - In the **Value - Advanced properties** dialog box, click **Add**.
    - In the **Name** column, type CMSCRIPT\_CS\_ID
    - In the **Value** column, type the user ID of the account under which the instance of the content store runs.

Use a different user account for each instance of Informix content store database.

9. From the **File** menu, click **Save**.

The logon credentials are immediately encrypted.

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.

## Results

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

## Configure Environment Properties for Content Manager Computers

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

After installing Content Manager on the computers you are using for failover protection, you must configure Content Manager on those computers. If you installed more than one Content Manager, you must list all Content Manager URIs on each Content Manager computer.

After you complete the required configuration tasks and start the IBM Cognos Analytics service, the certificate authority service is available to issue certificates to other computers. You can then perform the required configuration tasks on other computers, such as the Application Tier Components computer and gateway computers. Otherwise, you can continue to configure the Content Manager computers by changing the default property settings (see [“Changing default configuration settings” on page 169](#)) so that they better suit your environment. For example, you can configure IBM Cognos Analytics components to use an authentication provider (see [Chapter 13, “Configuring authentication providers,” on page 239](#)), enable and disable services (see [“Enable and Disable Services” on page 181](#)) on the Content Manager computers, or change global settings (see [“Changing Global Settings” on page 228](#)).

Note that if you change global settings on one Content Manager computer, you must make the same changes on the other Content Manager computers.

## Configuring the active Content Manager

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

### Procedure

1. On the Content Manager computer that you want to designate as the default active Content Manager, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, click the value for **Content Manager URIs** and then click the edit button.
4. Specify the URIs for the other Content Manager computers:

- In the **Value - Content Manager URIs** dialog box, click **Add**.
- In the blank row of the table, click and then type the full URI of the Content Manager computer.

Do not delete the first value in the table. This value identifies the local Content Manager computer and is required.

Replace the localhost portion of the URI with a host name or IP address. All URI properties must use the the same format: all host names or all IP addresses.

- Repeat the previous two bulleted steps for each URI to be added.

You must include all Content Manager URIs in the list.

- Click **OK**.

5. From the **File** menu, click **Save**.

## Configuring standby Content Managers

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

## Procedure

1. Ensure that you already configured the Environment properties on at least one Content Manager computer and that IBM Cognos Analytics 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 same URI list that is specified on the primary Content Manager computer.

**Important:** The **Content Manager URIs** setting is used to keep track of the Content Manager servers in the environment. The primary Content Manager server must be listed first, with all the standby Content Manager servers after. In all Content Manager URI instances, this list must be in the exact same order.

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 an email server

If you want to send Cognos Analytics content by email, you must configure a connection to your email server.

### Procedure

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) email server.

To be able to open content that is 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 content.

To be able to open content that is 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 click the edit button when it appears.
4. Type the values in the **Value - Account and password** dialog box, and click **OK**.

If logon credentials are not required for the SMTP server, remove the default information for the **Account and password** property. When you are prompted for confirmation to leave this property blank, click **OK**. Ensure that the default user name is removed. Otherwise, the default account is used and notifications do not work properly.

5. In the **Properties** window, type the appropriate value for the default sender account.
6. In the **Explorer** window, right-click **Notification**, and click **Test**.

IBM Cognos Analytics tests the email server connection.



## Enabling a secure TLS connection to your email server


Enable a secure TLS connection to your email server to allow encrypted TLS communication.

If SSL Encryption is configured, but a secure TLS connection is not enabled, the connection fails and the following message appears: 502 Unknown command.

### Before you begin

You must have a certificate, typically in .crt format, that is common to the email server.

### Procedure

1. Import the certificate into the JRE keystore to enable a trust between Cognos Analytics and the email server.
    - On Windows, type `install_location\bin\DLS_SSL_CertImportTool.bat certificate_location\email_certificate.crt -p keystore_password`
    - On Unix or Linux, type `install_location/bin/DLS_SSL_CertImportTool.sh certificate_location/email_certificate.crt -p keystore_password`
  2. In Cognos Configuration, select **Data Access > Notification** and edit the properties as follows:
    - SMTP mail server**  
Set the value to `email_server_name:port_number`, where `port_number` represents a port that is enabled for TLS/SSL or STARTTLS
    - Account and password**  
Set a userid and password when authentication to the email server is required.
    - Default Sender**  
Set the email account that sends emails from the email server.
    - SSL Encryption Enabled**  
Set the value to True.
  3. In Cognos Configuration, select **Local Configuration**.
    - a) Click the **Value** field for **Advanced properties**.
    - b) Click the pencil icon .
    - c) Click **Add**.
    - d) In the **Name** field, type `emf.mail.tls.enabled`
    - e) In the **Value** field, type `true`
    - f) Click **OK**.
  4. In Cognos Administration, configure the advanced setting `emf.mail.tls.enabled` with a value of `true`. For more information, see *Configuring advanced settings for specific services*.
- Note:** You must restart the delivery service after you make this change.

## Enable Security

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

### Procedure

1. In the IBM Cognos Configuration **Explorer** window, click **Security > Authentication > Cognos**.
2. Click the **Value** box for **Allow Anonymous Access**, and select **False**.
3. Right-click **Authentication**, and click **New Resource > Namespace**.
4. In the **Name** box, type a name for your authentication namespace.

5. In the **Type** list, click the appropriate namespace type and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.

6. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
7. From the **File** menu, click **Save**.

## Start Content Manager

After you have set the database connection properties for the content store and configured the security namespace, you can start the Content Manager computer.

### Before you begin

Ensure that user or service account is set up. For information, see [“Configure a User Account or Network Service Account for IBM Cognos Analytics” on page 15](#).

### Procedure

1. Start IBM Cognos Configuration.

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

2. Ensure that you save your configuration, otherwise you cannot start the IBM Cognos service.
3. From the **Actions** menu, click **Test**.

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

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

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

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

Do not start the service until all tests are error-free.

5. From the **Actions** menu, click **Start**.

It may take a few minutes for the IBM Cognos service to start.

This action starts all installed services that are not running and registers the IBM Cognos service on Windows.

## Test the Content Manager installation

You can test the installation using a web browser.

### Procedure

1. Open a web browser.
2. Test that Content Manager is running by typing the URI for the active Content Manager.

For example, `http://host_name:port/p2pd/servlet`

The default value for `host_name:port` is `localhost:9300`.

Content Manager is available when the **State** value is **Running** or **Standby**.

## Installing and configuring the Application services

You can install the Application services components on different computers or on the same computer.

## Install the Application services components

Ensure that the computer where you installed the active Content Manager is configured and available before you configure Application services components computers.

If you are upgrading, IBM Cognos Analytics uses the existing configuration data for the Application services components computers. However, if you installed the Application services components in a new location, you must configure the environment properties.

### 64-bit Installations

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

### Printer Requirements

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

## Installing the application services components on UNIX or Linux operating systems

You can install Application services components on one or more computers, depending on your environment.

### Before you begin

Go to the [IBM Cognos Analytics on Premises 12.0.x Supported Software Environments](https://www.ibm.com/support/pages/node/6966712) (<https://www.ibm.com/support/pages/node/6966712>) to verify that the required patches are installed on your computer.

### Procedure

1. Go to the location where the installation files were downloaded and extracted.

**Tip:** Use new versions of file compression software to extract the files. Older versions of such software might not extract the files.

2. To start the installation wizard, go to the operating system directory and then type `./ca_srv_<platform>_<build>.bin`

**Tip:** When you use the `ca_srv_<platform>_<build>.bin` 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. For more information, see Installation Guide.

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

- When selecting the directory, consider the following:

Install Application services components in a directory that contains only ASCII characters in the path name. Some UNIX and Linux Web servers do not support non-ASCII characters in directory names.

- When selecting components, clear all components except **Application services**.

#### 4. Click **Finish**.

Do not configure IBM Cognos Analytics immediately because you must do other tasks first to ensure that your environment is properly set up.

### What to do next

Configure IBM Cognos Analytics using IBM Cognos Configuration. Open this tool by typing `cogconfig.sh` in the `install_location/bin64` directory.

## Installing the application services components on Windows operating system

You can install application services components on one or more computers, depending on your environment.

For Windows computers, the default installation location uses the **Program Files** directory. If you install to this location, ensure that you run IBM Cognos Configuration as an administrator. Alternatively, you can install the product to a directory outside of **Program Files**, such as `C:\IBM\cognos\analytics`.

### Procedure

1. Go to the location where the installation files were downloaded and extracted, and double-click `ca_srv_<platform>_<build>.exe`.

**Tip:** Use new versions of file compression software to extract the files. Older versions of such software might not extract the files.

2. 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.

3. Select the **Custom** installation option, and follow the directions in the installation wizard to copy the files to your computer.

- When selecting the directory, consider the following:

Install application services components in a directory that contains only ASCII characters in the path name. Some web servers do not support non-ASCII characters in directory names.

- When selecting components, clear all components except **Application services**.

4. Click **Finish**.

### What to do next

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

## Set up database connectivity for reporting databases

To support communication between IBM Cognos Analytics and the data sources, you must install additional software for your data sources on the same computer that hosts the report server. Depending on the data source and query mode, the required software might include database clients, or Java Database Connectivity (JDBC) driver files, or both.

For IBM Cognos Analytics, the query database (also known as the reporting database) is only accessed by the reporting engine that runs reports. The reporting engine is installed with Application Tier Components and is also used by Framework Manager, and IBM Cognos Transformer.

### Compatible query mode

To run reports that use the compatible query mode, you must use 32-bit data source client libraries and configure the report server to be 32-bit. The compatible query mode uses native client and ODBC connections to communicate with data sources.

## Dynamic query mode

Dynamic query mode provides communication to data sources using Java/XMLA connections.

For supported relational databases, a type 4 JDBC connection is required. A type 4 JDBC driver converts JDBC calls directly into the vendor-specific database protocol. It is written in pure Java and is platform-independent.

For supported OLAP data sources, Java/XMLA connectivity optimizes access by providing customized and enhanced MDX for the specific source and version of your OLAP technology and it harnesses the smarts of the OLAP data source.

To review an up-to-date list of environments that are supported by IBM Cognos Analytics products, including information on operating systems, patches, browsers, web servers, directory servers, database servers, and application servers, see [IBM Cognos Analytics on Premises 12.0.x Supported Software Environments](https://www.ibm.com/support/pages/node/6966712) (<https://www.ibm.com/support/pages/node/6966712>).

## Access OLAP data sources on Windows operating systems

To access the relational databases and OLAP data sources for reporting, you must install the client API software that is provided by your data source vendor. The software must be installed on the same computer where the Application Tier Components are installed.

### Procedure

1. Install the database API software for your relational databases and OLAP data sources on the computer that hosts the report server (where Application Tier Components are installed).

On Microsoft Windows operating systems, the reporting engine supports either native database connectivity or ODBC.

2. If Framework Manager is installed in a separate location from the Application Tier Components, you must also install the client API software on the computer where Framework Manager is installed.

For more information, see [“Setting variables for data source connections for Framework Manager” on page 156](#).

## Access ODBC data sources on UNIX or Linux operating systems

To use an ODBC data source on UNIX or Linux to connect to a supported data source, you must configure the environment to locate the `.odbc.ini` file which contains the references to data source, the connectivity libraries, and their accompanying Driver Manager libraries.

To review supported ODBC data sources, see the [IBM Cognos Analytics on Premises 12.0.x Supported Software Environments](https://www.ibm.com/support/pages/node/6966712) (<https://www.ibm.com/support/pages/node/6966712>).

After configuring for the ODBC connections, you must create connections to the data sources in IBM Cognos Administration. For information, see the *IBM Cognos Administration and Security Guide*.

On Linux operating systems, the `unixODBC` package provided with the operating system provides the ODBC Driver Manager. You must install `unixODBC` version 2.2.11 or later before you can set up data source connections. To verify the version you have installed, use the following command: `odbcinst --version`. Check which version of `unixODBC` is required for the database you are using, and ensure you use that version.

On UNIX operating systems, you must have an ODBC driver manager on your system. You can then specify the `@DRIVERMANAGER` parameter to access the driver manager.

### Procedure

1. Create an environment variable to specify the location of the `.odbc.ini` file.

For example,

```
export ODBCINI=/usr/local/etc/.odbc.ini
```

2. Set the appropriate library path environment variable to specify the location of the 32-bit connectivity libraries and Driver Manager for your database.

The following table lists the environment variables for each operating system that must specify the location of the driver manager libraries.

| Table 15. Environment variables for your operating system |                      |
|-----------------------------------------------------------|----------------------|
| Operating system                                          | Environment variable |
| AIX                                                       | LIBPATH              |
| Linux                                                     | LD_LIBRARY_PATH      |

3. Specify the driver manager for your operating system.

- On UNIX, you must have an ODBC driver manager on your system. You then specify @DRIVERMANAGER=<driver manager name> in the connection string to override the default ODBC driver manager. Here are some examples:
  - To load the iODBC driver manager, type @DRIVERMANAGER=iodbc
  - To load the unixODBC driver manager, type @DRIVERMANAGER=unixodbc
  - To load the Postgres DataDirect ODBC driver manager, type @DRIVERMANAGER=datadirect
- On Linux, if your database vendor does not provide a driver manager, set the library path to include the path to your local unixODBC package, which provides the required driver manager libraries.

For example,

```
LD_LIBRARY_PATH=/usr/lib:$LD_LIBRARY_PATH
```

## What to do next

If you are using multiple ODBC sources on UNIX or Linux operating systems, you may encounter dependencies of library files with common names but different implementations for both the connectivity and the driver manager. In a scenario where one ODBC source validates while another fails based on a dependency, please contact Customer Support. Using a common `.odbc.ini` may result in having incompatible entries for different driver managers. To resolve the problem, review the structure requirements between the driver managers you are using and try to use syntax that is common between the conflicting driver managers.

## Start IBM Cognos Configuration

Use IBM Cognos Configuration to configure IBM Cognos Analytics components and to start and stop IBM Cognos services.

### Before you begin

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

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

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

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

Read [“Critical configuration actions to take first!”](#) on page 167.

## Procedure

1. On Microsoft Windows, click **Start > IBM Cognos Configuration**.

If you are using a Windows computer, and have installed the product to the Program Files (x86) directory, start IBM Cognos Configuration as an Administrator.

2. On UNIX or Linux operating systems, go to the *install\_location/bin64* directory and then type the following command:

```
./cogconfig.sh
```

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

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

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

## Configure Environment Properties for Application services components computers

If you install the Application services components on a different computer than Content Manager, you must configure the Application services components computer so that it knows the location of Content Manager. The distributed components can then communicate with each other.

The Application services components computer must know the location of the Content Manager computers and the notification database to use for job and schedule information. The Application services components computer must use the same notification database that the Content Manager computers use. For more information, see [“Change the notification database” on page 195](#).

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

## Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, change the **localhost** portion of the **Content Manager URIs** property to the name of any Content Manager computer.

4. Specify the URIs for the remaining Content Manager computers:

- In the **Value - Content Manager URIs** dialog box, click **Add**.
- In the blank row of the table, click and then type the full URI of the Content Manager computer.

Replace the localhost portion of the URI with a host name or IP address. All URI properties must use the the same format: all host names or all IP addresses.

- Repeat the previous two bulleted steps for each URI to be added.

You must include all Content Manager URIs in the list.

- Click **OK**.

5. Change the **localhost** portion of the **Gateway URI** property to the name of the computer on which you plan to install the gateway component.

This will ensure that users in different locations can connect to reports and workspaces that are sent by email.

6. Change the **localhost** portion of the remaining URI properties to the name or IP address of your IBM Cognos Analytics 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**.

## Enabling the 64-bit version of report server

You can choose to use a 32-bit or 64-bit version of the report server component. To use the 64-bit version, you must enable it using IBM Cognos Configuration. The default option is 32-bit.

A 32-bit report server can be used with both dynamic query mode and compatible query mode packages. A 64-bit report server can be used only with dynamic query mode packages.

The report server works with the query service. The query service is the engine that powers the dynamic query mode and dynamic cubes. In a 64-bit installation, the query service is 64-bit regardless of whether the report server component is configured to be 32-bit or 64-bit.

Using the 64-bit version of the report server allows more addressable memory for rendering report outputs. For example, out-of-memory conditions during the rendering stage of running a report can be avoided. It is only large report outputs, for example PDF reports with more than 1 thousand pages that require the 64-bit version of the report server component.

You must use the 32-bit version of report server for packages that do not use dynamic query mode. For example, if your package is based on IBM Cognos PowerCubes, you must use the 32-bit version of report server.

If you have multiple Application Tier Components instances in your environment, you can set one instance to use the 32-bit report server. You can then use routing rules so that report requests for non-dynamic query mode packages are routed to the instance that is running the 32-bit version of report server. For more information about routing rules, see the *Administration and Security Guide*.

To enable the 64-bit version, you must install the 64-bit version of the Application Tier Components on a 64-bit computer. If you install the 32-bit version of the Application Tier Components or are using a 32-bit computer, do not enable the 64-bit report server.

### Procedure

1. In the IBM Cognos Configuration **Explorer** window, click **Environment**.
2. Click the **Value** box for **Report server execution mode**, and select **64-bit**.
3. From the **File** menu, click **Save**.
4. Restart your IBM Cognos services if they are running.

## Start the Application services components

After you have configured the environment properties, you can start the services on the Application services components computer.

### Before you begin

To use IBM Cognos Analytics 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 Analytics”](#) on page 15.

### Procedure

1. Start IBM Cognos Configuration.



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

2. Ensure that you save your configuration, otherwise you cannot start the IBM Cognos service.
3. From the **Actions** menu, click **Test**.

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

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

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

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

Do not start the service until all tests are error-free.

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 services components

You can test the installation using a Web browser.

### Procedure

1. Open a Web browser.
2. Test the availability of the dispatcher by typing the **External dispatcher URI** value from IBM Cognos Configuration. For example,

`http://host_name:port/bi`

The default value for `host_name:port` is `localhost:9300`.

The dispatcher is available when the portal appears.



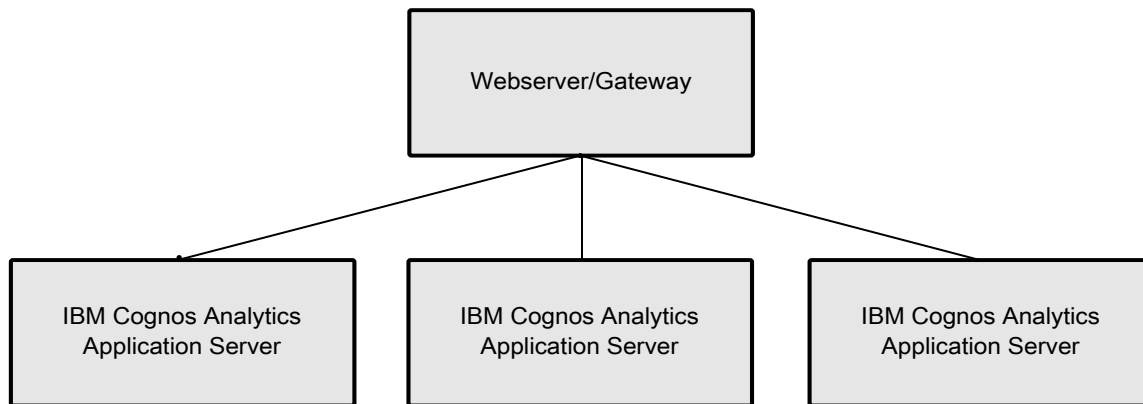
---

## Chapter 10. Configuring the gateway

You can install the optional gateway on one or more computers. Install the gateway if you plan on setting up advanced options such as single sign-on with Kerberos security with IIS, or an architecture where the web server is publicly available outside a firewall. IBM Cognos Analytics uses the web server for load balancing certain requests in addition to hosting and serving static content like icons and image files.

Ensure that the computer where you installed the active Application services is configured and available before you configure gateway computers.

The following diagram shows the gateway server and multiple Cognos Analytics servers. With load balancing enabled, the work load can be distributed across the servers.



This configuration is also recommended in a single application tier environment as the routing would just go to the one server and is ready to add additional tier servers when needed.

Perform the following steps to install and configure the gateway:

- Install the gateway components. See [“Installing the Cognos Analytics gateway”](#) on page 123.
- Configure IBM Cognos Analytics. See [“Configure Cognos Analytics with your web server”](#) on page 124.
- If your web server is Apache HTTP Server or IBM HTTP Server, perform the procedures in [“Configure Apache HTTP Server or IBM HTTP Server ”](#) on page 127 .
- If your web server is Microsoft Internet Information Services, perform the procedures in [“Configure Microsoft Internet Information Services ”](#) on page 138.
- [Test the gateway installation](#) .

---

### Installing the Cognos Analytics gateway

You can install the IBM Cognos Analytics gateway on one or more computers. If you have a web farm, you can install an IBM Cognos Analytics gateway on each web server.

#### Before you begin

Go to the [IBM Cognos Analytics on Premises 12.0.x Supported Software Environments](https://www.ibm.com/support/pages/node/6966712) (<https://www.ibm.com/support/pages/node/6966712>) to verify that the required patches are installed on your computer.

Ensure that the temporary directory has at least 5 GB of memory.

**Tip:** The temporary directory is set with the environment variable *IATEMPDIR* for the UNIX or Linux operating system or with *TMP* for the Microsoft Windows operating system.

## Procedure

1. Start the installation wizard.

- a) For UNIX or Linux, go to the operating system directory and type: `./ca_srv_platform_build.bin`

**Tip:** When you use the `ca_srv_<platform>_<build>.bin` 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. For more information, see [Chapter 5, “Silent installation, uninstallation, and configuration,”](#) on page 37.

- b) For Microsoft Windows, go to the operating system directory, or where the installation files were downloaded, and double-click `ca_srv_platform_build.exe`.

2. 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.

3. Select the **Custom** installation option, and 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 UNIX and Linux web servers do not support non-ASCII characters in directory names.

- When selecting components, clear all components except **Gateway**.

4. Click **Finish**.

## Configure Cognos Analytics with your web server

---

You must configure your web server before users can connect to the IBM Cognos Analytics portal.

For IBM Cognos Analytics 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.

### File permissions

The account under which the web server runs must have read, write and execute privileges to the Cognos installation location. Read access is required to the `./configuration` directory for the `cogstartup.xml` file. Write access is required to `./logs` if debug tracing is required. Execute access is required to the `./cgi-bin` directory so that the SSO modules for Apache HTTP Server, IBM HTTP Server, or Microsoft Internet Information Services can be run by the web server.

### Reference values for the configuration procedures

Refer to the following values where required:

- server name: host name of the web server
- port #: 80 (non-SSL) or 443 (SSL)
- virtual directory name: `ibmcognos`
- Cognos Analytics server name: host name of the IBM Cognos Analytics server(n)

**Important:** If your environment contains more than one Cognos Analytics server, do not include the server running Content Manager service in the steps below. Include only Cognos Analytics servers that have the application server components installed and configured.

- Cognos Analytics port #: 9300

Some or all of these URI settings are in Cognos Configuration, depending on the type of install used:

- **Gateway URI:** For non-SSL use `http://web_server_host_name:80/ibmcognos/bi/v1/disp`. For SSL use `https://web_server_host_name:443/ibmcognos/bi/v1/disp`

This is the URL for disconnected content such as links in PDFs, Excel, and Active Reports. It is also used in links sent by email.

- **Dispatcher URIs for gateway:** `http(s)://IBM_Cognos_Analytics_server_host_name:9300/bi/v1/disp`

This is the list of URIs that the Cognos Apache module or ISAPI code connects to when forwarding requests. Multiple entries are used for failover. Include all relevant IBM Cognos Analytics application servers.

- **Dispatcher URI for external applications:** `http(s)://IBM_Cognos_Analytics_server_host_name:9300/bi/v1/disp`

External applications such as Framework Manager connect on this URL to perform SDK operations.

## Microsoft Internet Information Services

For more detailed information on IIS and Cognos Analytics please see: [Configure IIS and Cognos Analytics](#).

Install the Application Request Routing extension for IIS. For information about how to do this, see <https://www.iis.net/downloads/microsoft/application-request-routing>. This will also install the URL Rewrite extension.

URL Rewrite enables web administrators to create powerful rules to implement URLs that are easier for users to remember and easier for search engines to find. Application Request Routing enables web server administrators to increase web application scalability and reliability through rule-based routing, client and host name affinity, load balancing of HTTP server requests, and distributed disk caching.

If you are upgrading from Cognos Analytics 11.0.3 to Cognos Analytics 11.0.4 (or later) and you had modified `server.xml` to configure an `sso/login` path pointing to `/ibmcognos/cgi-bin/cognosisapi.dll`, remove the following entry from `install_location/wlp/usr/servers/cognosserver/server.xml`:

```
<jndiEntry jndiName="glass/sso/login" value="/ibmcognos/cgi-bin/cognosisapi.dll"/>
```

For details on configuration for Active Directory Server, see [“Enable single signon between Active Directory Server and IBM Cognos components”](#) on page 254

## Enabling the 32-bit web gateway

For a 32-bit web server, you must manually move the 32-bit gateway files in your installation directory.

### Procedure

1. Go to the `install_location/cgi-bin`.
2. Type the following command:
  - On UNIX or Linux operating systems, type `./copyGateMod.sh 32bit`
  - On Windows operating systems, type `copyGateMod.bat 32bit`

### Results

The 32-bit gateway files are copied from the `cgi-bin/lib` directory to the `cgi-bin` directory.

**Note:** If you need to restore the default 64-bit gateway files, follow the procedure and type `./copyGateMod.sh 64bit` or `copyGateMod.bat 64bit`. The 64-bit gateway files are copied from the `cgi-bin/lib64` directory to the `cgi-bin` directory.

## Configuring dispatcher URIs

If you install the gateway component on a different computer than Content Manager or Application Tier Components, you must configure the gateway computer so that it knows the location of a dispatcher. A dispatcher is installed on every Content Manager and Application Tier Components computer. Configure the gateway to use the dispatcher on an Application Tier Components computer.

For failover protection, you can configure more than one dispatcher for a gateway computer. When multiple dispatchers are configured, requests are normally routed to the first dispatcher in the list. If this dispatcher becomes unavailable, the gateway determines the next functioning dispatcher on the list and routes requests there. The primary dispatcher status is monitored by the gateway, and requests are routed back to this component when it returns to service.

After you do the required configuration tasks, the gateway computer can work in your environment.

### Before you begin

Ensure that the computers where you installed Content Manager are configured and the default active Content Manager computer is available before you configure gateway computers.

### Procedure

1. Start IBM Cognos Configuration.

- a) On Microsoft Windows, click **Start > IBM Cognos Configuration**.

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

- b) On UNIX or Linux operating systems, go to the *install\_location/bin64* directory and then type the following command:

```
./cogconfig.sh
```

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

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

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

2. In the **Explorer** window, click **Environment**.

3. In the **Properties** window, under **Gateway Settings**, specify the values for **Dispatcher URIs for the gateway**:

- Click in the **Value** column.
- Click the **Edit** button.
- Change the *localhost* portion of the URI to the name or IP address of an Application Tier Components computer.

This will ensure that users in different locations can connect to reports and workspaces that are sent by email.

**Tip:** If you want to send requests to the dispatcher from a Software Development Kit application or an IBM Cognos Analytics modeling tool that is outside of a network firewall, connect to a dedicated gateway that is configured to connect to the dispatcher using the internal dispatcher URI for your environment (for example, `http://localhost:9300/p2pd/servlet/dispatch`). For security reasons, the default setting for the Dispatcher URI for gateway property prevents the dispatcher from accepting requests for an Software Development Kit application or modeling tool that is outside the firewall. Ensure that you configure appropriate security for this dedicated gateway, such as SSL (see “Configuring the SSL protocol for IBM Cognos components” on page 206). Do not change your main gateway to use the internal dispatcher URI. Doing so will reduce the security of the IBM Cognos Analytics 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 Analytics components check the common symmetric keys (CSK) availability.
8. From the **File** menu, click **Save**.

## Configure Apache HTTP Server or IBM HTTP Server

---

This section describes how to configure Apache HTTP Server or IBM HTTP Server as your web server in IBM Cognos Analytics.

### Configuring IBM HTTP Server V9

You can use IBM HTTP Server (IHS) V9 web server to support load balancing and failover across multiple IBM Cognos Analytics application servers.

To do that, you must install IHS V9 and the Web Server Plug-ins for IBM WebSphere Application Server V9, and then configure IHS V9 to use the `cognos.conf` file.

For more information about installing the Web Server Plug-ins for IBM WebSphere Application Server V9, see [this article](http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.installation.nd.doc/ae/rins_plugins_info.html) ([www.ibm.com/support/knowledgecenter/en/SSAW57\\_9.0.0/com.ibm.websphere.installation.nd.doc/ae/rins\\_plugins\\_info.html](http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.installation.nd.doc/ae/rins_plugins_info.html)).

### Before you begin

The following prerequisites are required:

- IBM SDK, Java Technology Edition, version 8 for Windows (CND15ML)
- IBM WebSphere Application Server V9.0 supplements - Web Server Plug-ins (CND1EML)
- IBM WebSphere Application Server V9.0 supplements - IBM HTTP Server (CND1DML)

### About this task

The directories and aliases for Windows-based IBM HTTP Server (IHS) setups must be properly specified. For example, the alias `ibmcognos` needs to be set to `/ibmcognos "c:/cognos_analytics_location/cognos/webcontent"`. Ensure that the forward slash (/) character is used in the path, and the location is enclosed in double quotation marks (" ").

### Procedure

1. Install IBM Installation Manager (IIM), preferably version 1.8.5 or later, if you do not already have it installed.

You can download IIM from [this location](http://www.ibm.com/support/docview.wss?uid=swg24041188) ([www.ibm.com/support/docview.wss?uid=swg24041188](http://www.ibm.com/support/docview.wss?uid=swg24041188)).

2. Using IIM, install IBM HTTP Server (IHS) V9 and the Web Server Plug-ins for IBM WebSphere Application Server V9 from [Online product repositories for Liberty offerings](http://www.ibm.com/support/knowledgecenter/SSEQTP_liberty/com.ibm.websphere.wlp.nd.multiplatform.doc/ae/cwlp_ins_repositories.html) ([www.ibm.com/support/knowledgecenter/SSEQTP\\_liberty/com.ibm.websphere.wlp.nd.multiplatform.doc/ae/cwlp\\_ins\\_repositories.html](http://www.ibm.com/support/knowledgecenter/SSEQTP_liberty/com.ibm.websphere.wlp.nd.multiplatform.doc/ae/cwlp_ins_repositories.html)).

Ensure that you use the following installation paths:

- /opt/IHS90 as the IHS V9 install root
- /opt/IHS90Plugin as the Web Server Plug-ins for IBM WebSphere Application Server install root

You cannot install the Plug-ins within the IHS V9 install root.

3. Associate the WAS Web Server Plug-ins V9 and IHS V9 by running the following commands:

```
cd /opt/IHS90
bin/simplepct.sh /opt/IHS90Plugin
```

The `simplepct.sh` file was introduced in IHS V9 fix pack 5, and is not available in earlier versions of IHS V9. For more information, see [this article](http://www.ibm.com/support/docview.wss?uid=swg24044965) ([www.ibm.com/support/docview.wss?uid=swg24044965](http://www.ibm.com/support/docview.wss?uid=swg24044965)).

**Tip:** On UNIX, check the `httpd.conf` file in your IHS V9 installation after running this command. If you see `$PLG_ROOT`, replace it with WAS Web Server Plug-ins V9 install root folder, such as `/opt/IHS90Plugin`.

4. Generate the `plugin-cfg.xml` file for WAS Web Server Plug-ins. For more information, see [“Generating the plugin-cfg.xml for Cognos Analytics servers”](#) on page 130.

5. Copy the `plugin-cfg.xml` file that was generated in step 4 to the `WAS_Web_Server_Plugins_install_root/config/webserver1` directory, such as `/opt/IHS90Plugin/config/webserver1`.

**Tip:** On UNIX, ensure that the `plugin-cfg.xml` file has read and execute permissions after copying the file.

6. Configure the IHS V9 using the following steps:

- a) Access the template file `cognos_IHS9_SS0.conf` or `cognos_IHS9.conf` in the Cognos Analytics `gateway_install_location/cgi-bin/templates` directory.
- b) Copy the template file to `IHS9_install_root/conf` directory, such as `/opt/IHS90/conf`, and rename it to `cognos.conf`. Modify the `cognos.conf` file to point to the proper installation location.
- c) Configure `httpd.conf`, as documented in the article [“Configuring Cognos Analytics with either Apache HTTP Server or IBM HTTP Server”](#) on page 136.
- d) Restart the IHS V9 web server.

## Configuring IBM HTTP Server V9 with SSL

If you use Secure Sockets Layer (SSL) on IBM Cognos Analytics with IBM HTTP Server V9 as your web server, you must set up SSL between WAS Web Server Plug-ins and the Cognos Analytics application server by extracting the IBM Cognos certificate and adding it to the WAS Web Server Plug-ins trust store.

If you use SSL on IBM HTTP Server V9, configure your environment as documented in the article [“Configuring IBM HTTP Server with SSL”](#) on page 132.

## Procedure

1. Start the IBM Cognos Analytics application server that is configured to use SSL.
2. Copy the Server section from the `Cognos_Analytics_application_server_install_root/wlp/usr/servers/cognosserver/logs/state/plugin-cfg.xml` file to the `plug-in/config/webserver1/plugin-cfg.xml` file. Ensure that the Cognos Analytics https entry point is specified, as shown in the following example:



```
<Server CloneID="a4949c5e-cb36-40dd-9f43-58702daf7b1a" ConnectTimeout="5"
ExtendedHandshake="false" LoadBalanceWeight="20" MaxConnections="-1"
Name="default_node_cognosserver" ServerIOTimeout="900" WaitForContinue="false">
  <Transport Hostname="hostname" Port="xxx" Protocol="https">
    <Property Name="keyring" Value="D:\install\IBM\WebSphere\Plugins\config\
webserver1\plugin-key.kdb"/>
    <Property Name="stashfile" Value="D:\install\IBM\WebSphere\Plugins\config\
webserver1\plugin-key.sth"/>
  </Transport>
</Server>
```

3. In the Plug-in/config/webserver1/plugin-cfg.xml file, add the following attribute to the Config section:

```
AutoSecurity="false"
```

4. Obtain the IBM Cognos certificate by using the following steps:
  - a) Go to the Cognos Analytics *applicaton\_server\_install\_root*/bin directory.
  - b) Extract the certificate by typing a command that is appropriate for your operating system.

On UNIX or Linux operating systems, type

```
ThirdPartyCertificateTool.sh -E -T -r destination file -p NoPassWordSet
```

On Windows operating systems, type

```
ThirdPartyCertificateTool.bat -E -T -r destination file -p NoPassWordSet
```

5. Copy the .cert file, for example ca-host1.cert, that was generated in step 4 to WAS Web Server Plug-ins host.
6. Add the Cognos Analytics .cert file to the WAS Web Server Plug-ins key store plugin-key.kdb. If the plugin-key.kdb file does not exist, create one as described in step 7.

You can use different methods to add the .cert file to the key store. The following steps describe how to do that by using the gskcapicmd tool that is shipped with IHS V9.

- a) Go to the IHS9 ROOT folder.
- b) Type a command that is appropriate for your operating system.

On UNIX or Linux operating systems, type

```
bin/gskcapicmd -cert -add -db WAS_Plugin_root/config/webserver1/plugin-key.kdb
-stashed -label ca-host1 -file ca-host1.cert
```

On Windows operating systems, type

```
bin\gskcapicmd.bat -cert -add -db WAS_Plugin_root\config\webserver1\plugin-key.kdb
-stashed -label ca-host1 -file ca-host1.cert
```

For information about other methods of adding certificate files to the key store, search [IBM Knowledge Center](http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0) (www.ibm.com/support/knowledgecenter/SSEP7J\_11.0.0).

7. Create an empty key store for WAS Web Server Plug-ins:
  - a) Go to the IHS9 ROOT folder.
  - b) Type a command that is appropriate for your operating system.

On UNIX or Linux operating systems, type

```
bin/gskcapicmd -keydb -create -db WAS_Plugin_root/config/webserver1
/plugin-key.kdb -pw xxx -stash
```

On Windows operating systems, type

```
bin\gskcapicmd.bat -keydb -create -db WAS_Plugin_root\config\webserver1
\plugin-key.kdb -pw xxx -stash
```

## Generating the plugin-cfg.xml for Cognos Analytics servers

In an environment with WebSphere Application Server, the `plugin-cfg.xml` file contains configuration information that determines how the web server plug-in forwards requests.

### About this task

This procedure is not applicable to the IBM Cognos Analytics servers that are used to run the Content Manager service.

For more information about merging `plugin-cfg.xml` from multiple standalone WebSphere Liberty Profile servers, see [this article](http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/twsv_merge_configfiles.html) ([www.ibm.com/support/knowledgecenter/en/SSAW57\\_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/twsv\\_merge\\_configfiles.html](http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/twsv_merge_configfiles.html)).

### Procedure

1. Go to the Cognos Analytics application server installation location.
2. Open the `ca_application_server_install_root/wlp/usr/servers/cognosserver/server.xml` file, and add the following setting to the file:

```
<pluginConfiguration pluginInstallRoot="WAS_plugin_install_root"
webserverPort="IHS9_port"/>
```

For example:

```
<pluginConfiguration pluginInstallRoot="/opt/IHS90Plugin" webserverPort="8080"/>
```

3. Configure and start the Cognos Analytics application server.

After the server is started, a file named `plugin-cfg.xml` is generated in the Cognos Analytics `application_server_install_root/wlp/usr/servers/cognosserver/logs/state` directory.

4. Open the `plugin-cfg.xml` file, and modify the `UriGroup` section by deleting everything except for the following two elements:

```
<UriGroup Name="default_host_cognosserver_default_node_Cluster_URIs">
  <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid"
    Name="/bi/*"/>
  <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid"
    Name="/bi/v1/*"/>
</UriGroup>
```

**Tip:** The second `Uri` entry doesn't exist in the file. You need to add it.

5. Save the `plugin-cfg.xml` file.

You just configured one Cognos Analytics application server for the `ServerCluster`.

6. To add another Cognos Analytics application server to the `ServerCluster`, perform the following steps:

- a) From the Cognos Analytics `application_server_install_root/wlp/usr/servers/cognosserver/logs/state` directory, open the `plugin-cfg.xml` file. Copy the `Server` element under the `ServerCluster` section. For example, copy the following `Server` element:

```
<Server CloneID="081cd7c5-bb6c-4a93-a074-33fa07e587f3" ConnectTimeout="5"
ExtendedHandshake="false" LoadBalanceWeight="20" MaxConnections="-1"
Name="default_node_cognosserver" ServerIOTimeout="900" WaitForContinue="false">
  <Transport Hostname="caserverhost" Port="9300" Protocol="http"/>
</Server>
```

- b) Paste the `Server` element to the `ServerCluster` section in the `plugin-cfg.xml` file that was generated in step 4. Ensure that the endpoint specified in the `Server` element is accessible from your web server host.

- c) Change the name of the server by modifying the value of the Name attribute. Ensure that the name is different than other server names in the ServerCluster. For example, change the value from `default_node_cognosserver` to `default_node_cognosserver_1`.
- d) Add the new server to the PrimaryServers section, as shown below:

```
<PrimaryServers>
  <Server Name="default_node_cognosserver"/>
  <Server Name="default_node_cognosserver_1"/>
</PrimaryServers>
```

- e) Save the `plugin-cfg.xml` file. The new server is added to the ServerCluster.

7. To add more servers, repeat step 6.

## What to do next

By default, WebSphere Liberty Profile (WLP) creates a random, unique ID. If the `server.xml` file of the WLP changes, for example as a result of changes to the Cognos Analytics configuration settings or resetting the WLP ( for example, cleaning the `cognos_analytics_install/wlp/usr/servers/cognosserver/workarea` ), the ID might change and break the link between IHS and Cognos Analytics. To prevent this issue, try using the following solution:

- Using a text editor, create a file named `local-server.xml`.
- Add the following content to the file:

```
<?xml version="1.0" encoding="UTF-8"?>
<server>
  <httpSession cloneID="MyCloneID"/>
</server>
```

The `MyCloneID` can be any unique, alphanumeric value. For ease of use, the fully qualified domain name could be used, unless multiple dispatchers are installed on the same server.

- Save the `local-server.xml` file to the `Cognos Analyticsinstall_location/configuration` directory.

## Configuring WebDAV on IBM HTTP Server or Apache HTTP Server

To view and browse images in Reporting, configure Web Distributed Authoring and Versioning (WebDAV) on your web server.

Report authors can browse for images to include in reports in a way that is similar to browsing a file system. On IBM HTTP Server or Apache HTTP Server, you must add directives to your server configuration file, and then configure the directory access.

Use the following procedure to configure WebDAV on Apache 2.4.

### Procedure

1. In the `webserver_location/conf` directory, open the `httpd.conf` file in a text editor.
2. Uncomment the directives that load `modules/mod_dav.so` and `modules/mod_dav_fs.so`.

```
LoadModule dav_module modules/mod_dav.so
LoadModule dav_fs_module modules/mod_dav_fs.so
```

3. Provide a location for the `DAVLockDB` directive.

For example,

```
DAVLockDB "webserver_location/var/DavLock"
```

Ensure that the directory exists.

4. Create an alias for the directory where your images are stored.
5. Add `Dav On` to the `<Directory>` information for the alias.

For example, for Apache 2.4

```
Alias /images "path/shared_images"

<Directory "path/shared_images">
    Dav On
    Options Indexes MultiViews
    AllowOverride None
    Require all granted
</Directory>
```

6. Save the file.
7. Restart your web server.

## Results

With WebDAV enabled, Reporting users can add images to their reports. When users click **Browse** in the image browser, the default location for browsing is `http://servername/ibmcognos/bi/samples/images`. If you created another location, users can enter that location.

## Configuring IBM HTTP Server with SSL

If you are using Secure Sockets Layer (SSL) on IBM HTTP Server, you must change the **Gateway URI** values in IBM Cognos Configuration to be able to access the portal.

To enable SSL on your web server, you must obtain a web server certificate signed by a Certificate Authority (CA) and install it into your web server. For more information about using certificates with your web server, see your web server documentation. These certificates are not provided with IBM Cognos products.

To enable users to access the IBM Cognos portal using SSL, you must change the **Gateway URI** values in IBM Cognos Configuration for each computer where the Application Tier Components and Framework Manager are installed.

### Before you begin

IBM HTTP Server must have IBM Global Security Kit (GSKit) installed. For more information about the supported versions of GSKit on IBM HTTP Server, see the IBM Software Compatibility Report.

### Procedure

1. On each computer where the Application Tier Components or Framework Manager are installed, start IBM Cognos Configuration.
2. Under **Local Configuration**, click **Environment**, and change the **Gateway URI** value from `http` to `https`.
3. In the **Gateway URI** value, change the port number to the SSL port number defined for your web server.  
For example, the default port number for SSL connections is usually 443.
4. On each computer where the Application Tier Components or Framework Manager are installed, go to the `install_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 truststore.

Import the certificates by typing the following command:

On UNIX or LINUX, type

```
ThirdPartyCertificateTool.sh -T -i -r path/certificate_fileName -p password
```

On Windows, type

```
ThirdPartyCertificateTool.bat -T -i -r path\certificate_fileName -p password
```

**Note:** If password is not set, the default password is NoPassWordSet.

5. Type the following command from the web server *ihp\_install\_root/bin* directory:

```
ihp_install_root/bin/script_name
```

Where *ihp\_install\_root* is the directory where IBM HTTP Server is installed and *script\_name* is *gskver.bat* for Microsoft Windows or *gskver.sh* for UNIX or Linux.

The GSKit shared libraries and version information are displayed. Verify that the version displayed is the minimum supported version as shown in the support document mentioned in the *Before you begin* section of this procedure.

6. Start the iKeyman utility by typing the following command:

```
ihp_install_root/bin/script_name
```

Where *ihp\_install\_root* is the directory where IBM HTTP Server is installed and *script\_name* is *ikeyman.bat* for Microsoft Windows or *ikeyman.sh* for UNIX or Linux.

7. From the menu, select **Key Database File > New**.

8. Enter the following values and click **OK**:

**File Name**

Name of the key database file. The default value is *key.kdb*.

**Location**

Place to store the *key.kdb* file. The default value is *ihp\_install\_root/bin*.

9. In the **Password Prompt** window, enter a password, select the **Stash a password to a file** check box, and click **OK**.

When you select the **Stash a password to a file** check box, the password is encrypted and is saved as a *.sth* file in the same directory as the key database file.

A completed successfully message displays.

10. Open the *ihp\_install\_root/conf/httpd.conf* file in a text editor.

11. Add the Keyfile directive with the path to your key database file. Put it after the VirtualHost section in the file.

For example,

```
<VirtualHost *:443>
...
</VirtualHost>
KeyFile ihp_install_root/key.kdb
```

12. Save and close the *httpd.conf* file.

13. Extract the Cognos Analytics certificate to a file. Run the following command from the IBM Cognos Analytics server in *ca\_install/bin*.

```
script_name -E -T -r ca_cert_file -p NoPassWordSet
```

Where *script\_name* is *ThirdPartyCertificateTool.bat* for Microsoft Windows or *ThirdPartyCertificateTool.sh* for UNIX or Linux and *ca\_cert\_file* is the name of the certificate file.

14. Copy the certificate file to *ihp\_install\_root/key\_database\_file\_directory* where *ihp\_install\_root* is the directory where IBM HTTP Server is installed and *key\_database\_file\_directory* is the directory where the key database file is stored.

15. In *ihp\_install\_root/bin*, type the following command:

```
script_name -cert -import -db ca_cert_file
-pw NoPassWordSet -target key.kdb -target_pw key_database_file_password
```

Where *script\_name* is *gskcapicmd.bat* for Microsoft Windows or *gskcapicmd.sh* for UNIX or Linux and *key\_database\_file\_password* is the password for the key database file.

16. Start IBM HTTP Server. Enter the following command in *ihp\_install\_root/bin*:

```
script_name -k start
```

Where *script\_name* is `apchttpd.bat` for Microsoft Windows or `./apchttpd` for UNIX or Linux. On Microsoft Windows, you can also start the script as a service.

17. Verify that IBM HTTP Server is running by entering the following URI in the address field of a web browser:

```
https://web_server_host_name:port
```

Where *web\_server\_host\_name* is the host name of IBM HTTP Server and *port* is the IBM HTTP Server port number.

18. Save your configuration, and restart your services.

## Results

When you access the portal using `https://servername:443/ibmcognos`, you are prompted to install a certificate. To avoid being prompted by a security alert for each new session, install the certificate into one of your web browser's certificate stores.

## Configuring Apache HTTP Server or IBM HTTP Server with Cognos Analytics

After you complete this procedure, the server can handle requests for static files (such as `.js`, `.html`, `.css`), load balance requests to IBM Cognos Analytics, and route SSO requests through the Cognos Analytics gateway code.

### About this task

You can use one of the sample gateway configuration files that are provided with Cognos Analytics. The sample files are located in `gateway_component_install_location/cgi-bin/templates` where *gateway\_component\_install\_location* is the directory where the gateway component is installed. The following table describes the sample files. Choose the file for your environment:

Environment	Sample file name
Apache 2.2 non-SSO	<code>cognos_apache22_loadbalance.conf</code>
Apache 2.2 SSO	<code>cognos_apache22_loadbalance_SSO.conf</code>
Apache 2.4 non-SSO	<code>cognos_apache24_loadbalance.conf</code>
Apache 2.4 SSO	<code>cognos_apache24_loadbalance_SSO.conf</code>
IBM HTTP Server 9.0 non-SSO	<code>cognos_IHS9_loadbalance.conf</code>
IBM HTTP Server 9.0 SSO	<code>cognos_IHS9_loadbalance_SSO.conf</code>

### Important:

Use caution if you plan to customize the sample HTTP server files. Doing so may prevent dashboard users from being able to [auto-create local data caches](#).

If you upgraded from an older version of Cognos Analytics, the HTTP configuration files may have been preserved and you must update them to the most recent version.

If your Cognos Analytics installation uses any additional HTTP server configuration files, including but not limited to the Apache HTTP Server `httpd.conf` file, you may need to update those files. Otherwise, dashboard users may not be able to [auto-create local data caches](#).

For information about how to resolve this local data caching issue, see ['Auto create data caches' progress starts but does not complete configuring data caches](#) (www.ibm.com/support/pages/node/6997029).

The directories and aliases for Windows-based IBM HTTP Server (IHS) setups must be properly specified. For example, the alias `ibmcognos` needs to be set to `/ibmcognos "c:/cognos_analytics_location/cognos/webcontent"`. Ensure that the forward slash (/) character is used in the path, and the location is enclosed in double quotation marks (" ").

## Procedure

1. Copy the sample configuration file associated with your gateway to `apache_install_root/conf` or `ihs_install_root/conf` directory, and rename it to `cognos.conf`.
2. Open `cognos.conf` in a text editor, and change the `BalancerMember` directive to use `https` and a fully qualified domain name.

For example,

```
<Proxy balancer://mycluster>
  BalancerMember https://ica-host1.domain:9300 route=1
  BalancerMember https://ica-host2.domain:9300 route=2
</Proxy>
```

3. Ensure that the following section is present in the sample file.

- For Apache HTTP Server:

```
# Send default URL to service
RewriteRule ^/ibmcognos/bi/($|[^/]+\.(jsp|.*))$ balancer://mycluster/bi/$1$3 [P]
RewriteRule ^/ibmcognos/bi/(login.*)$ balancer://mycluster/bi/$1 [P]
RewriteRule ^/ibmcognos/bi/(dashboard-print.html) balancer://mycluster/bi/$1 [P]
```

- For IBM HTTP Server:

```
# Send default URL to service
RewriteRule ^/ibmcognos/bi/$ /bi/ [PT,L]
RewriteRule ^/ibmcognos/bi/([^\.]+\.(jsp|.*))$ /bi/$1 [PT,L]
RewriteRule ^/ibmcognos/bi/(login.*)$ /bi/$1 [PT,L]
RewriteRule ^/ibmcognos/bi/(dashboard-print.html) /bi/$1 [PT,L]
```

4. Ensure that the following section is present in the sample file.

```
# Rewrite Saved-Output and Viewer static references
RewriteRule ^/ibmcognos/bi/rv/(.*)$ /ibmcognos/rv/$1 [PT,L]
```

If this section is missing, add it after the `# Rewrite Event Studio static references` section.

5. If you want to integrate Cognos Analytics for Jupyter Notebook Server, in an Apache 2.4 sample file, complete the following steps:
  - a) Locate the `# Rewrite jupyter websocket requests directly to jupyter server` section.
  - b) In this section, uncomment the line `#RewriteRule ^/ibmcognos/bi/v1/jupyter/(user/[^\/]*)/(api/kernels/[^\.]+\.(.*) ws://ica-jupyter-host.domain:8000/bi/v1/jupyter/$1/$2$3 [P,L]`

For more information, see [“Configuring Jupyter Notebook Server”](#) on page 52.

**Important:** Starting with Cognos Analytics version 11.1.6, Jupyter Notebook supports only Apache 2.4 gateways.

6. Find the `Directory` section and make sure it is pointing to the IBM Cognos Analytics installation location.
7. Save the `cognos.conf` file.
8. Configure `httpd.conf`, as documented in the article [“Configuring Cognos Analytics with either Apache HTTP Server or IBM HTTP Server”](#) on page 136.

## Configuring Cognos Analytics with either Apache HTTP Server or IBM HTTP Server

This topic explains how to configure either Apache HTTP Server or IBM HTTP Server to use the `cognos.conf` file. This configuration file contains all the settings required by IBM Cognos Analytics.

### About this task

Perform the following steps to configure your web server to use the `cognos.conf` file. This configuration file contains all the settings required by IBM Cognos Analytics.

### Procedure

1. Go to the `apache/conf` directory.
2. Open the `httpd.conf` file in a text editor.
3. If you are using SSL, follow these steps
  - a) Add the following lines to the file:

```
<VirtualHost *:443>
SSLEnable
SSLClientAuth None
SSLProxyEngine on
# IBM Cognos Analytics Configuration
  Include conf/cognos.conf
</VirtualHost>
SSLDisable
```

- b) If you are using SSL with IBM HTTP Server, follow these steps:

- i) Uncomment the following line:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
```

- ii) Update the value of the `ServerName` directory to be the host name of IBM HTTP Server.

4. If you are not using SSL, add the following lines to the file:

```
<VirtualHost *:80>
  Include conf/cognos.conf
</VirtualHost>
```

5. Save and close the `httpd.conf` file.

For UNIX only, define the MIME type for SVG files.

6. Open the `etc/mime.types` file in a text editor and add the following lines:

```
#MIME type      Extensions
image/svg+xml    svg
```

7. Save and close the file.
8. For the Cognos Analytics web module to work in a UNIX or Linux environment, you must append the IBM Cognos Analytics gateway `cgi-bin` directory to the library path.

Operating System	Variable
AIX	LIBPATH
Solaris or Linux	LD_LIBRARY_PATH

For example, in a Linux environment, sign in as the user that starts the web server. If you are using the Bash shell, you will be adding the following to the end of `$HOME/.bashrc`: `Export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/ibm/cognos/analytics/cgi-bin`



9. Restart the web server.

## Apache web server load balancing

Load balancing allows you to scale your Apache web server.

For information on Apache load balancing, see the following resources:

- [https://httpd.apache.org/docs/2.4/mod/mod\\_proxy\\_balancer.html](https://httpd.apache.org/docs/2.4/mod/mod_proxy_balancer.html)
- [https://httpd.apache.org/docs/2.4/mod/mod\\_proxy.html#balancermember](https://httpd.apache.org/docs/2.4/mod/mod_proxy.html#balancermember)

**Note:** Consult your Apache administrator for more configuration options appropriate for your Cognos Analytics environment.

## Enabling HTTP/2 for a web server

HTTP/2 is a networking protocol for low-latency transport of content. This protocol is essential for load balancing of certain requests, and serving static content, such as icons and image files, efficiently.

IBM Cognos Analytics doesn't require a web server like Microsoft IIS or Apache HTTP Server to be configured for HTTP/2. However, it's a best practice to do so.

Enabling HTTP/2 on your web server might improve the responsiveness of some of your Cognos Analytics dashboards. Compared to the traditional HTTP/1.1 protocol, HTTP/2 offers the following two key advantages that might improve the load times of widgets in your dashboards.

- Header compression

The HTTP header size is much smaller in HTTP/2 compared to HTTP/1.1, which means faster transfer of information.

- Increased concurrency of requests

HTTP/2 supports several requests on the same TCP connection. Dashboarding in Cognos Analytics is engineered for the parallel processing of widgets, but HTTP/1.1 throttles the number of concurrent queries much more than HTTP/2. By using HTTP/2, a greater number of dashboard widgets can be processed simultaneously compared to HTTP/1.1

The persistent client/server connection is another advantage of HTTP/2. This means that a TLS (the successor to SSL) handshake happens only once, rather than on each request. For higher latency environments, this factor can have a significant impact on user wait times.

Consider the following factors before you enable HTTP/2:

- HTTP/2 is supported only over TLS so you need to access your Cognos environment with the `https://` at the beginning of the URL. Otherwise, the system falls back to using HTTP/1.1.
- Not all web browser versions support HTTP/2 and connect by using HTTP/1.1 instead.
- When HTTP/2 is enabled, the web browser no longer limits the number of concurrent queries. HTTP/2 allows a busy dashboard to increase the workload on the Cognos Analytics server and on any underlying data servers in a way that is not possible with HTTP/1.1. Fewer users are now able to apply much greater load to back-end servers.

## Procedure

To learn about and enable HTTP/2, go to the following websites:

- Apache: <https://httpd.apache.org/docs/2.4/howto/http2.html>
- IIS: <https://docs.microsoft.com/en-us/iis/get-started/whats-new-in-iis-10/http2-on-iis>
- NGINX: <https://www.nginx.com/blog/http2-module-nginx/#config>

## Configure Microsoft Internet Information Services

---

This section describes how to configure Microsoft Internet Information Services (IIS) as your web server in IBM Cognos Analytics.

### Configuring WebDAV on IIS

To view and browse images in the Reporting, configure Web Distributed Authoring and Versioning (WebDAV) on your web server. Report authors can browse for images to include in reports in a way that is similar to browsing a file system. On Microsoft Internet Information Services (IIS) web servers, you must first enable the WebDAV feature, and then configure your web server to access the image location.

#### Procedure

1. In the Microsoft Windows **Control Panel**, click **Programs > Programs and Features**.  
If you are using Microsoft Windows 2012 Server, **Programs and Features** is available directly from the **Control Panel**.
2. Click **Turn Windows features on or off**.
3. If you are using Microsoft Windows 2008 Server, use the following steps:
  - a) Click **Server Manager > Roles > Web Server (IIS)**.
  - b) In the **Role Services** section, select **Add Role Services**.
  - c) Under **Web Server > Common HTTP Features**, select **WebDAV Publishing**.
  - d) Click **Next**, and then click **Install**.
4. If you are using Microsoft Windows 2012 Server, use the following steps:
  - a) In the **Add Roles and Features Wizard**, click **Role-based or feature-based installation**, and click **Next**.
  - b) Select your server, and click **Next**.
  - c) Expand **Web Server (IIS) > Web Server > Common HTTP Features**, and select **WebDAV Publishing**.
  - d) Click **Next > Next**, and then click **Install**.
5. In the **Internet Information Services (IIS) Manager** console, under **Connections**, select your server name.
  - If you are using Microsoft Windows 2012 Server, in **Server Manager**, select **IIS**, and then right-click your server name, and click **Internet Information Services (IIS) Manager**.
  - If you are using Microsoft Windows 2008 Server, in **Server Manager**, expand **Roles > Web Server (IIS)**, and then click **Internet Information Services (IIS) Manager**.
6. Under **Connections**, expand your web server, **Sites**, and select your website.  
For example, select **Default Web Site**.
7. Double-click **WebDAV Authoring**.
8. Click **Enable WebDAV**.
9. Click **WebDAV Settings**.
10. If you have anonymous access enabled, select **True** for **Allow Anonymous Property Queries**, and click **Apply**.
11. Select the directory or virtual directory to which you want to allow WebDAV access.
12. Double-click **WebDAV Authoring**.
13. Click **Add Authoring Rule**, and add the appropriate rules for your environment.  
For example, if you installed the samples and you want to use the default path, under the **ibmcognos** virtual directory, expand **bi/samples**, and select **images**, and add an authoring rule for the image files.
14. Right-click the directory or virtual directory you added authoring rules to, and click **Edit Permissions**.

15. Click **Security**, and add the appropriate permissions.

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

## Results

With WebDAV enabled, Reporting users can add images to their reports. When users click **Browse** in the image browser, the default location for browsing is `http://servername/ibmcognos/bi/samples/images`. If you created another location, users can enter that location.

## Configuring IIS with SSL

To configure Microsoft Internet Information Services (IIS) with secure sockets layer (SSL) you extract the IBM Cognos certificate and then add it to the truststore on IIS.

### Procedure

1. Go to the `install_location/bin` directory.
2. Extract the IBM Cognos certificate by typing the following command:

On UNIX or Linux operating systems, type `ThirdPartyCertificateTool.sh -E -T -r destination_file -p NoPassWordSet`

On Microsoft Windows operating systems, type `ThirdPartyCertificateTool.bat -E -T -r destination_file -p NoPassWordSet`

3. Perform [Copying the CA certificate to IBM Cognos servers](#).
4. Import the certificate to the truststore on IIS.

For more information about how to import the certificate to the truststore on IIS, see [Adding certificates to the Trusted Root Certification Authorities store for a local computer](#).

## Configuring IIS in Cognos Analytics

Use this information to configure Microsoft Internet Information Services (IIS) for IBM Cognos Analytics.

When complete, IIS will be configured to serve static content (such as `.js`, `.html`, `.css`) directly from IIS while sending REST and other server requests to the back-end Cognos Analytics servers.

IIS automated script is available [here](#).

### Procedure

1. Install the IIS Application Request Routing extension.
  - a) Install the Application Request Routing extension for IIS by going to the following URL: <https://www.iis.net/downloads/microsoft/url-rewrite>
  - b) When presented with the Microsoft Web Page, click on the green “Install this extension” button. Follow instructions to download and run the ARR extension.
  - c) To ensure that the ARR extension was installed successfully, launch the IIS Manager from the Windows **Start\Administrative Tools\** menu. Once the IIS Manager launches, click on the server name at the top left-hand side of the screen to display the available features. Within the middle IIS pane, the **URL Rewrite** feature should now be visible; it is installed when ARR is installed.
2. Create a new, dedicated application pool. Name it, for example, CAPool1.
  - a) Right-click **Application Pools**. Click **Add Application Pool**.
3. Optionally, create a server farm to provide load-balancing and failover for Cognos Analytics service requests. Include all Cognos Analytics servers that have the Application server components installed and configured.
  - a) Right-click on **Server Farms** in the left-hand tree and select **Create Server Farm**.

- b) Name the new server farm. For example, `ca_servers`.
  - c) For each Cognos Analytics server, perform the following steps:
    - Enter the server address. For example, `ca-host1`.
    - Click **Advanced settings**, and expand **applicationRequestRouting**. Set the `httpPort` or `httpsPort` (if you're using HTTPS). For example, `9300`.
  - d) Click **Finish**.
  - e) Click **No** when prompted to allow IIS Manager to create a rewrite rule.
  - f) Select your server farm in the left-hand tree and double-click **Server Affinity**.
  - g) Select the **Client Affinity** check box.
  - h) Click **Apply**.
  - i) Select your server farm in the left-hand tree and double-click **Caching**.
  - j) Change **Query String Support** to **Include Query String**.
  - k) Click **Apply**.
  - l) Select your server farm in the left-hand tree and double-click **Health Test**.
  - m) In the **URL Test** section, enter the URL: `http://ca_servers/bi/v1/ping`
  - n) Click **Apply**.
  - o) Select your server farm in the left-hand tree and double-click **Proxy**.
  - p) In the **Time-out (seconds)** field, change the value to `120`.
  - q) Click **Apply**.
4. Right-click **Default Web Site**, and then click **Add Application**.
    - Alias is `ibmcognos`.
    - Application pool is the one created in step 1.
    - Physical path is `install_location\webcontent`
    - a) Enable Web Content expiry.
      - i) Select `ibmcognos`, and double-click **HTTP Response Headers**.
      - ii) Click **Set Common Headers**.
      - iii) Check **Expire Web Content** and set an expiry that works best for you.
    - b) Select `ibmcognos` and double-click **Mime Types**.  
Add the following mime types to your IIS configuration if they are not already present.
      - `.svg` : `image/svg+xml`
      - `.woff` : `application/x-font-woff`
      - `.json` : `application/json`
      - `.woff2` : `font/woff2`
      - `.template` : `text/html`
      - `.txt` : `text/plain`
      - `.properties` : `text/plain`
      - `.wasm` : `application/wasm`
  5. If you are configuring single sign-on between IIS and Cognos Analytics, right-click `ibmcognos`, and click **Add Application**.
    - **Alias** to `sso`.
    - **Application pool** is the one you created in step 1.
    - **Physical path** is `install_location\cgi-bin`.
    - a) Select `sso` and double-click **Handler Mappings**.

- b) Click **Add Module Mapping** in the right **Actions** pane.
  - Request path is `cisapi`.
  - Module is **IsapiModule**.
  - Executable is `install_location\cgi-bin\cognosisapi.dll`.
  - Name is Cognos SS0.
  - Click **Request Restrictions**, and ensure that **Invoke Handler** is unchecked.
  - Click **OK** twice.
  - On the **Edit Script Map** dialog, click **Yes**.
  - Select **sso** and double-click **Modules**. If the WebDAVModule appears in the list, remove it.
6. Create URL-rewrite rules to map requests to the correct handlers.
  - a) Click on the `bi` directory under **ibmcognos**.
  - b) Double-click **URL Rewrite**.
  - c) Add a server variable to identify the Cognos Analytics location by clicking **View Server Variables**.
    - Click **Add**.
    - Name the variable `HTTP_X_BI_PATH`.
    - Click **Back to Rules**.
    - Click **View Server Variables**.
    - Click **Add**.
    - Name the variable `HTTP_X_WEBCONTENTROOT`.
    - Click **Back to Rules**.
    - Click **View Server Variables**.
    - Click **Add**.
    - Name the variable `HTTP_X_FORWARDED_HOST`.
    - Click **Back to Rules**.
    - Click **View Server Variables**.
    - Click **Add**.
    - Name the variable `HTTP_CAM_Namespace`.
    - Click **Back to Rules**.
  - d) If you want to integrate Cognos Analytics for Jupyter Notebook Server, you must add a rule to map WebSocket requests from IBM Cognos Analytics notebooks to the back-end Jupyter Notebook Server.  
  
 For more information, see [Chapter 6, “Installing IBM Cognos Analytics for Jupyter Notebook Server,” on page 45](#).  
  
**Important:** These steps use WebSocket Protocol, which is available only in IIS versions 8.0 and later.
    - i) Ensure that you have installed IIS version 8.0 or later.
    - ii) Install WebSocket Protocol support in IIS.  
  
 For more information, see [WebSocket <websocket>](https://docs.microsoft.com/en-us/iis/configuration/system.webserver/websocket) ([https://docs.microsoft.com/en-us/iis/configuration/system.webserver/web socket](https://docs.microsoft.com/en-us/iis/configuration/system.webserver/websocket)).
    - iii) Click **bi**, which is under the **ibmcognos** alias created in step 4.
    - iv) Click **Add Rules > Inbound Rules > Blank Rule**.
      - If proxies are not already enabled, you are prompted to enable them. Click **OK**.
      - The server name and port are defined in the `config.conf` file when you [configure Jupyter Notebook Server](#).

Select the newly created rule and click **Edit**.

- Pattern is `v1/jupyter/(user/[^/]*)(/api/kernels/[^/]+)/channels)`
- Action type is **Rewrite**.
- Rewrite URL (for SSL configurations) is `https://jupyter_host_name:jupyter_host_port/bi/v1/jupyter/{R:1}/{R:2}`  
For non-SSL configurations use the following rewrite URL: `http://jupyter_host_name:jupyter_host_port/bi/v1/jupyter/{R:1}/{R:2}`
- Check **Append query string**.
- Check **Stop processing of subsequent rules**.
- Click **Apply** and **Back to Rules**.

e) Re-select `bi` directory under **ibmcognos**.

f) Add a rule to pass the Cognos Analytics location to the `ca-host` machines by clicking **Add Rules > Inbound Rules > Blank Rule**.

- Name is **Headers**.
- Pattern is `(.*)`
- Action type is **none**.
- Expand **Server variables** and
  - Click **Add**. Select `HTTP_X_BI_PATH` and set the value to `/ibmcognos/bi/v1`.
  - Click **Add**. Select `HTTP_X_FORWARDED_HOST` and set the value to `{HTTP_HOST}`.
  - Click **Add**. Select `HTTP_X_WEBCONTENTROOT` and set the value to `/ibmcognos`.
- Clear **Stop processing of subsequent rules**.
- Click **Apply** and **Back to Rules**.

g) If you configured the SSO application in a previous step, add rules to map login and legacy UI service requests to the SSO handler.

i) Click **Add Rules > Inbound Rules > Blank Rule**.

- Name is **SSO Login**.
- Pattern is `v1/login$`
- Action type is **Rewrite**.
- Rewrite URL is `/ibmcognos/sso/cisapi/bi/v1/login`
- Check **Stop processing of subsequent rules**.
- Click **Apply** and **Back to Rules**.

ii) Click **Add Rules > Inbound Rules > Blank Rule**.

- Name is **Legacy SSO**.
- Pattern is `(v1/dispatch(/.*)?)`
- Action type is **Rewrite**
- Rewrite URL is `/ibmcognos/sso/cisapi/bi/{R:1}`
- Check **Stop processing of subsequent rules**.
- Click **Apply** and **Back to Rules**.

h) Add a rule to map Cognos Analytics REST service requests to the backend Cognos Analytics servers.

i) Click **Add Rules > Inbound and Outbound Rules > Reverse Proxy**.

- If proxies are not already enabled, you are prompted to enable. Click **OK**.
- Server name is `ca-host:9300/bi`

or if you have configured a server farm, `http://ca_servers/bi`

Select the newly created rule and click **Edit**.

- Pattern is `(^$)|(^v1(/.*)?)|(^[/]+\.jsp)|(^login$)|(^dashboard-print.html$)`
- Action type is **Rewrite**.
- Rewrite URL is `http://ca-host:9300/bi/{R:0}`  
or if you have configured a server farm, `http://ca_servers/bi/{R:0}`
- Check **Stop processing of subsequent rules**.
- Click **Apply** and **Back to Rules**.

ii) Click **Add Rules > Inbound Rules > Blank Rule**.

- Name is `Event Studio`.
- Pattern is `^(ags|cr1|prompting|ccl|common|skins|ps|cps4)/(.*)`
- Open the **Conditions** section.
- Change the **Logical Grouping** to **Match Any**
- Click **Add**.
  - **Condition input** is `{HTTP_REFERER}`
  - **Check if input string** is `Matches the Pattern`
  - Pattern is `v1/dispatch`
  - Check **Ignore case**.
- Click **Add**
  - **Condition input** is `{HTTP_REFERER}`
  - **Check if input string** is `Matches the Pattern`
  - Pattern is `(ags|cr1|prompting|ccl|common|skins|ps|cps4)/(.*)\.css`
  - Check **Ignore case**.
- Action type is **Rewrite**
- Rewrite URL is `/ibmcognos/{R:0}`
- Check **Stop processing of subsequent rules**.
- Click **Apply** and **Back to Rules**.

iii) Click **Add Rules > Inbound Rules > Blank Rule**

- Name is `Report Viewer`
- Pattern is `^rv/(.*)`
- Action type is **Rewrite**
- Rewrite URL is `/ibmcognos/{R:0}`
- Check **Stop processing of subsequent rules**.
- Click **Apply** and **Back to Rules**.

i) Add a rule to allow Cognos Analytics pages to load without a trailing slash in URL.

i) Click the **ibmcognos** alias.

ii) Double-click **URL Rewrite**

iii) Click **Add Rules > Inbound Rules > Blank Rule**

- Name is `Add Trailing Slash`
- Pattern is `^bi$`
- Action type is **Redirect**

- Redirect URL is {R:0}/
  - Check **Append query string**.
  - Redirect type is **Permanent (301)**
  - Click **Apply** and **Back to Rules**.
7. Adjust request size limits.
- a) Select the bi directory under the **ibmcognos** application created earlier.
  - b) Double-click **Request Filtering**.
  - c) Click **Edit Feature Settings...** from the right-hand panel.
    - Set **Maximum URL length (bytes)** to 8192.
    - Set **Maximum query string (bytes)** to 8192.
    - Click **OK**.
  - d) Double-click **Request Filtering**.
  - e) Select **Headers** tab and click **Add Header**.
  - f) In **Header Box**, type the header field name as **Referer**.
  - g) In the **Size Limit** box, type 8192.
  - h) Click **OK**.
  - i) Repeat process for a header field name entitled **Cookie** with the **Size Limit** of 4096.
  - j) Click **OK**.
  - k) Click the **ibmcognos** virtual directory.
  - l) In the **Home** view, **Management** section, double-click **Configuration Editor**.
  - m) In the **Section** drop-down list, expand **system.web**, and select **httpRuntime**.
  - n) Set the property **maxQueryStringLength** to 8192.
  - o) Apply the configuration change.
8. Configure IIS to allow to pass through the custom 441 errors that are used for recoverable exceptions from CAM. Otherwise, IIS can block these errors, and the customer sees the "Invalid Logon Response" error when trying to log on.
- a) Click the **ibmcognos** virtual directory.
  - b) In the Home view, **Management** section, double-click **Configuration Editor**.
  - c) In the **Section** drop-down list, expand **system.webServer**, and select **httpErrors**.
  - d) Set the **existingResponse** property to **PassThrough**.
  - e) Apply the configuration change.
9. If you configured the SSO application in previous steps, enable **Windows Authentication**.
- a) Select the SSO application. For Microsoft Edge browser, select the **ibmcognos** application.
  - b) Double-click **Authentication**. Disable **Anonymous Authentication**, and enable **Windows Authentication**.

Cognos Analytics should now be available at: <http://iis-host/ibmcognos/>.

**Troubleshooting:** If you are prompted repeatedly to enter your user id and password, follow these steps:

- Clear the cache of your web browser.
- Enter the Cognos Analytics URL from a different computer.
- Ensure that you type a slash (/) at the end of the Cognos Analytics URL.

**Note:** If you configured a multi level virtual directory folder above the **ibmcognos** application, such as Default Web Site > MyVirtualDirectoryFolder > **ibmcognos**, use /MyVirtualDirectoryFolder/**ibmcognos** instead of /**ibmcognos** in the URL-rewrite rules you created in Step 6.



## Configuring the CGI gateway on IIS version 7 or later

If you are using Microsoft Internet Information Services (IIS), configure the CGI gateway. This is required for single sign-on.

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

### About this task

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

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

### Procedure

1. Install the IIS Application Request Routing (ARR) extension.
  - a) Install the ARR extension for IIS by going to the following URL:  
<http://www.iis.net/downloads/microsoft/application-request-routing>
  - b) When presented with the Microsoft web page, click the green **Install this extension** button. Follow instructions to download and run the ARR extension.
  - c) To ensure that the ARR extension was installed successfully, launch the IIS Manager from the Windows **Start\Administrative Tools** menu. Once the IIS Manager launches, click on the server name at the top left-hand side of the screen to display the available features. Within the middle IIS pane, the **URL Rewrite** feature should now be visible; it is installed when ARR is installed.
2. In the Microsoft Windows **Control Panel**, click **Programs > Programs and Features**.

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

8. Under **Actions**, click **Add**.
9. Enter the path to the `cognos.cgi` file. The file is in the `install_location\cgi-bin` directory.  
You must enter the full path, including the file name. If the path includes spaces, ensure you use quotation marks around the path. For example, enter:  
"C:\Program Files\ibm\cognos\analytics\cgi-bin\cognos.cgi"
10. Enter a **Description**, such as `CognosCGI`.
11. Select **Allow extension path to execute**, and click **OK**.
12. Under **Connections**, expand **Sites**, and under your website, add the virtual directories as shown in the table:

Table 16. Required virtual directories	
Alias	Location
ibmcognos	<code>install_location/webcontent</code>
ibmcognos/cgi-bin	<code>install_location/cgi-bin</code>

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

13. Select the `cgi-bin` virtual directory that you created.
14. Double-click **Handler Mappings**.
15. Under **Actions**, click **Add Module Mapping**.
  - a) In **Request Path**, type `cognos.cgi`.
  - b) In **Module**, select `CgiModule`.
  - c) Leave **Executable (optional)** blank.
  - d) In **Name**, enter a name for the entry, such as `CognosCGI`.
  - e) Click **OK**.
16. Configure the reverse proxy.

This procedure provides the steps required to setup the reverse proxy to allow IIS to rewrite the gateway requests and pass them to the application tier. These steps assume a two server architecture where the IBM Cognos Analytics gateway is installed on `Server1_Gateway` and the IBM Cognos Analytics application is installed on `Server2_Application`

- a) On the `Server1_Gateway` server, launch IIS Manager and select the "**bi**" folder in the `ibmcognos` virtual directory set up previously.
- b) In the features view, start the **URL Rewrite** feature.
- c) Within the **Actions** pane, click on **Add Rule(s)**, and then select **Reverse Proxy**. Click **OK**.
- d) In the **Add Reverse Proxy Rule** dialog box, within the **Inbound Rules** section, fill in the **Enter the server name or the IP address...** field in the following format.  
`<Server2_Application:Port>/bi`. For example, `Server2_Application:9300/bi`
- e) Ensure the **Enable SSL Offloading** check box is checked, and then click **OK**.
- f) On the **Rules** page, in the **Action** pane, click on **View Server Variables**.
- g) Click **Add** and add a variable named `HTTP_X_BI_PATH`. Once completed, click **OK** to create the variable.
- h) Within the **Actions** pane, click **Back to Rules**.
- i) Select the previously created rule and in the **Inbound rules** pane on the right hand side, click **Edit...**
- j) Expand the **Server Variables** section.

- k) Inside the **Server Variables** section, click the **Add** button.
- l) In the **Set Server Variable** dialog, select the **HTTP\_X\_BI\_PATH** server variable and set the **Value** field to `/ibmcognos/bi/v1`
- m) Ensure the **Replace existing value** check box is checked.
- n) Click **OK** to save, and then, in the **Action** pane, click **Apply**.
- o) In the **Action** pane on the upper right, click **Back to Rules** to finish defining the rule.
- p) Test the configuration by entering the following URL pattern using a browser: `http(s)://<web_server>:<web_server_port>/<alias>/bi/`. For this example the URL would be: `http://Server1_Gateway:80/ibmcognos/bi/`.

## Results

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

## Configuring the gateway and web server to use specific namespaces

---

You can configure IBM Cognos Analytics to use the gateway namespace with all supported web servers, or configure a specific namespace for each web server.

Based on your configuration requirement, you can configure the namespaces in the following way:

- Specify the gateway namespace in IBM Cognos Configuration.

This option can be used for namespaces that are configured for single sign-on (SSO), and applies to all supported web servers. For more information, see [“Configuring a gateway namespace” on page 147](#).

- Add an HTTP header to the web server configuration.

This option can be used for namespaces that are or aren’t configured for single sign-on. The configuration steps are different for each web server. For more information, see [“Configuring a namespace to use with IIS” on page 148](#), and [“Configuring a namespace to use with Apache or IBM HTTP server ” on page 148](#).

## Configuring a gateway namespace

If IBM Cognos Analytics components use multiple namespaces, or if anonymous access is enabled and Cognos Analytics components use one namespace, you can configure the gateway to connect to one namespace.

Users logged to the web server where the gateway is located are not prompted to choose an authentication source. If you have multiple web servers, you can configure each web server to use a different namespace.

### About this task

This option can be used with namespaces that are configured for single sign-on (SSO), and applies to all supported web servers.

### Procedure

1. On the computer where the IBM Cognos Analytics gateway is installed, start IBM Cognos Configuration.
2. In the **Explorer** pane, click **Environment**.
3. In the **Properties** pane, for the **Gateway namespace** property, type the **Namespace ID** of the namespace that you want to use as a **Value** for this property.
4. From the **File** menu, click **Save**.

5. Restart your web server.

## Configuring a namespace to use with IIS

You can configure a specific Cognos Analytics namespace to use with Microsoft Internet Information Services (IIS).

### About this task

This option can be used with namespaces that are or aren't configured for single sign-on.

### Procedure

1. Follow the steps in the [“Configuring IIS in Cognos Analytics” on page 139](#) topic to configure IIS with IBM Cognos Analytics.
2. Add an HTTP header named **HTTP\_CAM\_Namespace** by using the following steps:
  - a) Click the **bi** directory under **ibmcognos**.
  - b) Double-click **URL Rewrite**.
  - c) Click **View Server Variables**, and add a server variable named **HTTP\_CAM\_Namespace** in the following way:
    - Click **Add**.
    - Name the variable **HTTP\_CAM\_Namespace**.
    - Click **Back to Rules**
  - d) Click on the rewrite rule named **Headers**, and click **Edit**.
  - e) Expand **Server variables**, and click **Add**.
    - Click **Add**.
    - Select **HTTP\_CAM\_Namespace**, and set the value to the **Namespace ID**, as specified in IBM Cognos Configuration, of the namespace that you want to use.
    - Click **Apply**, and then **Back to Rules**.
3. Restart IIS.

## Configuring a namespace to use with Apache or IBM HTTP server

You can configure a specific Cognos Analytics namespace to use with Apache HTTP Server or IBM HTTP Server.

### About this task

This option can be used with namespaces that are or aren't configured for single sign-on.

### Procedure

1. Follow the steps in the [“Configuring Apache HTTP Server or IBM HTTP Server with Cognos Analytics” on page 134](#) topic to configure Apache HTTP Server or IBM HTTP Server with IBM Cognos Analytics.
2. Add an HTTP header named **CAM-Namespace** by using the following steps:
  - a) Open the **cognos.conf** file that you configured in step 1 in a text editor.
  - b) For the **Location** parameter, add the **RequestHeader** parameter named **CAM-Namespace**, and set it to the **Namespace ID**, as specified in IBM Cognos Configuration, of the namespace that you want to use.

```
# Define cognos location
<Location /ibmcognos>
    RequestHeader set X-BI-PATH /ibmcognos/bi/v1
```

```
RequestHeader set CAM-Namespace your_namespace_id
</Location>
```

- c) Save the `cognos.conf` file, and restart the web server.

## Testing the gateway

---

You can test the installation using a web browser.

### Procedure

1. Ensure that your web server is running.
2. Open a web browser.
3. In the address field, type the **Gateway URI** from IBM Cognos Configuration. For example,

`http://host_name:port/ibmcognos`

The **Welcome** page of the IBM Cognos Analytics portal appears.



---

# Chapter 11. Installing and configuring optional modeling components

After you install and configure IBM Cognos Analytics server components, you can install and configure IBM Cognos Framework Manager, the modeling component for reporting, and IBM Cognos Transformer, the modeling tool for creating PowerCubes.

Install Framework Manager and Transformer to a different location than Cognos Analytics.

---

## IBM Cognos Framework Manager

IBM Cognos Framework Manager is the metadata modeling tool for IBM Cognos Analytics.

You can install it on the same computer as other IBM Cognos Analytics components, or on a different computer.

If you upgraded from an older version of Framework Manager, you can use the same models and projects that you used with the older version. To upgrade existing projects, you must open them in the new version of Framework Manager.

If you are upgrading Framework Manager from an older version, you must first uninstall the older version of Framework Manager. For more information, see [Chapter 16, “Uninstalling IBM Cognos Analytics,” on page 291](#).

Before you install Framework Manager, close all programs that are currently running to ensure that the installation program copies all the required files to your computer.

Also, ensure that you have administrator privileges for the Windows computer you are installing on. If you are not an administrator, ask your system administrator to add you to the Administrator group on your computer. Administrator privileges are also required for the account that is used to run Framework Manager.

Install and configure all IBM Cognos Analytics server components before you install Framework Manager.

Install to a directory that contains only ASCII characters in the path name. Some servers do not support non-ASCII characters in directory names. Installing Framework Manager in directory that has an apostrophe in the path name can result in the help not opening properly.

To help you manage, share, and secure different versions of your metadata, you can configure Framework Manager to use an external source control system. For more information, see the section about using external repository control in the *IBM Cognos Framework Manager User Guide*.

## System requirements for IBM Cognos Framework Manager

Before you install IBM Cognos Framework Manager, ensure that the Windows computer meets IBM Cognos Analytics software and hardware requirements. The size of your models determines the hardware requirements, such as disk space.

The following table lists the minimum hardware and software requirements to run Framework Manager.

Table 17. System requirement for Framework Manager	
Requirement	Specification
Operating system	Windows
RAM	Minimum: 512 MB Optimal: 1 GB

Table 17. System requirement for Framework Manager (continued)

Requirement	Specification
Disk space	Minimum: 500 MB of free space on the drive that contains the temporary directory that is used by Cognos Analytics.
Database	If you use the compatible query mode (CQM), the database client software must be installed on the same computer as Framework Manager.  Database connectivity must be set up.
Other	Microsoft Data Access Component (MDAC) 2.6 or later for use with product samples.

To help you manage, share, and secure different versions of your metadata, you can configure Framework Manager to use an external source control system. For more information, see the section about using external repository control in the *Framework Manager User Guide*.

To review an up-to-date list of environments that are supported by IBM Cognos Analytics products, see the [IBM Software Product Compatibility Reports page](http://www.ibm.com/support/pages/node/735235) (www.ibm.com/support/pages/node/735235).

## Installing IBM Cognos Framework Manager

For a complete installation of IBM Cognos Analytics, you must install Cognos Framework Manager on a Windows computer.

The installation location must be different than the IBM Cognos Analytics installation location.

### Procedure

1. Go to the location where the installation files were downloaded and extracted, and double-click the `installer.exe` file.
2. Point to appropriate repository and select **IBM Cognos Analytics Tools** and select **IBM Cognos Framework Manager**.
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.
5. Secure the installation directory from unauthorized access.

### What to do next

Default settings are used for the configuration. You can change these default settings during the installation or later, to better suit your environment.

## Configuring IBM Cognos Framework Manager

You must configure IBM Cognos Framework Manager to communicate with IBM Cognos Analytics and its components.

### Before you begin

Install and configure IBM Cognos Analytics before you configure Framework Manager. You must first install and configure Content Manager, and start the **IBM Cognos** service on at least one Content Manager



computer. This ensures that the certificate authority service issues a certificate to the Framework Manager computer.

You also need to configure the data sources that you plan to use in Framework Manager projects.

## About this task

If you install Framework Manager on the same computer as IBM Cognos Analytics (to a different directory), configuration is not required if the following conditions apply:

- Web server is configured to use the default virtual directories.
- Default ports, resources, and cryptographic settings are used.

When Framework Manager is installed outside the network firewall that protects the application tier components, communication issues with the dispatcher can arise. To avoid such issues, you can either install Framework Manager with the application tier components or install and configure a gateway that is dedicated to Framework Manager - dispatcher communications. For more information, see [“Configuring Framework Manager inside the network firewall” on page 153](#) or [“Configuring Framework Manager outside the network firewall” on page 154](#).

**Note:** If you receive the following error message, when testing after a fresh install or upgrade, save the configuration first and then test the configuration.

```
[Subject Alternative Name test] [ ERROR ] CAM-CRP-1655 Member coordination host
in Configuration Group is not configured properly. The host name must be configured
in one of the following ways:
- It must match the Subject Alternative Name DNS names or IP addresses
under the Cryptography configuration section.
- If Subject Alternative Name is not configured in Cryptography configuration, then it
must match the server common name.
```

## Procedure

1. On the computer where you installed Framework Manager, start IBM Cognos Configuration that is installed with Framework Manager.
2. In the **Explorer** pane, click **Environment**.
3. Specify appropriate values for the following settings, where the *ca\_server* placeholder represents the Cognos Analytics server.

### Gateway URI

Default: `http://ca_server:port/bi/v1/dispatch`

Example: `http://my_ca_server:9300/bi/v1/dispatch`

This URI must always be the same as for Cognos Analytics.

### Dispatcher URI for external applications

Default: `http://ca_server:port/bi/api/soap`

Example: `http://my_ca_server:9300/bi/api/soap`

If the URIs contain **localhost**, replace **localhost** with a fully-qualified host name or IP address.

4. From the **File** menu, click **Save**.

## Results

Framework Manager is configured to communicate with IBM Cognos Analytics.

## Configuring Framework Manager inside the network firewall

Use the following steps to set up communication between Framework Manager and IBM Cognos Analytics components when Framework Manager is installed inside a network firewall.

## About this task

You must specify fully qualified host names in the values for the following Cognos Configuration fields. Each value you specify must also appear in either the field **Subject Alternative Name > DNS names** or the field **Subject Alternative Name > IP addresses**.

- **Environment**
  - **Gateway URI**
  - **External dispatcher URI**
  - **Internal dispatcher URI**
  - **Dispatcher URI for external applications**
  - **Content Manager URIs**
- **Environment > Configuration Group**
  - **Group contact host**
  - **Member coordination host**
- **Security > Cryptography > Cognos**
  - **Server common name**
  - **Subject Alternative Name > DNS names**
  - **Subject Alternative Name > IP addresses**

## Procedure

1. On the computer where you installed Framework Manager, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, for the **Gateway URI**, type the appropriate value.  
Use the HTTPS or HTTP protocol to select SSL or non-SSL communication.
4. Change the host name portion of the **Gateway URI** from localhost to either the IP address or the host name of the computer where the Gateway component is installed.
5. Specify the value for the **Dispatcher URI for external applications** by typing the URI of the server where Application Tier Components are installed. For more information about this parameter, see [“Configuring IBM Cognos Framework Manager” on page 152](#).
6. In the **Explorer** window, under **Cryptography**, click **Cognos**, the default cryptographic provider.
7. Under the **Certificate Authority settings** property group, for the **Password** property, type the same password that you configured on the default active Content Manager computer.
8. From the **File** menu, click **Save**.

## Configuring Framework Manager outside the network firewall

When Framework Manager is installed outside the network firewall, you can install and configure a gateway that is dedicated to communications with the dispatcher.

## Procedure

1. [Set up a dedicated gateway](#) for Framework Manager.
2. On the gateway computer, open IBM Cognos Configuration, and change the property **Dispatcher URIs for gateway**. For more information about this parameter, see [“Configuring IBM Cognos Framework Manager” on page 152](#).
3. On the Framework Manager computer, start IBM Cognos Configuration.
4. In the **Explorer** window, click **Environment**.
5. In the **Properties** window, for **Gateway URI**, type the appropriate value for the server that you are using as the dedicated gateway.

- If your web server is configured for the ISAPI gateway, replace `cognos.cgi` with `cognosisapi.dll`.
  - If your web server is configured to use Apache modules, use the following syntax:  
`http://host_name:port/ibmcognos/cgi-bin/module_alias`
6. Change the localhost portion of the **Gateway URI** to either the IP address or the host name of the dedicated gateway server.
  7. For the **Dispatcher URI for external applications**, type the URI that is specified for **Internal dispatcher URI** on the server where application tier components are installed.  
For more information about this parameter, see [“Configuring IBM Cognos Framework Manager” on page 152](#).
  8. In the **Explorer** window, under **Cryptography**, click **Cognos**, the default cryptographic provider.
  9. Under the **Certificate Authority settings** property group, for the **Password** property, type the same password that you configured on the default active Content Manager computer.
  10. From the **File** menu, click **Save**.

## Results

Framework Manager is configured to communicate with IBM Cognos Analytics and its components.

## Configuring authentication using WebView2

Cognos Analytics Framework Manager 12.0.2 and later supports using Microsoft Edge WebView2 for authentication through a feature flag. Enabling this feature flag allows Framework Manager to be compatible with newer web standards when you authenticate with the Cognos Analytics server.

To use WebView2 for authentication in Framework Manager version 12.0.2 or later, follow these steps:

1. Download and install [Microsoft Edge WebView2 Runtime](https://developer.microsoft.com/en-us/microsoft-edge/webview2/) (https://developer.microsoft.com/en-us/microsoft-edge/webview2/).
- Note:** WebView2 might already be installed on your computer. To check if you have WebView2 Runtime installed, go to **Apps & features** (Start > Settings > Apps) and search for WebView2.
2. Enable WebView2.
    - a. Go to `installation_location\configuration`
    - b. Open `fm.ini` in a text editor.
    - c. In the `webview2` section, change this text:

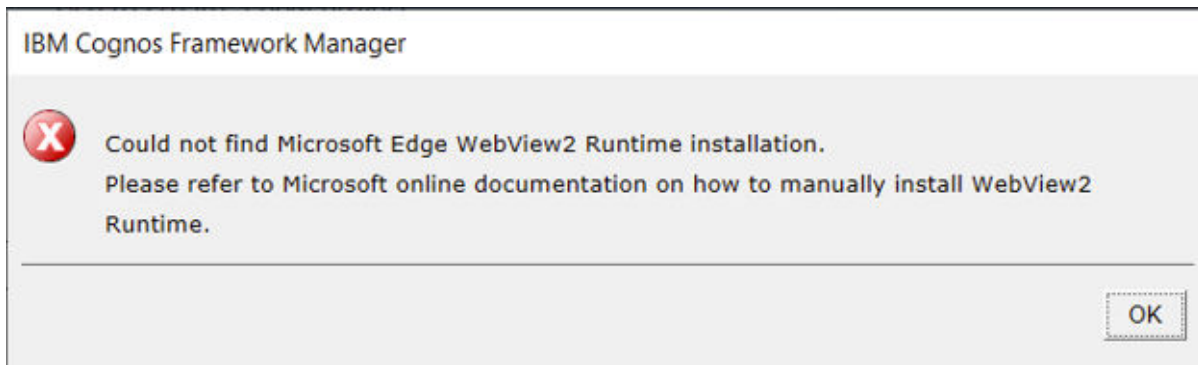
```
<Preference Name="logonPage">FALSE</Preference>
```

to this text:

```
<Preference Name="logonPage">TRUE</Preference>
```

3. Restart Framework Manager if it is open.

If you do not have WebView2 Runtime installed on your computer and you enable WebView2 in Framework Manager, the following message appears:



Click **OK** and install the appropriate Microsoft Edge WebView2 Runtime to use WebView2.

## Setting variables for data source connections for Framework Manager

The IBM Cognos Analytics modeling tools create and manage metadata. Framework Manager creates and manages metadata for the reporting functions. Because metadata is derived from data sources in multi-platform or multilingual environments, there are several things you must think about or do when you set up the data source environment for Framework Manager. Commonly, these things depend on the other technology you use for your data or import source.

If you upgraded from an older version of Framework Manager, you are not required to set up anything in the data source environment. You must set up the data source environment only if you installed Framework Manager in a different location from the older version.

Users operating in different languages can connect to an MSAS 2005 data source from the same instance of IBM Cognos Analytics. Modelers must create a separate package for each language. Users can run reports in any language.

For more information about data source connections, see the *IBM Cognos Administration and Security Guide*.

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.

Perform the following steps in the location where you installed Framework Manager.

### Procedure

1. Set the environment variable for multilingual support:

- For Oracle, set the **NLS\_LANG** (National Language Support) environment variable on each computer where Framework Manager and IBM Cognos Analytics server are installed by typing the following command:

```
NLS_LANG = language_territory.character_set
```

Examples are:

```
NLS_LANG = AMERICAN_AMERICA.UTF8
```

```
NLS_LANG = JAPANESE_JAPAN.UTF8
```

The value of the variable determines the locale-dependent behavior of IBM Cognos Analytics. Error messages, sort order, date, time, monetary, numeric, and calendar conventions automatically adapt to the native language and locale.

- For IBM Db2, set the **DB2CODEPAGE** environment variable to a value of 1252.

For more information about whether to use this optional environment variable, see the Db2 documentation.

No settings are required for SAP BW. SAP support only a single code page on non-Unicode SAP BW systems.

2. For Oracle, add \$ORACLE\_HOME/lib to your **LD\_LIBRARY\_PATH** variable.

When you set the load library paths, ensure that the 32-bit Oracle libraries are in the library search path, which is usually the \$ORACLE\_HOME/lib directory or the \$ORACLE\_HOME/lib32 directory if you installed a 64-bit Oracle client.

3. For SAP BW, configure the following authorization objects so that the modeling tool can retrieve metadata.

Where default values are specified, you may want to modify the values on the SAP system.

- **S\_RFC**

Set the **Activity** field to **16**.

Set the **Name of RFC to be protected** field to **SYST, RSOB, SUGU, RFC1, RS\_UNIFICATION, RSAB, SDTX, SU\_USER**.

Set the **Type of RFC object to be protected** field to **FUGR**.

- **S\_TABU\_DIS**

Set the **Activity** field to **03**.

Set the **Authorization Group** field to **&NC&**.

**Note:** **&NC&** represents any table that does not have an authorization group. For security reasons, create an authorization group and assign the table **RSHIEDIR** to it. The new authorization group restricts the user's access to the table only, which is needed by the modeling tool. Create the authorization group as a customization in the SAP system.

- **S\_USER\_GRP**

Set the **Activity** field to **03, 05**.

Set the **User group in user master main** field to the default value.

- **S\_RS\_COMP**

Set the **Activity** field to the default value.

Set the **Info Area** field to *InfoArea Technical Name*.

Set the **Info Cube** field to the value: *InfoCube Technical Name*.

Set the **Name (ID) of reporting components** field to the default value.

Set the **Type of reporting components** field to the default value.

- **S\_RS\_COMP1**

Set the **Activity** field to the default value.

Set the **Name (ID) of reporting components** field to the default value.

Set the **Type of reporting components** field to the default value.

Set the **Owner (Person Responsible)** field to the default value.

- **S\_RS\_HIER**

Set the **Activity** field to **71**.

Set the **Hierarchy Name** field to *Hierarchy Name*.

Set the **InfoObject** field to *InfoObject Technical Name*.

Set the **Version** field to *Hierarchy Version*.

- **S\_RS\_ICUBE**

Set the **Activity** field to **03**.

Set the **InfoCube sub-object** field to the values **DATA** and **DEFINITION**.

Set the **Info Area** field to *InfoArea Technical Name*.

Set the **InfoCube** field to *InfoCube Technical Name*.

For more information about SAP BW authorization objects, see Transaction SU03.

## Testing the Framework Manager installation

You can test your configuration by starting the application and creating a project.

### Procedure

To start Framework Manager, from the **Start** menu, click **All Programs > IBM Cognos Framework Manager > .**

On Microsoft Windows 2012 Server, double-click the **Framework Manager** icon on the **Start** panel.

You may be prompted to upgrade if the model schema version is older than the currently supported version.

If you see the **Welcome** page of Framework Manager, your installation is working.

## IBM Cognos Transformer

IBM Cognos Transformer is the metadata modeling tool for creating PowerCubes for use with IBM Cognos products.

Transformer can be made available more easily for business specialists who want to design models and build PowerCubes for their own use. For example, IT departments can provide business specialists or Transformer modelers with a Web-based, downloadable installation program from a corporate or secured portal, allowing for easy distribution of the installation files.

Transformer consists of the following components:

- UNIX and Linux operating system utility for building PowerCubes
- IBM Cognos Transformer client

This component must be installed on a Windows computer.

Both components must be installed to a different location than IBM Cognos Analytics.

Default settings are used for the configuration. You can change these default settings if necessary. However, the settings must be the same as for IBM Cognos Analytics.

## System requirements for Cognos Transformer

Before you install IBM Cognos Transformer, ensure that the computer meets software and hardware requirements. The size of your PowerCubes determines the hardware requirements, such as disk space.

The following table lists the minimum hardware and software requirements to run IBM Cognos Transformer.

Table 18. System requirements for Transformer	
Requirement	Specification
Operating system	Windows UNIX: IBM AIX Linux

Table 18. System requirements for Transformer (continued)	
Requirement	Specification
RAM	Minimum: 512 MB Optimal: 4 GB
Disk space	Minimum: 500 MB of free space on the drive that contains the temporary directory
Data source	Database client software installed on the same computer as IBM Cognos Transformer Database connectivity set up
Other	Microsoft Visual C++ Redistributable 2015-2022 or later (both the x86 and x64 versions) <b>Note:</b> If you don't install Microsoft Visual C++ + Redistributable 2015-2022 or later, Cognos Configuration will produce error messages and configuration cannot be completed. Microsoft Data Access Component (MDAC) 2.6 or later for use with product samples

## Installing IBM Cognos Transformer

Install IBM Cognos Transformer if you plan to create PowerCubes for use with IBM Cognos products.

The Transformer installation location must be different than the IBM Cognos Analytics installation location.

The Cognos Analytics server components must be installed and configured before you install Transformer.

The language that you select in the installation wizard determines the language of the user interface for both the installation wizard and for IBM Cognos Transformer. All available languages are installed.

With a UNIX or Linux operating system, the installation of IBM Cognos Transformer is not complete until you also install IBM Cognos Transformer on a computer with a Microsoft Windows operating system. All components are installed in both environments and you then use the features and tools that are appropriate for each environment. For example, the IBM Cognos Transformer client provides a graphical user interface for designing models on Windows computers. You then build cubes on your UNIX or Linux computer. Models that contain an IQD data source are not supported on Linux.

Install in a directory that contains only ASCII characters in the path name. Some servers do not support non-ASCII characters in directory names.

Before you install IBM Cognos Transformer, close all programs that are currently running to ensure that the installation program copies all the required files to your computer.

If you are installing on Windows, ensure that you have administrator privileges for the Windows computer you are installing on. If you are not an administrator, ask your system administrator to add you to the Administrator group on your computer.

## Installing IBM Cognos Transformer on Unix and Linux operating systems

Use the following steps to install IBM Cognos Transformer on UNIX or Linux operating systems.

### Procedure

1. Download the installer executable and repository zip files from [Passport Advantage](#).

2. Double-click the installer executable.
3. Follow the directions in the installation wizard to copy the required files to your computer.
4. In the **Install Complete** page of the installation wizard, click **Done**.

## What to do next

For information about the syntax for UNIX command line options that are supported by IBM Cognos Transformer, see *Transformer Unix Commands*.

The man page for IBM Cognos Transformer is accessible in UNIX by typing `cogtr man` from the `install_location/bin64` directory.

## Installing IBM Cognos Transformer on Windows operating systems

Use the following steps to install IBM Cognos Transformer on Microsoft Windows operating systems.

### Procedure

1. Download the installer executable and repository zip files from [Passport Advantage](#).
2. Double-click the installer executable.
3. Follow the directions in the installation wizard to copy the required files to your computer.
4. In the **Install Complete** page of the installation wizard, click **Done**.

## What to do next

To configure Transformer, start IBM Cognos Configuration.

## Configuring Transformer authentication using WebView2

Cognos Analytics Transformer 12.0.3 and later supports using Microsoft Edge WebView2 for authentication through a feature flag. Enabling this feature flag (it is disabled by default) allows Transformer to be compatible with newer web standards when you authenticate with the Cognos Analytics server.

To use WebView2 for authentication in Transformer version 12.0.3 or later, follow these steps:

1. Download and install [Microsoft Edge WebView2 Runtime](https://developer.microsoft.com/en-us/microsoft-edge/webview2/) (https://developer.microsoft.com/en-us/microsoft-edge/webview2/).

**Note:** WebView2 might already be installed on your computer. To check if you have WebView2 Runtime installed, go to **Apps & features** (Start > Settings > Apps) and search for WebView2.

2. Enable WebView2.
  - a. Go to `installation_location\configuration`
  - b. Open `cogtr.xml` in a text editor.
  - c. In the Transformer section, change this text:

```
<Preference Name="UseWebView" Value="0"/>
```

to this text:

```
<Preference Name="UseWebView" Value="1"/>
```

3. Restart Transformer if it is open.

If you do not have WebView2 Runtime installed on your computer and you enable WebView2 in Transformer, an error message appears. Click **OK** and install the appropriate Microsoft Edge WebView2 Runtime to use WebView2.



## Setting up data sources for Transformer

IBM Cognos Transformer creates and manages metadata for PowerCubes. The metadata is derived from data sources in multi-platform or multilingual environments.

There are several things you must consider when you set up the data source environment for IBM Cognos Transformer. Commonly, these things depend on other technology you use for your data or import source.

If users operating in different languages connect to a Microsoft Analysis Services (MSAS) 2000 data source, you must create a separate IBM Cognos Analytics instance for each language.

Users operating in different languages can connect to an MSAS 2005 data source from the same instance of IBM Cognos Analytics. Modelers must create a separate package for each language. Users can run reports in any language.

For more information about data source connections, see the *IBM Cognos Analytics Administration and Security Guide*.

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.

Use the following steps to set up Oracle or SAP BW data sources for IBM Cognos Transformer.

### Procedure

1. Set the environment variable for multilingual support:

- For Oracle, set the **NLS\_LANG** (National Language Support) environment variable on each computer where Framework Manager and IBM Cognos Analytics server are installed by typing the following command:

```
NLS_LANG = language_territory.character_set
```

Examples are:

```
NLS_LANG = AMERICAN_AMERICA.UTF8
```

```
NLS_LANG = JAPANESE_JAPAN.UTF8
```

The value of the variable determines the locale-dependent behavior of IBM Cognos Analytics. Error messages, sort order, date, time, monetary, numeric, and calendar conventions automatically adapt to the native language and locale.

- For IBM Db2, set the **DB2CODEPAGE** environment variable to a value of 1252.

For more information about whether to use this optional environment variable, see the Db2 documentation.

No settings are required for SAP BW. SAP support only a single code page on non-Unicode SAP BW systems.

2. For Oracle, add \$ORACLE\_HOME/lib to the library path.

When you set the load library paths, ensure that the 32-bit Oracle libraries are in the library search path, which is usually the \$ORACLE\_HOME/lib directory or the \$ORACLE\_HOME/lib32 directory if you installed a 64-bit Oracle client.

3. For SAP BW, configure the following authorization objects so that the modeling tool can retrieve metadata.

Where default values are specified, you may want to modify the values on the SAP system.

- **S\_RFC**

Set the **Activity** field to **16**.

Set the **Name of RFC to be protected** field to **SYST, RSOB, SUGU, RFC1, RS\_UNIFICATION, RSAB, SDTX, SU\_USER**.

Set the **Type of RFC** object to be protected field to **FUGR**.

- **S\_TABU\_DIS**

Set the **Activity** field to **03**.

Set the **Authorization Group** field to **&NC&**.

**Note:** **&NC&** represents any table that does not have an authorization group. For security reasons, create an authorization group and assign the table **RSHIEDIR** to it. The new authorization group restricts the user's access to the table only, which is needed by the modeling tool. Create the authorization group as a customization in the SAP system.

- **S\_USER\_GRP**

Set the **Activity** field to **03, 05**.

Set the **User group in user master main** field to the default value.

- **S\_RS\_COMP**

Set the **Activity** field to the default value.

Set the **Info Area** field to *InfoArea Technical Name*.

Set the **Info Cube** field to the value: *InfoCube Technical Name*.

Set the **Name (ID) of reporting components** field to the default value.

Set the **Type of reporting components** field to the default value.

- **S\_RS\_COMP1**

Set the **Activity** field to the default value.

Set the **Name (ID) of reporting components** field to the default value.

Set the **Type of reporting components** field to the default value.

Set the **Owner (Person Responsible)** field to the default value.

- **S\_RS\_HIER**

Set the **Activity** field to **71**.

Set the **Hierarchy Name** field to *Hierarchy Name*.

Set the **InfoObject** field to *InfoObject Technical Name*.

Set the **Version** field to *Hierarchy Version*.

- **S\_RS\_ICUBE**

Set the **Activity** field to **03**.

Set the **InfoCube sub-object** field to the values **DATA** and **DEFINITION**.

Set the **Info Area** field to *InfoArea Technical Name*.

Set the **InfoCube** field to *InfoCube Technical Name*.

For more information about SAP BW authorization objects, see Transaction SU03.

## Configuring communication between Transformer and Cognos Analytics

You must configure IBM Cognos Transformer to communicate with IBM Cognos Analytics.

### Before you begin

Install and configure IBM Cognos Analytics components before you configure IBM Cognos Transformer. You must first install and configure Content Manager and start the **IBM Cognos** service on at least one Content Manager computer before you configure IBM Cognos Transformer. This ensures that the certificate authority service issues a certificate to the IBM Cognos Transformer computer.

To support the use of IBM Cognos Analytics data sources (including packages and reports) in Transformer, ensure that the database client is installed on the computer where Transformer is installed.

When Transformer is outside a network firewall that protects the application tier components, communication issues with the dispatcher can arise. To avoid such issues, you can install Transformer in the same architectural tier as the application tier components or you can install and configure a gateway that is dedicated to Transformer communications. For more information, see [“Firewall considerations” on page 67](#).

If you are using a dedicated gateway, you must also configure the gateway computer. For more information, see [Chapter 10, “Configuring the gateway,” on page 123](#).

## About this task

The instructions in this topic are for the installer or administrator. If you are the Transformer modeler or business specialist who wants to download and use Transformer, see [“Deploying IBM Cognos Transformer for Modelers” on page 165](#).

If IBM Cognos Analytics was installed in more than one location, ensure that all URIs point to the correct version of IBM Cognos Analytics.

## Procedure

1. On the computer where you installed IBM Cognos Transformer, start IBM Cognos Configuration.
2. In the **Explorer** pane, click **Environment**.
3. Specify appropriate values for the following settings, where the *ca\_server* placeholder represents the Cognos Analytics server:

### Gateway URI

Default: `http://ca_server:port/bi/v1/disp`

Example: `http://my_ca_server:9300/bi/v1/disp`

This URI must always be the same as for Cognos Analytics.

### Dispatcher URI for external applications

Default: `http://ca_server:port/bi/api/soap`

Example: `http://my_ca_server:9300/bi/api/soap`

If the URIs contain **localhost**, replace **localhost** with a fully-qualified host name or IP address.

4. From the **File** menu, click **Save**.

## Results

IBM Cognos Transformer is configured to communicate with IBM Cognos Analytics.

## Testing the Transformer installation

You can test your configuration by starting the application and creating a model.

## Procedure

To start IBM Cognos Transformer, from the **Start** menu, go to programs and click **IBM Cognos Transformer**.

On Microsoft Windows 2012 Server, double-click the **IBM Cognos Transformer** icon on the **Start** panel.

To start IBM Cognos Transformer manually, double-click the `cogtr.exe` file in the `install_location\bin` directory.

If you see the **Transformer** window, your installation is working.

## Additional configuration tasks for Cognos Transformer

The tasks in this section apply to Cognos Transformer modelers.

To make Transformer available for modelers to install and use, perform the following tasks:

- [Create a network installation location for Transformer modelers](#)
- [Export configuration data for Transformer modelers](#)
- [Deploy IBM Cognos Analytics Transformers for modelers](#)

### Create a Network Installation Location for Transformer Modelers

Your organization may have specialized business or power users who want to build PowerCubes that are modeled on a combination of corporate and personal data sources. These users may want to do their own analysis of the data for their line of business or a small group of users. An installer or administrator can download an executable file to a Web or LAN location, where modelers can run the file to launch the IBM Cognos Transformer installation wizard.

The instructions in this topic are for the installer or administrator. If you are the Transformer modeler or business specialist who wants to download and use Transformer, see [“Deploying IBM Cognos Transformer for Modelers”](#) on page 165

### Before you begin

Before you make the installation file available to Transformer modelers, other resources and permissions must be set up:

- Database client software is installed, or available for modelers to install, on the Transformer computers that are used to access IBM Cognos Analytics data sources.
- Modelers must have privileges to create a data source in IBM Cognos Administration.

Modelers do not need direct access to IBM Cognos Administration. They can create and update data sources by using Transformer or command line tools. You can provide modelers with a secured folder in the portal in which to publish PowerCube packages.

- Modelers must have access to a location in which to store the PowerCube after building it.

This location must also be accessible to the IBM Cognos service and can be a secured share on a LAN.

- To build PowerCubes on a specific Transformer server, modelers should have FTP privileges to transfer models and execute privileges to build cubes on that server.

Modelers can transfer models and execute cube builds using scripts. Modelers can also use automated methods to build PowerCubes. For more information, see the *Administration and Security Guide*.

### Procedure

1. Insert the disk for IBM Cognos Transformer modeling product.
2. If the **Welcome** page of the installation wizard appears, exit the wizard.
3. On the disk, locate the C8transformerinstall.exe file.
4. Copy the file to a secure location to which your Transformer modelers have access.

### Configuration data for Transformer modelers

If you want to make the Transformer installation file available to Transformer modelers, the modelers will need the dispatcher and encryption settings to configure Transformer on their local computer.

You can export the configuration from one Transformer computer for use with all other Transformer computers. The modelers can copy the exported configuration file to their Transformer installation directory and then run the command to configure the Transformer computer silently.

The instructions in this topic are for the installer or administrator. If you are the Transformer modeler or business specialist who wants to download and use Transformer, see [“Deploying IBM Cognos Transformer for Modelers”](#) on page 165.

If you updated the coglocale, cogtr.xml, or cs7g.ini files on the Transformer computer, you must copy these files to the Web or LAN location so that Transformer modelers can download them to their computer.

To export the configuration, the source computer must have the same IBM Cognos Analytics components as the Transformer modeler computers [“Configuring communication between Transformer and Cognos Analytics”](#) on page 162.

### ***Exporting the Transformer configuration***

Use IBM Cognos Configuration to export the configuration from one Transformer computer for use with all other Transformer computers.

#### **Procedure**

1. In IBM Cognos Configuration, from the **File** menu, click **Export as**.
2. If you want to export the current configuration to a different folder, in the **Look in** box, locate and open the folder.  
  
Ensure that the folder is protected from unauthorized or inappropriate access.
3. In the **File name** box, type a name for the configuration file.
4. Click **Save**.
5. Rename the exported file to cogstartup.xml.
6. Copy the exported cogstartup.xml file from the source computer to the same Web or LAN location as the Transformer installation file.
7. If you changed the global configuration on the source computer, copy the coglocale.xml file from the source computer to the same Web or LAN location as the Transformer installation file.

The default location of the coglocale.xml file is *install\_location/configuration*.

### ***Copying updated Transformer configuration files***

If you updated certain configuration files, you must copy them to the same location as the Transformer installation file.

#### **Procedure**

1. If you updated the cogtr.xml, copy it from the *install\_location/configuration* directory to the same Web or LAN location as the Transformer installation file.
2. If you updated the cs7g.ini file, copy it from the *install\_location/CS7Gateways/bin* directory to the same Web or LAN location as the Transformer installation file.

## **Deploying IBM Cognos Transformer for Modelers**

If you are the business specialist or Transformer modeler, you must now deploy Transformer so that you can build PowerCubes and publish them to selected users or groups.

If you have not completed the installation, follow the [steps to install Transformer](#). To configure Transformer so that it can communicate with the IBM Cognos Analytics dispatcher, follow the [steps to configure Transformer](#).

To support the use of IBM Cognos Analytics data sources (including packages and reports) in Transformer, ensure that the database client is installed on the Transformer computer.

### ***Installing Transformer***

As a business specialist or Transformer modeler, use the following steps to install Transformer from the Web or LAN location that the administrator provided.

## Procedure

1. From the Web or LAN location that the administrator provided, run the C8transformerinstall.exe file.
2. Follow the directions in the installation wizard and copy the required files to your computer.

**Tip:** The Series 7 IQD Bridge component is not supported on Linux.

3. In the **Finish** page of the wizard, click **Finish**.

## What to do next

The *IBM Cognos Transformer UNIX Commands Guide* provides the syntax for UNIX command line options that are supported by Cognos Transformer. You can access this document in [IBM Cognos Analytics Knowledge Center](http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0) (www.ibm.com/support/knowledgecenter/SSEP7J\_11.0.0).

## Configuring Transformer

As a business specialist or Transformer modeler, use the following steps to configure Transformer.

## Procedure

1. Go to the same Web or LAN location as the Transformer installation file.
2. If any .xml files are present, copy them to the *Transformer\_location*\configuration directory, where *Transformer\_location* is the directory where you installed Transformer.
3. If an .ini file is present, copy it to the *Transformer\_location*\CS7Gateways\bin directory.
4. Go to the *Transformer\_location*\bin directory.
5. Type the configuration command:

```
./cogconfig.bat -s
```

IBM Cognos Configuration applies the configuration settings specified in the local copy of cogstartup.xml, encrypts credentials, generates digital certificates, and starts the IBM Cognos services.

6. To test IBM Cognos Transformer, from the **Start** menu, go to programs and click **IBM Cognos Transformer**.

If you see the **Transformer** window, your installation is working.

7. After Transformer is installed and running successfully, delete the installation files that were extracted from the installation file.

---

## Chapter 12. Configuration options

After you install and configure IBM Cognos components, you can change the configuration for your environment. Initially, default property settings are used to configure the components. However, you can change these default settings if existing conditions make the default choices inappropriate, or to better suit your environment.

For example, you can configure features for IBM Cognos Application Firewall or specify the amount of resources that IBM Cognos components use. Also, you can deliver IBM Cognos content using another portal by configuring Portal Services.

You can configure IBM Cognos components to use other resources, such as using an authentication provider and then enabling single signon for the database connection and the users.

If you use a load-balancing scheme in your environment, you can change settings to improve performance. For example, you can balance requests among dispatchers by changing their processing capacity or by setting the minimum and maximum number of processes and connections. For more information about tuning server performance, see the *Administration and Security Guide*.

For all Microsoft Windows operating system and most UNIX and Linux operating system installations, use IBM Cognos Configuration to configure your settings. However, if the console attached to the UNIX or Linux computer on which you are installing IBM Cognos components does not support a Java-based graphical user interface you must manually edit the `cogstartup.xml` file in the `install_location/configuration` directory, and then run IBM Cognos Configuration in silent mode.

Use these optional configuration tasks to customize your configuration so that IBM Cognos components easily integrate into your existing environment.

---

### Start IBM Cognos Configuration

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

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

You should start IBM Cognos Configuration in the last page of the installation wizard on Microsoft Windows, UNIX, or Linux operating systems only if additional setup is not required. For example, if you use a database server other than Microsoft SQL for the content store, copy the JDBC drivers to the appropriate location before you start the configuration tool.

To start IBM Cognos Configuration on a Windows computer,

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

To start IBM Cognos Configuration on a UNIX or Linux computer,

- Go to the `install_location/bin` directory and then type  
`./cogconfig.sh`

---

### Critical configuration actions to take first!

These configuration actions are critical to the success of your installation. Take these actions after you install the components.

#### Ensure that JDBC drivers are in the correct location

For the IBM Cognos Analytics 11.1.x release, the JDBC drivers must be copied to the `install_location/drivers` directory.

The use of `install_location\webapps\p2pd\WEB-INF\lib` for JDBC drivers is not supported.

## Replace the JSQL driver for Microsoft SQL Server with the Microsoft JDBC driver

Starting with IBM Cognos Analytics version 11.0.5, the JSQL driver for Microsoft SQL Server has been replaced with the Microsoft JDBC driver. You must download and place the required JAR file in the *install\_location\drivers* directory. For more information, see [Set up for a Microsoft SQL Server content store](#).

## Specify the Configuration Group property

If you used the **Custom** installation to install IBM Cognos Analytics, open IBM Cognos Configuration and set the **Configuration Group** property. For more information, see [Managing the Configuration Group](#).

## Enable or disable web-based modeling

By default, JDBC data source connections that were created in IBM Cognos Administration are not exposed in the **Manage > Data servers** administration interface for use in data modules. If you want to use your existing (upgraded) data source connections to create data modules, you must enable web-based modeling on those connections.

Some data sources are inappropriate to use as sources for creating data modules. In this case, you can prohibit the use of web-based modeling on the data source connections.

To enable or disable web-based modeling for your data source connections, perform the following steps:

1. In IBM Cognos Analytics, go to **Manage > Administration console**.
2. In IBM Cognos Administration, on the **Configuration** tab, select **Data source connections**.
3. Locate the data source, and click its **Set properties** action.
4. On the **Connection** tab, select or clear the **Allow web-based modeling** check box.

## Changing the version of Java used by IBM Cognos Analytics components

---

IBM Cognos Analytics components require a Java Runtime Environment (JRE) to operate.

You can change the Java version in situations where you want to use IBM Cognos Analytics components with an application server that requires a specific JRE version or you already use a JRE version with other applications. You change Java versions by setting the JAVA\_HOME environment variable.

### JAVA\_HOME

Set a JAVA\_HOME environment variable if you want to use your own Java.

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

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

To verify that your JRE is supported, see the [IBM Cognos Analytics on Premises 12.0.x Supported Software Environments](https://www.ibm.com/support/pages/node/6966712) (<https://www.ibm.com/support/pages/node/6966712>).

### Unrestricted JCE Policy File

JREs include a restricted policy file that limits you to certain cryptographic algorithms and cipher suites. If you require a wider range of cryptographic algorithms and cipher suites, unrestricted (unlimited) policy files are now provided by default. They can be found here:

- `install_location\ibm-jre\jre\lib\security\policy\unlimited\US_export_policy.jar`
- `install_location\ibm-jre\jre\lib\security\policy\unlimited\local_policy.jar`



In addition, for Java that is provided by IBM, the unrestricted JCE policy files are also available [here](#).

## Steps

1. Launch Cognos Configuration.
2. Click **File** > **Export As...** and export the configuration to a text file such as `export_cogstartup.xml` in the configuration folder. Exit Cognos Configuration.
3. Backup the following files and folders:
  - **Files**
    - `install_location/configuration/cogstartup.xml`
    - `install_location/configuration/caSerial`
  - **Folders**
    - `install_location/configuration/csk`
    - `install_location/configuration/certs`
4. Remove the folders and files you backed up, **except** the folder `install_location/configuration/certs/mobile`. Remove all of the other files in the `install_location/configuration/certs` folder.
5. Rename the configuration backup file you created in **step 2** to `cogstartup.xml`.
6. Set the `JAVA_HOME` system environment variable to the JRE you want to use.
7. Launch Cognos Configuration, save the configuration, and restart the server. As an alternative, use the command line from the `install_location/bin64` folder, and run this command: `cogconfig.bat -s`.

This will regenerate the keys for the new JRE.

## 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 the default configuration settings on other IBM Cognos computers

After you change the default behavior of IBM Cognos components to better suit your IBM Cognos environment, you can [configure an authentication provider](#), and install and configure Framework Manager.

## Port and URI settings

You can change certain elements in a URI depending on your environment. An IBM Cognos URI contains the following elements:

Additional information about ports is available in the topic [“Review the default port settings” on page 9](#)

- 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`

**Important:** For HTTPS/SSL configurations, make sure to use fully qualified hostname for URIs.

The elements are described in the following table:

Table 19. IBM Cognos URI elements and descriptions	
Element	Description
protocol	<p>Specifies the protocol used to request and transmit information, either Hyper Text Transfer Protocol or Hyper Text Transfer Protocol (Secure).</p> <p><b>Example:</b> http or https</p>
host name or IP	<p>Specifies the identity of the host on the network. You can use an IP address, a computer name, or a fully qualified domain name.</p> <p>In a distributed installation, you must change the localhost element of a URI.</p> <p>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.</p> <p><b>Example:</b> localhost or 192.168.0.1 or [2001:0db8:0000:0000:0000:148:57ab]:80</p>
port	<p>Specifies the port on which the host system listens for requests.</p> <p>The default port for the IBM Cognos Analytics services is 9300. The default port for a web server is 80.</p> <p><b>Example:</b> 9300 or 80</p>
context root	<p>Used by the application server to determine the context of the application so that the request can be routed to the correct Web application for processing.</p> <p><b>Example:</b> p2pd</p>
alias path	<p>Used by the application server to route a request to the correct component within a Web application.</p> <p>The alias path must not be modified or IBM Cognos components will not function properly.</p> <p><b>Example:</b> servlet/dispatch</p>
virtual directory	<p>Used by the Web server to map a virtual directory or alias to a physical location.</p> <p>For example, in the default Gateway URI of http://localhost:80/ibmcognos/bi/v1/disp, the virtual directory is ibmcognos/cgi-bin.</p> <p><b>Example:</b> ibmcognos/</p>
gateway application	<p>Specifies the name of the Cognos gateway application that is used.</p> <p>For example, if you are accessing IBM Cognos components using a Common Gateway Interface (CGI), then the default gateway application would be cognos.cgi.</p> <p><b>Example:</b> cognos.cgi</p>

If you are using collaboration with IBM Connections, ensure that you include the full domain for all hostname entries in IBM Cognos Configuration. For example, if your computer is named MyComputer and your domain is **MyCompanyName.com**, then for the host\_name\_or\_IP value, use **MyComputer.MyCompanyName.com**. The domain must be included in order for IBM Connections to allow access.

## Changing a port or URI setting

Use the following procedure to change URI properties in IBM Cognos Configuration.

**Important:** You must specify fully qualified host names in the values for the following Cognos Configuration fields. Each value you specify must also appear in either the field **Subject Alternative Name > DNS names** or the field **Subject Alternative Name > IP addresses**.

- **Environment**
  - **Gateway URI**
  - **External dispatcher URI**
  - **Internal dispatcher URI**
  - **Dispatcher URI for external applications**
  - **Content Manager URIs**
- **Environment > Configuration Group**
  - **Group contact host**
  - **Member coordination host**
- **Security > Cryptography > Cognos**
  - **Server common name**
  - **Subject Alternative Name > DNS names**
  - **Subject Alternative Name > IP addresses**

## Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click the appropriate group or component:
  - To change an element for the dispatcher, click **Environment**.
  - To change an element for the local log server, under **Environment**, click **Logging**.
3. In the **Properties** window, click the **Value** box next to the URI property that you want to change.
4. Select the element and type the new information.
  - 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.
  - For HTTPS/SSL configurations, make sure to use fully qualified hostname for URIs.
5. From the **File** menu, click **Save**.

## Verifying configuration settings

Use this feature to verify settings in Cognos Configuration and avoid conflicts.

**Important:** You must specify fully qualified host names in the values for the following Cognos Configuration fields. Each value you specify must also appear in either the field **Subject Alternative Name > DNS names** or the field **Subject Alternative Name > IP addresses**.

- **Environment**
  - **Gateway URI**
  - **External dispatcher URI**
  - **Internal dispatcher URI**
  - **Dispatcher URI for external applications**
  - **Content Manager URIs**
- **Environment > Configuration Group**
  - **Group contact host**
  - **Member coordination host**
- **Security > Cryptography > Cognos**
  - **Server common name**
  - **Subject Alternative Name > DNS names**
  - **Subject Alternative Name > IP addresses**

## Procedure

1. Start **Cognos Configuration**.
2. Select action item, then select **Verify**.
3. Without starting the Cognos Analytics server, the following action items can be verified to ensure validity.
  - **Environment > External Dispatcher URI**
  - **Environment > Internal Dispatcher URI**
  - **Environment > Dataset service port number**
  - **Environment > Logging > Local log server port number**
  - **Environment > Configuration Group > Member synchronisation port**
  - **Environment > Configuration Group > Member coordination port**
4. Verify if the settings are configured properly in the **Environment > Configuration Group** section. These settings need to be configured to match with the active Content Manager server.

## Managing the Configuration Group

The configuration group defines a group of servers that share configuration. This is critical in multi-server installations so that configuration values remain available and consistent on all nodes, even after network partitions. The configuration group contact host runs on the same instance as the active content manager.

### About this task

- In an **Easy** installation, these values are set for you.
- For a **Custom** installation, the host and port properties are pre-populated during installation. However, you must follow the steps below to verify if the pre-populated settings are appropriate for your environment.

## Procedure

1. Start Cognos Configuration.
2. In the **Explorer** window, under **Local Configuration**, click **Environment**.
3. Click **Configuration Group**.
4. Specify the **Local Member Settings** values.
  - a) Set the **Member synchronization port** and **Member coordination port** values.

**Important:** These two ports must be open to both inbound and outbound traffic.

Ensure that the two ports are two different local ports that are not in use. If all of the applications on your computer were running during the installation, these ports should already be set, using available ports.

- **Member synchronization port** is the local port used for network communication that transfers and synchronizes configuration information from one server to another. Every install needs to be able to talk to the `MutualAuthSSLHttpEndpoint` on the other installs. For example, any firewall between application and data tier needs to be open on that port. The `httpEndpoint` is used strictly for internal communication from one Cognos Analytics instance to another. The default is 4300.
- **Member coordination port** is the local port used for network communication for group coordination. This port is used to discover and join a group, and to maintain an up to date list of configuration group members. On the primary Content Manager install group contact port is the same port. Each install needs to be able to talk to any of the other installs on the group coordination port, so again, any firewall between tiers of the installation needs to be open for that port. The default is 5701.

b) Configure the **Member coordination host** property.

This setting specifies the local host name for coordinating network communication within the Configuration group.

**If your computer has only one network adapter:**

Set the value of **Member coordination host** to the fully qualified domain name (FQDN) of the local computer.

**If your computer has more than one network adapter:**

Use one of these methods:

- Set the value of **Member coordination host** to a specific IP address to ensure that the product uses the correct adapter.

**OR**

- Use this pattern-matching method:
  - i) Set the value of **Member coordination host** to the fully qualified domain name (FQDN) of the local computer.
  - ii) Edit the file `installation_location/wlp/usr/servers/cognosserver/bootstrap.properties` and add this entry that specifies a pattern matching the correct adapter:

```
com.ibm.bi.jgroups.matchaddress=matched_pattern
```

where *matched\_pattern* can have one of two formats:

– `match-address:IP_address_pattern`

This format identifies the correct adapter by matching its IP address with a pattern of IP addresses.

For example, add the following line in the `bootstrap.properties` file:

```
com.ibm.bi.jgroups.matchaddress=match-address:10\\.\\.\\.\\.* to match any IP address that starts with 10., such as 10.1.2.3
```

**Tip:** The correct match-address syntax is `match-address:n\\.\\.\\.\\.*` (that is, using a single backslash). However, in the example above, you are editing the `bootstrap.properties` file. In `.properties` files, a backslash (`\`) is a special character. Therefore, you must add an extra backslash.

– `match-address:name_pattern`

This format identifies the correct adapter by matching the adapter name with a pattern of names.

For example, add the following line in the `bootstrap.properties` file:

```
com.ibm.bi.jgroups.matchaddress=match-interface:eth.*
```

to match any adapter that starts with the name `eth`, such as `eth2`

For more information about the pattern-matching method used above, visit these sites:

- <http://www.jgroups.org/manual/index.html#Transport>
- <https://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html>

#### 5. Configure the **Group Settings** properties.

The three **Group Settings** properties define the configuration group that shares the configuration. You must set the same values on all of the Cognos Analytics servers in your distributed environment.

a) On the computer where the primary Content Manager server is installed, set these values:

- **Group name**

Choose a name for the group.

- **Group contact port**

Set the same value as you did for the **Member coordination port** property.

- **Group contact host**

Set the same FQDN of this computer as you did for the **Member coordination host** property.

b) On each of the other computers in your distributed environment, set the same values that you used on the primary Content Manager server:

- **Group name**

Enter the same name that you set on the primary Content Manager server.

- **Group contact port**

Set the same value that you specified on the primary Content Manager server.

- **Group contact host**

Set the same value that you specified on the primary Content Manager server.

**Tip:** An alternate method for setting the values on a computer that is not the primary Content Manager server is to follow these steps:

i) Right-click **Configuration Group**, click on the **Retrieve** button to launch **Retrieve Configuration Servers** dialog.

If the active Content Manager is SSL enabled, you can retrieve the configuration group properties **after** Content Manager URL and other properties have been correctly configured and saved.

ii) Enter the proper information to access the active Content Manager server, and then click **OK**.

**User ID** - The ID with administration privileges on the server.

**Password** - The password for the User ID.

**Namespace ID** - The value can be found in the **Security, Authentication** resource. For example, `CognosEx`

**Cognos Analytics URL** - The URL used to run Cognos Analytics. For example, `http://myserver:9300/bi`

#### 6. Save the configuration.

## 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

### Configuring general cryptographic settings

In a distributed installation, IBM Cognos computers communicate with Content Manager to establish trust and obtain some cryptographic keys from Content Manager.

If you change the cryptographic keys in Content Manager, such as by changing application servers or reinstalling Content Manager, you must delete the cryptographic keys on the other IBM Cognos computers. You must then save the configuration on each computer so that they obtain the new cryptographic keys from Content Manager. In addition, all IBM Cognos components in a distributed installation must be configured with the same cryptographic provider settings.

Also, in a distributed environment, the symmetric key should only be stored on computers where Content Manager has been installed.

You can configure the following general cryptographic settings:

- Standards conformance

Specifies which cryptographic standard is to be used, IBM Cognos or NIST SP 800-131A.

- 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, confidentiality and SSL Transport Layer Security settings.

**Note:** Transport Layer Security consists of a set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol. Choose from 1.1, 1.2, or the combination setting.

- Advanced algorithm settings

These include signing and digest algorithms.

### Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, click **Cryptography**.
3. In the **Properties** window, change the default values by clicking the **Value** box and then selecting the appropriate value:

#### Standards conformance

The supported values are **IBM Cognos** and **NIST SP 800-131A**. This property might cause the save operation to fail if other parameters are not allowed in the selected standard. You must change the selected algorithm or the standards conformance. You may need to install the JRE's unlimited jurisdiction policy files to enable all the supported algorithms. They are available from [IBM](#)

#### CSK settings

On computers that do not contain Content Manager, if you do not want to store the CSKs locally, change the **Store symmetric key locally** property to **False**.

When the **Store symmetric key locally** property is set to **False**, the key is retrieved from Content Manager when required. The **Common symmetric key store location** property is ignored.

## SSL Settings

If you want the computers at both ends of a transmission to prove their identity, change **Use mutual authentication** to **True**.

Do not change the **Use confidentiality** setting.

## Advanced algorithm settings

If you want to change the digest algorithm, for the **Digest algorithm** property, select another value.

4. From the **File** menu, click **Save**.
5. Test the cryptographic provider on a gateway computer only. In the **Explorer** window, right-click **Cryptography**, and click **Test**.

IBM Cognos components check the availability of the symmetric key.

## Results

After you configure the cryptographic settings, passwords in your configuration and any data that you create are encrypted.

## Configuring the Cognos cryptographic provider

Cognos Analytics includes its own cryptographic provider, named **Cognos**.

**Tip:** The provider default name **Cognos** can be changed to any other name. The provider type is always **Cognos**.

## Before you begin

- If you are using a JRE other than the one provided with IBM Cognos server, go to the *install\_location/ibm-jre/jre/lib/ext*, and copy *bcprov-jdkversion.jar* to *JRE\_location/lib/ext*.
- If you are using a JRE other than the one that IBM Cognos provides, you must also download and install the unrestricted Java Cryptograph Extension (JCE) policy file for your JRE to ensure that all available algorithms and cipher suites are shown in IBM Cognos Configuration.

## Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security > Cryptography**, click **Cognos**.
3. In the **Properties** window, change the properties as needed.

**Tip:** For detailed information about each property, view the property description in IBM Cognos Configuration when you click the property.

- To configure the confidentiality algorithm, under **Cryptography, 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.


JREs include a restricted policy file that limits you to certain cryptographic algorithms and cipher suites. If you require a wider range of cryptographic algorithms and cipher suites, unrestricted (unlimited) policy files are now provided by default. They can be found here:



- install location/ibm-jre/jre/lib/security/policy/unlimited/US\_export\_policy.jar
- install location/ibm-jre/jre/lib/security/policy/unlimited/local\_policy.jar

In addition, for Java that is provided by IBM, the unrestricted JCE policy files are also available [here](#).

- To adjust the cipher suites, under **Supported ciphersuites**, click in the **Value** column and then click

the edit icon .

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 crypto keys, under **Encryption key settings**, change **Encryption key store location** to the new location.
- If configuring for HTTPS/SSL, change the **Server common name** from CAMUSER to the fully qualified domain name of the server.
- To configure the **Subject Alternative Name**, specify **DNS names**, **IP addresses**, and **Email addresses** (optional) that are associated with the server certificate. The values are added to the Subject Alternative Name extensions in the server certificate. You can specify multiple values for each property. Separate the values using the space character.

4. From the **File** menu, click **Save**.

## Results

If you use another certificate authority (CA), see [“Configuring Cognos Analytics to use another certificate authority \(CA\) certificate”](#) on page 200.

## Enabling FIPS mode

Federal Information Processing Standards (FIPS) is an American cryptographic standard that is published by the National Institute of Standards and Technology (NIST). IBM Cognos Analytics is not FIPS-certified. However, you can configure Cognos Analytics on all platforms to use only FIPS-certified security modules. When you complete this configuration, Cognos Analytics is in "FIPS mode".

For more information, see [Federal information processing standards \(FIPS\)](https://www.nist.gov/federal-information-processing-standards-fips) (<https://www.nist.gov/federal-information-processing-standards-fips>).

## Before you begin

You must be running IBM JRE. Other JRE versions are not supported.

## About this task

When in FIPS mode, IBM Cognos Analytics uses the FIPS 140-2 approved cryptographic providers; IBM® Crypto for C (Certificate 3064) and Openssl (Certificate 4282). The certificates are listed on the NIST web site at <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search>.

**Note:** IBM® Crypto for C is in the process of achieving FIPS 140-3 certification, as seen here: <https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List>

## Limitations of FIPS mode

When Cognos Analytics is configured in FIPS mode,

- the Series 7 authentication provider is not available

- PDF password protection is disabled
- cogstartup.xml, keystores, and deployment archives are not encrypted using a FIPS-certified provider. If these files must be manually moved to a different computer, you must ensure that they are adequately protected during transport.

The supported cryptographic algorithms are limited only by the cryptographic providers listed above. You can configure IBM Cognos Analytics to use specific algorithms and TLS cipher suites. However, no runtime check is made to verify that the selected algorithms adhere to FIPS or any other standard. You are responsible for this verification.

If you use an existing content store, some legacy encrypted data that was persisted use algorithms that were configured when they were generated. Currently, the only method of re-encrypting data in the content store is to do a full deployment export/import. If possible, this import should be into an empty content store.

#### Note:

Your authentication provider must use the CAMKeystore method for LDAPS authentication. LDAPS that uses the legacy certutil database (NSPR networking) is not supported with FIPS.

If you try to use certutil LDAPS with FIPS, this error message appears:

```
CAM-AAA-0026 The function call to 'ldap_simple_bind_s' failed with error code: '81'
```

By default, Cognos Analytics FIPS mode is not enabled, as it can result in slightly reduced product performance.

## Procedure

1. Add a FIPS-certified security encryption module to your list of service providers.

- a) Go to the *installation\_location/ibm-jre/lib/jre/security* folder.
- b) Open the file `java.security` in a text editor.

A list of security providers is displayed. Each entry contains a number that indicates the ranked preference for that provider. Here is an example:

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.crypto.plus.provider.IBMJCEPlus
```

**Important:** The existing provider `IBMJSSEProvider2` must remain first in the list. You must now add `IBMJCEPlusFIPS` as the second provider in the list.

- c) Add a new line to the second position of the list that defines `IBMJCEPlusFIPS` as the service provider. Then re-number each provider's rank to reflect the new order.

Using the previous example, the expanded list now appears as follows:

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.plus.provider.IBMJCEPlusFIPS
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.crypto.plus.provider.IBMJCEPlus
```

2. Enable the FIPS service provider.

- a) Go to the *installation\_location/bin64* folder.
- b) Open the file `bootstrap_wlp_xxxx.xml` in a text editor.
- c) Add the following two lines in the `<start>` section:

```
<param condName="{java_vendor}" condValue="IBM">-Dcom.ibm.jsse2.usefipsprovider=true</param>
<param condName="{java_vendor}" condValue="IBM">-Dcom.ibm.jsse2.usefipsProviderName=IBMJCEPlusFIPS</param>
```

3. Specify FIPS conformance in Cognos Configuration.

- a) In Cognos Configuration, select **Security > Cryptography**.

- b) Set the **Standard conformance** property to **FIPS 140-2**.
- c) Save the configuration.

## IBM Cognos Application Firewall

IBM Cognos Application Firewall analyzes and validates HTTP and XML requests before they are processed by IBM Cognos servers. IBM Cognos Application Firewall may modify these HTTP and XML requests.

IBM Cognos Application Firewall protects IBM Cognos Web products from malicious data. The most common forms of malicious data are buffer overflows and cross-site scripting (XSS) attacks, either through script injection in valid pages or redirection to another Web site.

You can track firewall activity by checking the log file, which contains rejected requests. By default, log messages are stored in the *install\_location/logs/cogaudit.log* file.

If you are using the collaboration features with IBM Connections, you must add the host name, domain, and port number on which IBM Connections is running to the **Valid domains and hosts** property for the Cognos Application Firewall.

All Cognos Application Firewall settings must be the same for all computers where IBM Cognos Application Tier Components are installed within a distributed environment. For example, if Cognos Application Firewall is disabled on some computers and enabled on others, unexpected behavior and product errors may result.

The following types of URLs are accepted by Cognos Application Firewall validation:

- fully qualified (absolute) URLs
  - in the format *protocol://host:port/path*, where *protocol* is http or https and *host* is validated against the valid domain list
- URLs relative to the Web installation directory
  - in the format */Web\_installation\_root/\** where *Web\_installation\_root* is the gateway Web directory, based on the ibmcognos alias that you configured on your Web server.
  - For example,  
*/ibmcognos/ps/portal/images/action\_delete.gif*
- specific allowed URLs, including the following (all case insensitive)
  - about:blank
  - JavaScript:window.close()
  - JavaScript:parent.close()
  - JavaScript:history.back()
  - parent.cancelErrorPage()
  - doCancel()

## Configuring IBM Cognos components to use IBM Cognos Application Firewall

Using IBM Cognos Configuration, you can change settings for other XSS tool support, and you can add host and domain names to the IBM Cognos list of valid names.

### Procedure

1. Start IBM Cognos Configuration in each location where Application Tier Components are installed.
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**.

For SiteMinder, when this property is set to **True**, the default values for **BadURLChars** and **BadCSSChars** are masked by Cognos Analytics. The HTTP verbs PUT and DELETE are also masked.

Examples of **BadURLChars** and **BadCSSChars** are: a tilde (~), a period (.), period and a forward slash (./), greater than sign (>), and more. For more information, see the SiteMinder documentation.

5. Add host and domain names to the IBM Cognos list of valid names:

- For the **Valid domains and hosts** property, click the value and then click the edit icon .
- In the **Value - Valid domains or hosts** dialog box, click **Add**.

You must include the domains from all hyperlinks that are added in the portal. For more information, see the topic about creating a URL in the *IBM Cognos Analytics Administration and Security Guide*.

**Tip:** If you are using drill-through from IBM Cognos Series 7 to reports in IBM Cognos Analytics, add the host names 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.

If you are using the collaboration features with IBM Connections, you must add the host, domain, and port number for the IBM WebSphere profile where you have installed IBM Connections. For example, if you installed IBM Connections on a computer named **myserver**, and your domain is **mycompany.com**, you would add **myserver.mycompany.com:9080**, where 9080 is the IBM WebSphere port number on which IBM Connections is running.

- 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 Analytics 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 turn off the encryption of the content.

By default, IBM Cognos components store temporary files in the *install\_location\temp* directory and the files are not encrypted.

For optimum security, deny all access to the temp directory, except for the service account used to start the IBM Cognos services. Read and write permissions are required for the service account.

### Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.

3. In the **Properties** window, for the **Temporary files location** property, specify the new location.
4. If you do not want the content of temporary files to be encrypted, set the **Encrypt temporary files** property to **False**.
5. Ensure that the user account under which IBM Cognos Analytics 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

## 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.

**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.

**Restriction:** When restarting services manually, (if applicable) the **ApacheDS - cognos** service must be started before the **IBM Cognos** service.

## Enabling and disabling services

Use the following procedure to disable selected services on components in a distributed installation.

### Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Environment**, click **IBM Cognos services**.
3. In the **Properties** window, click the **Value** next to the service that you want to disable or enable.

By default, all services are enabled.

4. Click the appropriate state for the services:

- To disable the service, click **False**.
- To enable the service, click **True**.

When restarting services manually, (if applicable) the **ApacheDS - cognos** service must be started before the **IBM Cognos** service.

5. From the **File** menu, click **Save**.

## Configuring fonts

IBM Cognos products use fonts to render PDF reports on the IBM Cognos server. They also use fonts to render charts used in PDF and HTML reports.

To show output correctly, fonts must be available where the report or chart is rendered. For charts and PDF reports, the fonts must be installed on the IBM Cognos server. If a requested font is not available, IBM Cognos components substitute a different font.

Because HTML reports are rendered on a browser, the required fonts must be installed on the computer of each IBM Cognos user who views the report. If a requested font is not available, the browser substitutes a different font.

Use the following checklist if you want to use a new font in your reports.

- \_\_\_ • [Add the font to the list of supported fonts.](#)
- \_\_\_ • [Specify the file location of the new font.](#)
- \_\_\_ • [Map the new font to the physical font name, if required.](#)

## Considerations to support Simplified Chinese

IBM Cognos products support the GB18030-2000 character set, which is used in the encoding of Simplified Chinese locales.

If you install on Microsoft Windows, support is provided for the GB18030-2000 character set in the SimSun-18030 font that is provided by Microsoft.

On operating systems other than Windows, you must install a font that supports GB18030-2000.

## Add Fonts to the IBM Cognos Environment

You can add fonts to the list of supported fonts in your IBM Cognos environment if you want to generate reports that use fonts that are currently not available. You can also remove fonts. By default, IBM Cognos components use a set of global fonts, which are available on all IBM Cognos server computers.

### Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Fonts** tab.
4. Click **Add**.

**Tip:** To remove a font from the list of supported fonts, click the box next to the font name and then click **Remove**.

5. In the **Supported Font Name** box, type the font name and then click **OK**.
6. From the **File** menu, click **Save**.

All global fonts, including new fonts that you add, must be installed on all IBM Cognos computers in your environment.

### Results

If a global font is not installed on all IBM Cognos computers, you must [map the global font to an installed, physical font](#).

## Specifying 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 that are installed in the *install\_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 that are installed in the Windows font directory.

You specify the font location on all computers where Application Tier Components are installed.

### Procedure

1. On each Application Tier Components computer, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.

3. In the **Properties** window, for the **Physical fonts locations** property, specify the location of the fonts.  
If there are multiple font paths, separate each path by a semicolon (;).  
If you are using an application server other than one that is provided with IBM Cognos Analytics, enter the fully qualified path to the font location. For example: *install\_location\bin\fonts*.
4. From the **File** menu, click **Save**.

## Map Supported Fonts to Installed Fonts

You can substitute global fonts, which are not installed on the computer, for physical fonts.

You map fonts on each computer where the Application Tier Components are installed.


For example, you add a font to the list of supported fonts that is not installed on the IBM Cognos computer. You can specify which font to use as a substitute.

If you want to print reports faster by using the built-in PDF fonts, you can map a global font such as Arial to one of the built-in PDF fonts, such as Helvetica-PDF, using the following steps. You can also select one of the built-in PDF fonts for a text object in Reporting or Query Studio. For more information, see the *Query Studio User Guide* or the *Reporting User Guide*.

No mapping is required if you add a font to the supported font list that is installed on IBM Cognos computers. However, you must specify the location of the font.

## Procedure

1. On each Application Tier Components computer, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, click the **Value** box next to the **Physical fonts map** property, and then


click the edit icon .

The **Value - Physical fonts map** dialog box appears.

4. Click **Add**.

**Tip:** To remove a font, select the check box next to the font and click **Remove**.

5. In the **Global Font Name** box, type the name of the font you added to the supported font list.
6. Click the **Physical Font Name** box.

7. If you know the physical font name, type it. Otherwise, click the edit icon .

In the **Physical Font Name** dialog box, click **Search Now** and then click a font name from the results.

8. Repeat steps 4 to 7 for each global font that requires mapping.
9. Click **OK**.
10. From the **File** menu, click **Save**.

## Results

Now, if required, you must specify the installation location of the fonts.

## Using system fonts in IBM Cognos Configuration

You can set IBM Cognos Configuration to use your system fonts on Microsoft Windows operating systems.

**Note:** If you enable system font settings, you cannot change the font settings within IBM Cognos Configuration.

## Procedure

1. Go to the *install\_location/configuration* directory.

2. Open the `cogconfig.prefs` file in a text editor.
3. Add the following line:

```
UseSystemDisplaySetting=true
```

4. Save and close the file.
5. Restart IBM Cognos Configuration.


## 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 Analytics embeds required fonts in reports by default. To minimize the file size, IBM Cognos Analytics embeds only the characters (also called glyphs) used in the report rather than all characters in the font set. IBM Cognos Analytics embeds fonts only if they are licensed for embedding. The license information is stored in the font itself and is read by IBM Cognos Analytics.

If you are confident that the fonts used in reports are available on users' computers, you can limit or eliminate embedded fonts to reduce the size of PDF reports. When limiting fonts, you specify whether a font is always or never embedded, using an embedded fonts list in IBM Cognos Configuration.

### Procedure

1. On the Content Manager computer, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, under **Font Settings**, click the value for **Fonts to embed (Batch report service)** or **Fonts to embed (Report service)**, and then click the edit icon .
4. If you are not using the default fonts directory or if you want to add a path to an additional directory, in the **Fonts to Embed in PDF Reports** dialog box, specify the new path in the font paths box.

**Tip:** Click **Search Now** to get a list of the available fonts in the specified path or paths.

5. For a font that will always be available on users' computers, scroll to the font name, and click the **Never** check box.

IBM Cognos Analytics 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 Analytics embeds the font with all reports that use it. Adobe Reader uses the embedded font when the report is opened.

7. Click **OK**.

## Changing the location of temporary report output

When users run interactive reports, the report output is stored in Content Manager or in a temporary session cache in the local report file system. You can change the location of the temporary session cache to a remote computer such as a shared directory on a Microsoft Windows based system or a common mounted directory on a UNIX or Linux based system.

By default, the location of the temporary session cache on the report file system is `install_location/temp/session`. The session directory is created by the report server when the first request from a user session is received.



## Procedure

1. Start IBM Cognos Configuration on the computers where Application Tier Components are installed.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, click the value for **Temporary files location**, and then click the edit icon



4. In the **Select Folder** dialog box, use the **Save in** box to locate the computer and directory, and then click **Select**.
5. From the **File** menu, click **Save**.

When a user runs an interactive report session, the temporary report output is now stored in the new location.

## Changing the location of data files

You can change the location of the data folder, which contains data files created by Cognos Analytics components.

The default location of this folder is *installation\_location/data*

**Important:** The data folder must reside locally on the active Content Manager computer as well as on each standby Content Manager computer.

If you specify that data files reside on a shared network drive, then the active and standby Content Manager computers will try to access the same Search Index files in the data/search folder. As a result, users will see this message:

Unable to retrieve activities at this time. ADM-ERR-001

In addition, error messages will be logged and the index may get corrupted. Here is an example of a logged error message caused by the data folder being configured on a shared disk:

```
org.apache.lucene.store.AlreadyClosedException: Already closed:
MMapIndexInput(path="\
\myshare\cognos11\data\search\collections\cm\data\index\_c0d_Lucene50_0.tim")
at
org.apache.lucene.store.ByteBufferIndexInput.readBytes(ByteBufferIndexInput.jav
a:106) ~[lucene-core-8.2.0.jar:8.2.0 31d7ec7bbfdcd2c4cc61d9d35e962165410b65fe -
ivera - 2021-04-19 15:05:56]
```

## Procedure

1. On the Application Tier Components computer, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, click the value for **Data files location**.



4. Click the edit button.
5. In the **Select Folder** window, navigate to the directory you want and then click **Select**.
6. From the **File** menu, click **Save**.

## Tuning WebSphere Liberty Profile

In production environments, tune the WebSphere Liberty Profile to allow for the maximum number of concurrent users you expect by adjusting the **coreThreads** and **maxThreads** values in the Advanced properties of the resources. These values set the core and maximum executor thread counts.

### Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Environment**, under **IBM Cognos services** click the Resources name (default is **IBM Cognos**).
3. In the **Properties** window, next to **Advanced properties**, click inside the **Value** box, and then click the

edit icon .

4. Adjust the parameter values as needed.

Table 20. Service Resource parameter names and values	
Parameter Name	Value
<b>coreThreads</b>	The core number of threads that the WebSphere Liberty Profile server starts up with. If this value is less than 0, a default value is used. This default value is calculated based on the number of hardware threads on the system.
<b>maxThreads</b>	The maximum number of threads that can be associated with the WebSphere Liberty Profile server.

For more information, refer to the WebSphere Liberty Profile knowledge center, Tuning the Liberty profile ([https://www.ibm.com/support/knowledgecenter/en/SSEQTP\\_liberty/com.ibm.websphere.wlp.doc/ae/twlp\\_tun.html](https://www.ibm.com/support/knowledgecenter/en/SSEQTP_liberty/com.ibm.websphere.wlp.doc/ae/twlp_tun.html)).

5. From the **File** menu, click **Save**.

## Enabling session replication for standby Content Manager services

The session replication feature allows for seamless IBM Cognos Content Manager failover between an active Content Manager service and a standby Content Manager service.

With session replication enabled, user session data are replicated among all Content Manager instances. If the active Content Manager fails, the user session data is preserved and users continue to use the application without disruption.

Session replication uses two ports to securely communicate with the different IBM Cognos Content Managers configured within a single environment.

### Procedure

1. On a computer where the IBM Cognos Content Manager is installed, start IBM Cognos Configuration.
2. In the **Explorer** pane, under **Security**, click **Replication**.
3. Specify the following properties:

a) Set **Enable replication** to **True**.

b) In the **Peer listener port number** value box, enter a port number.

A value of 0 selects the first available dynamic port during the IBM Cognos service startup.

c) In the **RMI replication port number** value box, enter a port number.

**Note:** The **Advanced properties** should be used only under guidance from IBM Technical Support.

4. Save the configuration and restart the IBM Cognos service.
5. Repeat the steps for each Content Manager instance in your environment.

The port numbers that you specify do not need to be identical for each Content Manager instance.

## Use an external object store for report output and datasets

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

Using an external object store for report output reduces the size of the content store and provides performance improvements for Content Manager.

### Before you begin

Ensure that you do the following before you create an external object store connection.

- Provide Content Manager computers with access to the file location of the external object store.
- Provide the user account that runs the IBM Cognos service with read and write access to the file location.
- Create the content store.

### Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, under **Data Access > Content Manager**, right-click the name of your **Content Store**, and then click **New resource > External Object Store**.
3. In the **New Resource - External Object Store** window, type a unique name for your file system repository, and click **OK**.

You can have only one external object store.

4. Click the name for the repository.
5. In the **External Object Store - Resource Properties** window, click inside the value field, click edit, and when the **URI values** window opens, type the path to your file system location, where file-system-path is the full path to an existing file location.

Table 21. Examples of URI values	
File system	URI value
Windows	file:///c:/file-system-path
	file://host/share/file-system-path
UNIX or Linux	file:///file-system-path

**Note:** Relative paths, such as file:///../file-system-path and drive mappings are not supported.

In a distributed installation, all Content Managers must have read and write access to the file system location. To improve performance when reading outputs, Application Tier Components, essentially the repository service, should have read access to the file system location. If they do not have read access, requests are routed to the active Content Manager.

6. Restart the IBM Cognos service.

## Verify access to the external object store

Use IBM Cognos Configuration to verify that IBM Cognos components can connect to the external object store.

### Procedure

1. Start IBM Cognos Configuration.
2. From **Explorer > Data Access**, right-click the name of your external object store connection.
3. Click **Test**.

IBM Cognos Configuration verifies access to the external object store file location.

You can also test this connection by right-clicking **Local Configuration** and selecting **Test**.

## Configuring query settings

---

To optimize data access, you can configure parameters that are used by the query service.

### Changing the cache size of dynamic queries

When a user's content (a dashboard for example) has more than 25 queries set to run concurrently, some query results may fail to load. To mitigate this issue, you can increase the values assigned to the `queryReuse` parameter.

#### About this task

Dynamic Query can improve query execution by reusing previously computed results. As queries are planned, Dynamic Query determines if there are applicable results in the cache that it can leverage. Each instance of Dynamic Query manages a cache, which can hold up to 250 entries. Each user session accessing that instance can have up to 25 entries in that cache. Cached entries are removed based on either inactivity or to make space for new entries.

Potentially, dashboards may include many widgets in one or more tabs. The queries generated by those widgets may cause entries to be evicted from the cache to make room for new entries. As a user interacts with the dashboard, they may observe that some queries respond more slowly. This may be due to the number of widgets on the dashboard that they are using and how they interact with it.

**Tip:** Raising the cache size increases both memory usage and temporary disk space. Before you raise the cache size, review the extent to which queries are embedded in your content. For example, perhaps your dashboards can be re-designed with fewer widgets. Or maybe you can move rarely used widgets to a different tab to reduce how often they are executed.

#### Removing partially filled result sets from the cache

When a query is executed against a data source, the data source executes a statement and produces a result set. The data source may create locks or consume temporary space, which it releases as the result set or statement objects it is managing are closed.

In many cases, Dynamic Query executes a statement and reads all the rows returned by the data source result set. Dynamic Query can then call the methods in the data source client library to indicate that those objects are to be closed, and in turn, the data source can release any resources it created.

You may be viewing a report interactively in the viewer, and slowly page through the output and may not read all the rows. When query re-use is active, the cached result set is only partially filled, and the associated database objects is long-lived.

Should those resources impede other activity in the data source, you may need to set `qs.general.queryReuse.retention.removePartialDataset` to `true`.

In applications that use Framework Manager, you can consider setting the Cursor Mode policy to Load in Background.

## Procedure

1. Start the Administration console.
2. Follow the steps in "Setting query service properties" in the *Cognos Analytics Administration and Security Guide*.
3. In step **6** of the procedure above, select **Advanced settings**.
4. Enter new values for the **qs.general.queryReuse.size** and **qs.general.queryReuse.data.threshold** parameters.

### Example

You want to make these changes to the query cache:

- Increase the maximum number of queries per user from 25 to 30.
- Increase the maximum number of queries in the global pool to 350.

Enter these *name/value* pairs for **Parameter** and **Value**:

**qs.general.queryReuse.size**

30

**qs.general.queryReuse.data.threshold**

350

5. From the **Actions** menu for the **QueryService - dispatcher\_name**, click **Start** to restart the service.

## Results

The query service is configured with the new settings.

**Note:** As an alternative to using the Administration console, as described in the previous steps, you can create an `xqe.config.custom.xml` file. To make the same changes as in the previous example, follow these steps:

1. Stop the IBM Cognos Analytics service.
2. Go to `installation_location\configuration`
3. If the file `xqe.config.custom.xml` does not yet exist, copy the file `xqe.config.xml` and rename it `xqe.config.custom.xml`
4. Edit `xqe.config.custom.xml`:
  - a. Enter the `queryReuse` parameter and its values after the `<general>` line.

```
<queryReuse enabled="true|false" size="number_of_queries_in_user_cache">
  <!-- reusable objects retention in seconds -->
  <retention maxIdle="number_of_seconds" maxAge="number_of_seconds"/>
  <!-- result sets held for reusable objects. Memory is maximum per result set in
  megabytes.-->
  <data threshold="number_of_queries_in_global_cache"/>
</queryReuse>
```

### Example

You want to make these changes to the query cache:

- Increase the maximum number of queries per user from 25 to 30.
- Remove query results after 3600 seconds of inactivity.
- Increase the maximum number of queries in the global pool to 350.

Add the following lines immediately after the `<general>` line:

```
<queryReuse enabled="true" size="30">
  <!-- reusable objects retention in seconds -->
  <retention maxIdle="300" maxAge="3600"/>
  <!-- result sets held for reusable objects. Memory is maximum per result set in
  megabytes.-->
  <data threshold="350" maxMemory="6"/>
</queryReuse>
```

- b. Save `xqe.config.custom.xml`.
5. Start the IBM Cognos Analytics service.

## Reverting to missing values in list reports

The format property `Missing Value Characters` defined in Framework Manager models is now honored in list reports.

### About this task

In previous releases, when the `Missing Value Characters` format property was defined against an item in a Framework Manager model, it would get applied for crosstab reports, but not for list reports. In other words, null values for the given model item would appear as blank in a list report instead of displaying the characters defined in the format property `Missing Value Characters`. This was not the desired behavior and has been rectified for release 11.1.7.

If you wish to revert to the Cognos Analytics behavior that was exhibited prior to release 11.1.7, follow this procedure:

### Procedure

1. Stop the IBM Cognos Analytics service.
2. Go to `installation_location\configuration`
3. If the file `xqe.config.custom.xml` does not yet exist, copy the file `xqe.config.xml` and rename it `xqe.config.custom.xml`
4. Edit `xqe.config.custom.xml`:
  - a) Immediately after the `<queryPlanning>` line, add the following line:

```
formatMissingValuesInListReports enabled="false"/>
```

- b) Save `xqe.config.custom.xml`.
5. Restart the IBM Cognos Analytics service.

## Ensuring that root members in a Planning Analytics data source match those in the TM1 client

If you import a TM1 data source into Cognos Analytics and select the data source type as **IBM Planning Analytics**, the list of root members in the metadata tree may look different than the list that appears in TM1 client.

### Solution

You can enable the REST API `tm1.RootMembers()`. This REST API returns root members from the Planning Analytics data source that match the root members returned from the TM1 Client.

**Important:** You must be using a Planning Analytics server version of 2.0.6 or later.

Follow these steps:

1. Stop the IBM Cognos Analytics service.
2. Go to `installation_location\configuration`
3. If the file `xqe.config.custom.xml` does not yet exist, copy the file `xqe.config.xml` and rename it `xqe.config.custom.xml`
4. Edit `xqe.config.custom.xml`:
  - a. Immediately after the `<queryExecution>` line, add the following line:

```
<paUseRootMembers enabled="true"/>
```

- b. Save `xqe.config.custom.xml`.
5. Start the IBM Cognos Analytics service.

## Disabling filler members in a Planning Analytics package

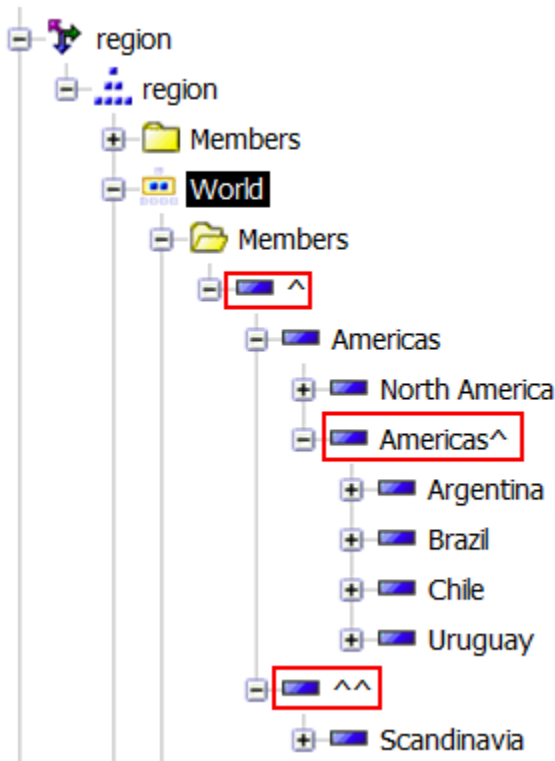
You can disable automatic generation of filler members so that a Planning Analytics package imported to Cognos Analytics shows the same characteristics as it does in the TM1 client.

In Cognos Analytics, by default, filler members are generated to fill gaps due to restricted access from the root of the hierarchy down to members whose data are visible to the user. In IBM Cognos TM1 however, the default behavior is that filler members are not generated.

### Example 1: Filler members enabled

When filler members are enabled, the caption of a filler member in the data tree is the caption of the parent member with a caret character (^) appended. If access to a root member is not granted to the user, the root member's caption is a caret character (^) only.

A metadata tree with filler members enabled is shown in the following image:



A chart for the same cube appears as follows:

Budget	1 Quarter	2 Quarter	3 Quarter	4 Quarter
Americas^				
North America	825517.05	846801.29	830379.17	868830.05
Total(children(Am))	825517.05	846801.29	830379.17	868830.05

### Example 2: Filler members disabled

**Note:** Since access to the root member is restricted for the cube in example 1, if filler members are disabled, the user cannot see any members at all in the data tree.

A chart from the same cube appears as follows:

Budget	1 Quarter	2 Quarter	3 Quarter	4 Quarter
North America	825517.05	846801.29	830379.17	868830.05
Total(children(Am))	825517.05	846801.29	830379.17	868830.05

## Procedure

To ensure that a data source displays the same characteristics in both TM1 client and Planning Analytics, follow these steps:

1. Stop the IBM Cognos Analytics service.
2. Go to *installation\_location*\configuration
3. If the file `xqe.config.custom.xml` does not yet exist, copy the file `xqe.config.xml` and rename it `xqe.config.custom.xml`
4. Edit `xqe.config.custom.xml`:
  - a. Immediately after the `<queryExecution>` line, add the following line:

```
<!-- Set the paUseFillerMember enabled attribute value to false to turn the Filler Member OFF -->  
<paUseFillerMember enabled="false"/>
```

- b. Save `xqe.config.custom.xml`.
5. Start the IBM Cognos Analytics service.

## Configuring the Dataset service port number exchange timeout

To prevent Dataset service timeouts, you can increase the value of the **dssPortNumberExchangeTimeout** parameter.

The Dataset service can take a significant amount of time to start and prepare to serve incoming requests. If this time exceeds the default service port exchange timeout value of 5 minutes, the Dataset service is terminated.

The **dssPortNumberExchangeTimeout** parameter is contained in the `xqe.config.xml` file. To increase its value from the default value, follow these steps:

## Procedure

1. Stop the IBM Cognos Analytics service.
2. Go to *installation\_location*\configuration
3. If the file `xqe.config.custom.xml` does not yet exist, copy the file `xqe.config.xml` and rename it `xqe.config.custom.xml`
4. Edit `xqe.config.custom.xml`:
  - a) At the end of the `<network>` section, uncomment the following line:

```
<!-- <dssPortNumberExchangeTimeout value="600"/> -->
```

The end of the `<network>` section now looks like this:

```
<!-- The dataset-service port number exchange timeout in seconds. Default is 300 (5 minutes). -->  
  <dssPortNumberExchangeTimeout value="600"/>  
</network>
```



- b) Save `xqe.config.custom.xml`.
5. Restart the IBM Cognos Analytics service.  
The Dataset service port number exchange timeout is now set to 600 seconds, or 10 minutes.

## 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 Analytics. If you use this option, a descriptor file with an `_descr` extension is also saved. Saved files are not managed by IBM Cognos Analytics.

### Save Report Output Outside IBM Cognos Analytics

If you configure a file system location that is outside of IBM Cognos Analytics, you can then share the report output with external applications or people who don't have IBM Cognos Analytics. 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 Analytics, in the *IBM Cognos Analytics Administration and Security Guide*.

Report outputs will always be written to the directory configured for each Delivery Service instance. In order to avoid having report outputs written to multiple locations, ensure that you are either running only one instance of the Delivery Service, or configure all service instances to use a shared network file location. Any Dispatcher running the Delivery Service must have access to the file system or be disabled on all systems not intended to save report output.

#### Procedure

1. Create a directory for your file system.

**Tip:** Ensure that the directory is accessible to users and separate from the installation directory. For example, in a distributed installation on Microsoft Windows, an archive folder such as `\servername\directory` could be used.

2. On the Content Manager computer, start IBM Cognos Configuration.
3. From the **Actions** menu, click **Edit Global Configuration**.
4. In the **Global Configuration** window, click the **General** tab.
5. For **Archive Location File System Root**, type a URI using the format

`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`

**Tip:** Ensure that you do not use a mapped drive when running Cognos as a Microsoft Windows service.

6. To confirm that the correct location will be used, click **Test**.
7. Click **OK**.
8. From the **File** menu, click **Save**.

#### Results

The administrator must now configure the file location. For information, see the topic about setting a file location for report output saved outside of IBM Cognos Analytics, in the *IBM Cognos Analytics Administration and Security Guide*.

## Save Report Output Inside IBM Cognos Analytics

If you configure a file system location that is inside IBM Cognos Analytics, 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 Analytics, in the *IBM Cognos Analytics Administration and Security Guide*.

Report outputs will always be written to the directory configured for each Delivery Service instance. In order to avoid having report outputs written to multiple locations, ensure that you are either running only one instance of the Delivery Service, or configure all service instances to use a shared network file location. Any Dispatcher running the Delivery Service must have access to the file system or be disabled on all systems not intended to save report output.

To protect the security of the report output when using this feature, the file system must have third-party encryption.

### Procedure

1. Create a directory for your file system.

**Tip:** Ensure that the directory is accessible to authorized users only.

2. On the Content Manager computer, start IBM Cognos Configuration.
3. In the **Explorer** window, click **Data Access > Content Manager**.
4. For the **Save report outputs to a file system** property, click **True**.
5. To test the connection to the report output directory, from the **Actions** menu, click **Test**.
6. From the **File** menu, click **Save**.

### Results

The administrator must now configure the file location using the `CM.OutPutLocation` parameter. For information, see the topic about setting a file location for report output saved inside IBM Cognos Analytics, in the *IBM Cognos Analytics Administration and Security Guide*.

## Customizing Server-side Printing for UNIX and Linux Platforms

---

The way in which the IBM Cognos Analytics portal handles server printing can differ depending on your platform.

For this reason, you can customize the way in which the portal handles the printing of PDF format reports for UNIX and Linux platforms by configuring the `rsprintpdf.sh` file.

The `rsprintpdf.sh` file should not be configured for Microsoft Windows operating system print servers.

When a user selects **Run with Options**, changes the **Format** to PDF, selects **Print the Report** from the **Delivery** section, and then specifies additional formats through **advanced options** such as Landscape orientation, A4 paper size or a **Time and Mode** to run the report, problems might occur when printing to a UNIX or Linux print server. The output might not be generated, or it might appear cropped or incorrectly orientated.

### Procedure

1. Open the `rsprintpdf.sh` file located in the `install_location/bin` directory.
2. In a text editor, customize the section that is specific to your print server's platform, for example AIX, or Linux.

3. Use the following information for customization. The information is passed to the *rsrintpdf.sh* script by the server process as command line options.

Table 22. Customization options for the printing of PDF format reports		
Option	Name	Description
-p	printer	Specifies the print queue. If no print queue is specified, the default queue is used.
-o	orientation	Specifies the page orientation for a file, for example landscape or portrait. If no orientation is specified, portrait orientation is used.
-m	media	Specifies the media size of the output, for example letter or A4 paper size. If no media, or no height or width are specified, the default paper tray is used.
-h	height	For custom page sizes. Specifies the height of the page in points. It is valid only if specified with the -w option, and without the -m option.
-w	width	For custom page sizes. Specifies the width of the page in points. It is valid only if specified with the -h option, and without the -m option.
-L	log file	Specifies a path to a user-specified file for logging error messages. The default filename for the log file is <i>rsrintpdf.errors.log</i> .

4. **Tip:** Keep a copy of the *rsrintpdf.sh* file in case it should be overwritten by a future software upgrade.

## Change the notification database

By default, the notification server uses the same database that Content Manager uses for the content store. You can use a separate database for notification in situations where you run large volumes of batch reports and email.

Using a separate database for notification involves the following tasks:

- Creating a notification database.

For IBM Db2, Oracle, Microsoft SQL Server, use the same procedure that was used to create the content store database. Use the instructions in [“Guidelines for creating the content store”](#) on page 10.

**Note:** If you are using Db2, you cannot generate a script to create the notification database in the same way as you can the content store.

For Db2 on z/OS, use the instructions in [“Suggested settings for creating a notification database on IBM Db2 on z/OS”](#) on page 195.

- Setting up the database connectivity.

You can use the same procedure as to set the connectivity for the content store database, [“Set up database connectivity for the content store database”](#) on page 99.

- Changing the connection properties for the notification database.

Use the instructions in [“Change the Connection Properties for the Notification Database”](#) on page 197.

## Suggested settings for creating a notification database on IBM Db2 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 Analytics 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 [“Creating tablespaces for a notification database on IBM Db2 for z/OS”](#) on page 196.
- \_\_\_ • Your database administrator must back up IBM Cognos Analytics databases regularly because they contain the IBM Cognos data.  
To ensure the security and integrity of databases, protect them from unauthorized or inappropriate access.

## Creating tablespaces for a notification database on IBM Db2 for z/OS

If you are using Db2 for 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 for z/OS. For example, all names of parameters must start with a letter and the length must not exceed 6 characters. For more information, see the Db2 Knowledge Center.

### Procedure

1. Connect to the database as a user with privileges to create and drop tablespaces and to allow execution of SQL statements.
2. To create the notification tablespaces, go to the *install\_location/configuration/schemas/delivery/zosdb2* directory.
  - a) Make a backup copy of the NC\_TABLESPACES.sql script file and save the file to another location.
  - b) Open the original NC\_TABLESPACES.sql script file and use the following table to help you to replace the placeholder parameters with ones appropriate for your environment.

<i>Table 23. Tablespace parameter names and descriptions for the Db2 notification database on z/OS</i>	
Parameter Name	Description
NCCOG	Specifies the name of the notification database.
DSN8G810	Specifies the name of the storage group.
BP32K	Specifies the name of the buffer pool.

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

- c) Save and run the script.

For example,

```
db2 -tvf NC_TABLESPACES.sql
```

- d) Open the NC\_CREATE\_DB2.sql script file and replace the NCCOG placeholder parameter with the name of the notification database.
- e) Save the script.

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

## Change the Connection Properties for the Notification Database

After you create a separate database for notification, you must configure IBM Cognos components to use the new database.

You must configure all Content Managers and Application Tier Components to use the same notification database.

### Procedure

1. In 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.

### Results

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.

## External certificate management in Cognos Analytics

---

IBM Cognos Analytics uses certificates to establish the root of trust between its different components. The certificates from an internal (default) or external certificate authority (CA) are supported.

The `ThirdPartyCertificateTool` command-line tool is used to manage the certificates.

For the external certificate authority (CA), you can configure a new certificate or an existing certificate.

### Minimum requirements for external CA certificates

These requirements are defined in IBM Cognos Configuration, **Security > Cryptography > Standards conformance**.

Select **IBM Cognos** for certificates that use a digital signature with SHA-1 algorithm and an RSA key of the size <2048.

Select **NIST SP 800-131A** or **FIPS 140-2** if all the certificates do not contain SHA-1 based digital signatures and have an RSA key of the size ≥2048.

## ThirdPartyCertificateTool commands and usage examples

The **ThirdPartyCertificateTool** is used to create a certificate signing request (CSR), import a certificate or private key, and export a certificate.

This tool can be used with both the internal (default) and external certificate authority (CA).

The tool is located in the Cognos Analytics *install\_location/bin* directory.

The sections in this topic provide descriptions of commands and usage examples for the **ThirdPartyCertificateTool**.

**Tip:** The same information can be accessed by using the `-help` parameter with the tool. For example, `ThirdPartyCertificateTool.bat -help`

### ThirdPartyCertificateTool commands

Use the following commands to specify the main operation mode for the tool.

- c**  
Creates a certificate signing request (CSR).
- i**  
Imports a certificate or a private key.
- E**  
Exports a certificate.

**Note:** If the built-in Cognos certificate authority (CA) is used, the export command exports the certificate that was issued by the local CA. This might not be the latest CA certificate, if one was remotely regenerated and both local certificates are still valid.

Use the following commands to specify the operation modifiers:

- T**  
Works with the trust store. Use only with the **-i** and **-E** commands.
- e**  
Works with the crypto identity.

Use the following commands to specify the information flags:

- p**  
Keystore password. If this command is not included, the default password is used.
- a**  
Key pair algorithm, which is either **RSA** (default) or **ECC**.
- r**  
CSR or certificate file location (depends on the operation mode).
- t**  
Certificate authority chain file. It can be PEM, binary PKCS#7 CA certificate chain, or a single DER-format CA certificate.
- d**  
The certificate distinguished name (DN), such as CN=product name, OU= unit, O=company, C=country.
- w**  
Private key source (PKCS#8, PKCS#12) password.
- H**  
Subject Alternative Name DNS names, such as DNS\_host\_1 [DNS\_host\_n]
- I**  
Subject Alternative Name IP addresses (IPv4, IPv6), such as IP\_address\_1 [IP\_address\_n].

- j JRE certificates key store password. If this command is not included, the JRE certificates keystore default password is used.
- k PKCS#8 private key file location.
- K PKCS#12 private key and certificate authority chain file location.
- M Subject Alternative Name e-mail addresses, such as email\_1 [email\_n].

## ThirdPartyCertificateTool usage examples

This section contains examples of commands that you can run using the **ThirdPartyCertificateTool**.

**Note:** The examples include the *keystore\_password* placeholder. This password must match the **Key store password** that is set in IBM Cognos Configuration, under **Security > Cryptography > Cognos**. The default key store password is NoPassWordSet. If you changed the default key store password, use the password that you specified.

The following list specifies the tasks that you can accomplish by using the **ThirdPartyCertificateTool**, and the related command syntax:

- Generate a certificate signing request (CSR).

```
ThirdPartyCertificateTool.(bat|sh) -c -e
[-p keystore_password] -a key_pair_algorithm
-r path_to_cert_or_csr
-d dn
[-H subject_alternative_nameDns_name_dn]
[-I subject_alternative_ip_addresses]
[-M subject_alternative_email_addresses]
```

- Import the crypto target certificate.

```
ThirdPartyCertificateTool.(bat|sh) -i -e [-p keystore_password]
-r path_to_cert_or_csr -t path_to_cert_chain
```

- Import the trusted certificate.

```
ThirdPartyCertificateTool.(bat|sh) -i -T [-p keystore_password]
-r path_to_cert_or_csr
```

- Import the crypto key using separate entries.

```
ThirdPartyCertificateTool.(bat|sh) -i -e [-p keystore_password]
-a key_pair_algorithm -r path_to_cert_or_csr
-t path_to_cert_chain
-w private_key_source_password -k path_to_PKCS#8
```

- Import the crypto key from PKCS#12.

```
ThirdPartyCertificateTool.(bat|sh) -i -e [-p keystore_password]
-a key_pair_algorithm -w private_key_source_password
-K path_to_PKCS#12
```

- Export the CA certificate.

```
ThirdPartyCertificateTool.(bat|sh) -E -T [-p keystore_password]
-r path_to_cert_or_csr
```

**Note:** If the built-in Cognos certificate authority (CA) is used, the export -E command exports the certificate that was issued by the local CA. This might not be the latest CA certificate, if one was remotely regenerated and both local certificates are still valid.

- Export the crypto certificate.

```
ThirdPartyCertificateTool.(bat|sh) -E -e [-p keystore_password]  
-r path_to_cert_or_csr
```

## Configuring Cognos Analytics to use another certificate authority (CA) certificate

You can configure IBM Cognos Analytics to use a certificate from an external certificate authority (CA) to establish the root of trust in the security infrastructure.

By default, Cognos Analytics uses its own CA for this purpose.

Use the following process to configure Cognos Analytics to use another certificate authority:

1. [“Delete the existing keystore” on page 200](#)
2. [“Create the certificate signing request \(CSR\) files” on page 200](#)
3. [“Import the certificate authority \(CA\) certificates” on page 202](#)
4. [“Enable the external certificate authority \(CA\) certificate” on page 203](#)

The configuration steps must be performed on each computer where the following Cognos Analytics components are installed: Content Manager, the Application Tier Components, the gateway, and the client components such as Framework Manager, and other components if you use them.

**Important:** The process of configuring an external certificate authority (CA) that is documented here doesn’t apply to IBM Cognos PowerPlay. For this product, you must use the CA process for the IBM Cognos Business Intelligence product, version 10.2.2. For more information, see the *IBM Cognos Business Intelligence PowerPlay Installation and Configuration Guide*, version 10.2.2.

### Delete the existing keystore

When configuring IBM Cognos Analytics to use an external certificate authority (CA), you must start with a stopped system and an empty keystore.

#### Procedure

1. Stop the Cognos Analytics service, and ensure that Cognos Configuration is closed.
2. From the Cognos Analytics *install\_location*\configuration\certs directory, delete the following files: CAMKeystore, CAMKeystore.bkup, and CAMKeystore.jks.

### What to do next

Continue with the following steps:

1. [“Create the certificate signing request \(CSR\) files” on page 200](#)
2. [“Import the certificate authority \(CA\) certificates” on page 202](#)
3. [“Enable the external certificate authority \(CA\) certificate” on page 203](#)

### Create the certificate signing request (CSR) files

To obtain a certificate from a certificate authority (CA), you must generate the certificate signing request (CSR) files for the crypto key from the Cognos Analytics keystore. The CA uses this file to produce a crypto certificate, and a CA certificate that you import into your keystore.

### Before you begin

On UNIX or Linux operating systems, ensure that you set a JAVA\_HOME environment variable before you use the [ThirdPartyCertificateTool](#).



On Microsoft Windows installations, you can run the tool with the `-java:local` command to use the JRE that is provided with the installation, as shown in the following example:  
`ThirdPartyCertificateTool.bat -java:local -c -d ...`

## About this task

If you changed the **Key store password** in IBM Cognos Configuration, under **Cryptography > cryptographic\_provider\_name**, use the new password as the *keystore\_password* when running the `ThirdPartyCertificateTool` commands below. The default password is **NoPasswordSet**.

## Procedure

1. From the *install\_location*\bin directory, run the **ThirdPartyCertificateTool**.
2. Type the following command to create the certificate signing request for the crypto key:

- On UNIX or Linux, type

```
ThirdPartyCertificateTool.sh -c -e -d "CN=EncryptCert,O=MyCompany,C=CA" -r  
encryptRequest.csr -p keystore_password -a RSA
```

- On Windows, type

```
ThirdPartyCertificateTool.bat -c -e -d "CN=EncryptCert,O=MyCompany,C=CA" -r  
encryptRequest.csr -p keystore_password -a RSA
```

The distinguished name (DN) value in the command ("CN=EncryptCert,O=MyCompany,C=CA") uniquely identifies the Cognos Analytics installation. The attributes that are used in this parameter reflect a hierarchical structure in your organization.

The password that you enter for this key must be used again when you import the certificate, and again in IBM Cognos Configuration.

3. Run the command.

You can ignore any warnings about logging.

**Important:** The certificates that are generated by your CA must be PEM (Base-64 encoded ASCII) format.

## Results

The command generates the following CSR files:

- The CAMKeystore file in the *install\_location*\configuration\certs directory.
- The `encryptRequest.csr` file in the *install\_location*\bin directory.

## What to do next

Continue with the following steps:

1. Share the crypto key file `encryptRequest.csr`, or its contents, with the external CA.

Using this key, the CA produces a crypto key certificate, a root certificate, and an intermediate certificate for the request, and shares them with your organization.

For details about the certificate exchange process between your organization and the external CA, see the third-party CA documentation.

2. Copy the certificates from the external CA to the Cognos Analytics installation directory, such as *install\_location*\configuration\bin.
3. Import the certificates into your Cognos Analytics keystore. For more information, see [“Import the certificate authority \(CA\) certificates” on page 202](#).

## Import the certificate authority (CA) certificates

You must import the certificates from the external certificate authority (CA) into your IBM Cognos Analytics keystore.

The import must be done on each computer where the following Cognos Analytics components are installed: Content Manager, the Application Tier Components, the gateway, and the client components such as Framework Manager, and other components if you use them.

### Before you begin

On UNIX or Linux operating systems, ensure that you set a `JAVA_HOME` environment variable before you use the **ThirdPartyCertificateTool**.

On Microsoft Windows installations, you can run the tool with the `-java:local` command to use the JRE that is provided with the installation, as shown in the following example:

```
ThirdPartyCertificateTool.bat -java:local -c -d ...
```

### About this task

If you changed the **Key store password** in IBM Cognos Configuration, under **Cryptography** > **cryptographic\_provider\_name**, use the new password as the *keystore\_password* when running the **ThirdPartyCertificateTool** commands below. The default password is `NoPassWordSet`.

### Procedure

1. Go to the location where you saved the certificate files from the CA authority, and do the following:
  - a) Create a copy of the crypto certificate, and name it `encryptCertificate.cer`.
  - b) Create a copy of the root CA certificate, and name it `ca.cer`.
2. If the files are not already there, copy the `encryptCertificate.cer`, and `ca.cer` files to the *install\_location/bin* directory.
3. From *install\_location/bin* directory, start the **ThirdPartyCertificateTool** command line tool.
4. Type the following command to import the CA root certificate into the Cognos Analytics trust store:

- On UNIX or Linux operating systems, type

```
ThirdPartyCertificateTool.sh -i -T -r ca.cer -p keystore_password
```

- On Windows operating systems, type

```
ThirdPartyCertificateTool.bat -i -T -r ca.cer -p keystore_password
```

The command reads the `ca.cer` file and imports the contents into the `CAMKeystore` file in the `certs` directory using the specified password.

5. Optional: If you use intermediate CA certificates, import all the intermediate certificates into the Cognos Analytics trust store by using the same commands as in step 4.
6. Import the crypto certificate into the Cognos Analytics encryption keystore by typing the following command:

- On UNIX or Linux operating systems, type

```
ThirdPartyCertificateTool.sh -i -e -r encryptCertificate.cer -p keystore_password -t ca.cer
```

- On Windows operating systems, type

```
ThirdPartyCertificateTool.bat -i -e -r encryptCertificate.cer -p keystore_password -t ca.cer
```

**Important:** Ensure that the *keystore\_password* is the same password that you entered when you exported the encryption key in the previous task.

You can ignore any warnings about logging.

## Results

The command reads the `encryptCertificate.cer` and `ca.cer` files in the `install_location\bin` directory and imports the certificates from both files into the `CAMKeystore` file in the `install_location/configuration/certs` directory using the specified password.

## What to do next

You can now configure the Cognos Analytics components to use the external CA certificates. For more information, see [“Enable the external certificate authority \(CA\) certificate” on page 203](#).

## Enable the external certificate authority (CA) certificate

Configure each computer where an IBM Cognos Analytics component is installed to use the external certificate authority (CA).

### Before you begin

Ensure that the following steps were completed:

1. [“Delete the existing keystore” on page 200](#)
2. [“Import the certificate authority \(CA\) certificates” on page 202](#)

### About this task

The keystore locations and passwords in IBM Cognos Configuration match the ones that you typed in **ThirdPartyCertificateTool**.

### Procedure

1. Open IBM Cognos Configuration as an administrator.
2. In the **Explorer** window, under **Cryptography**, right-click the current cryptographic provider name, and select **Delete**.  
**Note:** **Cognos** is the default cryptographic provider. However, it is possible to rename the default provider, so the provider name that you see might be different. This can also be an external provider name.
3. In the **Explorer** window, under **Security**, right-click **Cryptography**, then select **New resource > Certificate authority**.
4. In the **New Resource - Certificate authority** box, enter a name for the CA and, in the **Type(Group)** field, select **Third party certificate authority**.
5. For the **Key store password** property, enter the password that you used for the crypto key.
6. Click **File > Save** to save the configuration.
7. Start your Cognos Analytics service.

## Configuring Cognos Analytics to use an existing certificate authority (CA) certificate

You can configure Cognos Analytics to use an existing external certificate authority (CA) certificate and private key pair.

Using this process, you can also configure a corporate wildcard certificate, and a certificate that was issued by the CA without using the [ThirdPartyCertificateTool](#) to create the certificate signing request (CSR).

The configuration steps must be performed on each computer where the following Cognos Analytics components are installed: Content Manager, the Application Tier Components, the gateway, and the client components such as Framework Manager, and other components if you use them.

## Delete the existing keystore

When configuring IBM Cognos Analytics to use an existing external certificate authority (CA) certificate, you must start with a stopped system and an empty keystore.

### Procedure

1. Stop the Cognos Analytics service, and ensure that Cognos Configuration is closed.
2. From the Cognos Analytics *install\_location*\configuration\certs directory, delete the following files: CAMKeystore, CAMKeystore.bkup, and CAMKeystore.jks.

## What to do next

Continue with the following steps:

1. [“Import the existing certificate authority \(CA\) certificates” on page 204](#)
2. [“Enable the external certificate authority \(CA\) certificate” on page 203](#)

## Import the existing certificate authority (CA) certificates

You must import the existing certificates from the external certificate authority (CA) into your IBM Cognos Analytics keystore.

The import must be done on each computer where the following Cognos Analytics components are installed: Content Manager, the Application Tier Components, the gateway, and the client components such as Framework Manager, and other components if you use them.

## Before you begin

Ensure that:

- The existing [keystore is deleted](#).
- Your administrator provided you with the certificate and private key in a single pkcs12/pfx file.

## About this task

If you changed the **Key store password** in IBM Cognos Configuration, under **Cryptography > cryptographic\_provider\_name**, use the new password as the *keystore\_password* when running the [ThirdPartyCertificateTool](#) commands below. The default password is NoPassWordSet.

### Procedure

1. Go to the location where you saved the pkcs12/pfx file, and do the following:
  - a) Create a copy of the pkcs12/pfx file, and name it `encryptCertificate.pfx`.
  - b) Create a copy of the root CA certificate, and name it `ca.cer`.
  - c) Copy `encryptCertificate.pfx` and `ca.cer` to the *install\_location*/bin directory.
2. Start a command prompt and go to the Cognos Analytics *install\_location*/bin directory.
3. Type the following command to import the CA root certificate into the Cognos Analytics truststore:
  - On UNIX or Linux operating systems, type

```
ThirdPartyCertificateTool.sh -i -T -r ca.cer -p keystore_password
```

- On Windows operating systems, type

```
ThirdPartyCertificateTool.bat -i -T -r ca.cer -p keystore_password
```

The command reads the `ca.cer` file and imports the contents into the `CAMKeystore` file in the `certs` directory using the specified password.

4. Optional: If you have intermediate CA certificates, import all the intermediate certificates (ICA) into the Cognos Analytics trust store by using the same commands as in step 3.
5. Type the following command to import the preexisting certificate and private key into the Cognos Analytics keystore:

- On UNIX or Linux operating systems, type

```
ThirdPartyCertificateTool.sh -i -e -a RSA -p keystore_password -K encryptCertificate.pfx  
-w pfx_file_password
```

- On Windows operating systems, type

```
ThirdPartyCertificateTool.bat -i -e -a RSA -p keystore_password -K encryptCertificate.pfx  
-w pfx_file_password
```

## Results

The command reads the `encryptCertificate.pfx` and `ca.cer` files in the `install_location\bin` directory and imports the certificates from both files into the `CAMKeystore` file in the `install_location\configuration\certs` directory using the specified password.

## What to do next

You can now configure the Cognos Analytics components to use the certificates. For more information, see [“Enable the external certificate authority \(CA\) certificate” on page 205](#).

## Enable the external certificate authority (CA) certificate

Configure each computer where an IBM Cognos Analytics component is installed to use the certificate authority (CA).

### Before you begin

Ensure that the following steps were completed:

1. [“Delete the existing keystore” on page 204](#)
2. [“Import the existing certificate authority \(CA\) certificates” on page 204](#)

### About this task

The keystore locations and passwords in IBM Cognos Configuration must match the ones that you typed in **ThirdPartyCertificateTool**.

### Procedure

1. Open IBM Cognos Configuration as an administrator.
2. In the **Explorer** window, under **Cryptography**, right-click the cryptographic provider name, and select **Delete**.

**Note:** **Cognos** is the default cryptographic provider. However, it is possible to rename the default provider, so the provider name that you see might be different. This can also be an external provider name.

3. In the **Explorer** window, under **Security**, right-click **Cryptography**, then select **New resource > Certificate authority**.

4. In the **New Resource - Certificate authority** box, enter a name for the CA and, in the **Type(Group)** field, select **Third party certificate authority**.
5. For the **Key store password** property, enter the password that you used for the crypto key.
6. Click **File > Save** to save the configuration.
7. Start your Cognos Analytics service.

## Configuring the SSL protocol for IBM Cognos components

---

You can use the Secure Sockets Layer (SSL) protocol for communication between IBM Cognos components in single server and distributed installations.

### IBM WebSphere Liberty Profile 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 Liberty HTTP/1.1 and SSL Liberty HTTP/1.1 connectors are enabled in the `server.xml` file.

If the internal and external dispatcher URIs use different protocols or ports, the internal dispatcher port is accessible only to the components on the local computer. The internal dispatcher URI must also specify localhost.

### Single computer installations

In a single computer installation, if you are not currently using SSL, you must stop the service before changing the protocol to https. After you save the configuration with SSL settings, you can restart the services.

### Distributed installations

In distributed installation, you must first configure the default active Content Manager computer to use the SSL protocol and start the services on that computer before you configure the Application Tier and gateway components to use SSL.

### Add a computer to an installation

If you add a computer to an SSL-enabled environment, you will be prompted to temporarily accept trust for a certificate when you save the configuration. Accepting the temporary certificate will allow permanent trust to be established with the existing components.

### Add a component to a computer

If you add a component to an installation that has already been configured for SSL, the trust to the SSL certificates is inherited from the existing components. If you add the component to a different location on the same computer but to an environment already configured for SSL, you will be prompted to temporarily accept trust for a certificate when you save the configuration. Accepting the temporary certificate will allow permanent trust to be established with the existing components.

## Configuring SSL for Cognos Analytics components

For IBM Cognos components, you can use SSL for internal connections, external connections, or both.

If you configure SSL for internal connections only, IBM Cognos components on the local computer 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.

By default, IBM Cognos Analytics components use an internal certificate authority (CA) to establish the root of trust in the IBM Cognos security infrastructure. This applies to both SSL and non-SSL connections. If you want to use certificates that are managed by another service, see the topic [“Configuring Cognos Analytics to use another certificate authority \(CA\) certificate”](#) on page 200.

If you use an optional gateway (either HTTP or HTTPS), you must configure the web server to trust Cognos Analytics certificates. For more information, see [“Copying the IBM Cognos certificate to another server”](#) on page 209.

In a distributed installation, you must first configure the default active Content Manager computer to use the SSL protocol, and start the services on that computer before you configure the Application Tier Components computer.

## Before you begin

Starting with Cognos Analytics 11.1.7, it is recommended to configure dispatcher URIs to use https with fully qualified domain host name.

If for some reason you want to configure the external dispatcher and internal dispatcher to use different http schemas and ports, you need to update the `wlp/usr/servers/cognos/server.xml` file to open the internal dispatcher port to listen on all interfaces. Edit the `server.xml` file in the following way:

1. Search for `httpEndpoint` with `id = "defaultHttpEndpoint"`, and `host="localhost"`.

For example, if port 9400 was configured for **Internal dispatcher URI** in Configuration Manager, locate the following lines of code:

```
<httpEndpoint id="defaultHttpEndpoint" httpPort="9400" host="localhost">
  <httpOptions CookiesConfigureNoCache="false" AutoDecompression="false"
    removeServerHeader="true"
    persistTimeout="{persist.timeout}"/>
</httpEndpoint>
```

2. Change `localhost` to `*`, as shown in the following line of code:

```
<httpEndpoint id="*defaultHttpEndpoint" httpPort="9400" host="*/>
```

3. Save the `server.xml` file.
4. Ask your IT services to disable external access to the port that you used, 9400 in this example, if you want to do so.

## About this task

You must specify fully-qualified host names in the values for the following Cognos Configuration fields. Each value that you specify must also appear in either the **Subject Alternative Name > DNS names** field, or the **Subject Alternative Name > IP addresses** field.

- **Environment**
  - **Gateway URI**
  - **External dispatcher URI**
  - **Internal dispatcher URI**
  - **Dispatcher URI for external applications**
  - **Content Manager URIs**
- **Environment > Configuration Group**

- **Group contact host**
- **Member coordination host**
- **Security > Cryptography > Cognos**
  - **Server common name**
  - **Subject Alternative Name > DNS names**
  - **Subject Alternative Name > IP addresses**

## Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** pane, click **Environment**.

In the **Environment - Group Properties** pane, configure all the URIs with the fully-qualified domain name of the server, as required for the following SSL connection scenarios:

### SSL is used for all connections

Enter the same URI for **Internal dispatcher URI**, **External dispatcher URI**, and **Dispatcher URI for external applications** for external applications properties. Enter https and a port number for SSL communication.

Additionally, if Content Manager is also installed and enabled on the same instance, enter https and a port number for SSL communication in the **Content Manager URIs** property.

### Gateway is installed on a separate computer, and SSL is used for external connections on Application Tier dispatcher

Start IBM Cognos Configuration on the gateway computer. Enter https and the port number for SSL communication in the **Dispatcher URIs for gateway** property that points to the Application Tier dispatcher.

3. In the **Explorer** pane, click **Environment > Configuration Group**. Then, in the **Configuration Group - Component Properties** pane, do the following:
  - a) Set **Group contact host** to the fully-qualified domain name of the computer where your primary Content Manager is installed.
 

**Important:** Every computer, whether in the application tier or the data tier, should use the same value that is specified on the primary Content Manager computer.

If you are configuring the primary node for the configuration group, the value in this field must match the DNS name or IP address specified for the **Subject Alternative Name** in step 4b.
  - b) Set **Member coordination host** to the same fully-qualified domain name that you set in step 2.
4. In the **Explorer** pane, click **Security > Cryptography > Cognos**. Then, in the **Cognos - Provider - Resource Properties** pane, do the following:
  - a) Ensure that the **Server common name** value is the fully-qualified domain name of the server.
  - b) Under **Subject Alternative Name**, specify DNS names, IP addresses, and Email addresses (optional) that are associated with the server certificate.
 

**Important:** The DNS names and IP addresses must match the fully-qualified domain name in the environment URIs in step 2. If the server has multiple DNS names, you must enter each name, separated by a space. If the server has multiple IP addresses, you must enter each address, separated by a space.
5. From the **File** menu, click **Save**.
6. Restart your services.

In a distributed environment, start the services on the Content Manager computer first, followed by the services on the Application Tier Components computers.



## Set up shared trust between IBM Cognos servers and other servers

If you want to use the default IBM Cognos certificate authority, and you want to use SSL for connections from other servers to IBM Cognos servers, you must add the IBM Cognos certificate to the trust store on the other servers.

**Note:** If you use browsers to connect to IBM Cognos components, the browsers automatically prompt users to update their trust stores.

If you want the connection between IBM Cognos servers and the other server to be mutually authenticated, you must also copy the certificate from your certificate authority to the trust store for IBM Cognos servers.

If you have configured IBM Cognos components to use another certificate authority (CA), you do not have to set up shared trust between IBM Cognos server and other servers.

### Copying the IBM Cognos certificate to another server

To add the IBM Cognos certificate to the trust store on other servers, you need to copy the certificate to the server.

For multi-server environments, you need to export all Cognos Analytics authority certificates for every install containing an active Content Manager, and import them into target web servers, for which trust is needed.

#### Procedure

1. Go to the *install\_location/bin* directory.
2. Extract the IBM Cognos certificate by typing the following command:
  - On UNIX or Linux operating systems, type  
`ThirdPartyCertificateTool.sh -E -T -r destination_file -p NoPasswordSet`
  - On Microsoft Windows operating systems, type  
`ThirdPartyCertificateTool.bat -E -T -r destination_file -p NoPasswordSet`
3. Import the certificate to the trust store on your server.

For information on updating the server trust store, see the documentation for your server.

### Copying the CA certificate to IBM Cognos servers

After copying the IBM Cognos certificate to other servers, copy the certificate from the certificate authority to the IBM Cognos server.

Some servers that the IBM Cognos Analytics server needs to trust, have their certificates signed by a third-party Intermediate Certificate Authority (ICA). The ICA certificate can be signed either by one or more ICAs or by the final third-party Certificate Authority.

You need to import the full root of trust into the Cognos keystore, starting with the Root Certificate Authority, and each ICA involved in the signing of the server certificate that the CA certificate needs to establish trust with.

#### Procedure

1. Copy the certificate from your certificate authority to a secure location on the IBM Cognos server.  
Ensure that the CA certificate is in Base-64 encoded X.509 format.
2. Go to the *install\_location/bin* directory.
3. Import the CA certificate by typing the following command:
  - On UNIX or Linux operating systems, type the following:  
`ThirdPartyCertificateTool.sh -T -i -r CA_certificate_file -p NoPasswordSet`

- On Microsoft Windows operating systems, type

```
ThirdPartyCertificateTool.bat -T -i -r CA_certificate_file -p NoPassWordSet
```


## Select and rank cipher suites for Secure Socket Layer

An SSL connection begins with a negotiation in which the client and server present a list of supported cipher suites in a priority sequence. A cipher suite provides the quality of protection for the connection. It contains cryptographic, authentication, hash, and key exchange algorithms. The SSL protocol selects the highest priority suite that the client and the server both support.

A list of supported cipher suites for SSL is provided. You can eliminate cipher suites that do not meet your requirements and then assign a priority, or preference, to the remaining cipher suites. The selected cipher suites are presented in priority sequence for the client and server sides of the negotiation. At least one of the selected cipher suites between the client and server platforms must match.

The list of supported cipher suites is dynamically generated on each computer, and depends on the Java Runtime Environment (JRE) or whether you have other cryptographic software installed on the computer. If you have made changes to a computer, such as upgraded the JRE or installed software that has upgraded the JRE, this may affect the supported cipher suites available on that computer. If you no longer have a supported cipher suite that matches the other computers in your environment, you may have to change the JRE on the computer to match the other computers in your environment.

### Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Cryptography**.
3. In the **Properties** window, click the **Value** column for the **Supported ciphersuites** property.
4. Click the edit icon .
  - To move a cipher suite to the **Current values** list, click the check box in the **Available values** list and then click **Add**.
  - To move a cipher suite up or down in the **Current values** list, click the check box and then click the up or down arrows.
  - To remove a cipher suite from the **Current values** list, click the check box and then click **Remove**.
5. Click **OK**.
6. From the **File** menu, click **Save**.

## Using the SSL protocol for database communications

You can enable the secure sockets layer (SSL) protocol for communications between IBM Cognos Analytics and databases that are used by the **Content Manager**, **Notification**, **Mobile**, **Human Task** and **Annotation Services**, and **Logging** services.

The databases must already be configured for use with IBM Cognos Analytics. For more information about configuring the supported databases, see the following topics: [“Guidelines for creating the content store”](#) on page 10, [“Change the notification database”](#) on page 195, and [“Guidelines for creating a logging database”](#) on page 220.

SSL must be enabled on the database server, and the database client must be configured to use SSL connections to the database server before you enable SSL encryption in IBM Cognos Configuration.

For more information, review your database vendor documentation and verify which SSL properties must be specified for the different database versions.

## Enabling SSL for communications with Microsoft SQL Server databases

You can enable secure sockets layer (SSL) protocol for communications between IBM Cognos Analytics and Microsoft SQL Server databases.

The databases that can be configured are the **Content Manager**, **Notification**, **Mobile**, **Human Task and Annotation Services**, and **Logging** databases.

For more information about configuring SQL Server for SSL, see the documentation for your version of Microsoft SQL Server.

**Note:** Microsoft SQL server uses different driver JAR file names, such as `sqljdbc4.jar`, `sqljdbc41.jar`, and `sqljdbc42.jar`. Officially, `sqljdbc42.jar` supports JRE8, which is the version that is used by IBM Cognos Analytics.

### Before you begin

Ensure that you enable SSL on your database server before you perform the steps in IBM Cognos Configuration.

### Procedure

1. Obtain the root Certificate Authority (CA) certificate that issued your SQL Server certificate, and copy the CA certificate to the computer where Cognos Analytics is installed, to a location that's easy to access. For example, if the certificate name is `sqlcert.cer`, the location can be `c:\sqlcert.cer`.

Then, from a command line tool, run the following command:

```
C:\Progra~1\ibm\cognos\analytics\ibm-jre\jre\bin\keytool
-import -trustcacerts -file "c:\sqlcert.cer"
-keystore C:\Progra~1\ibm\cognos\analytics\ibm-jre\jre\lib\security\cacerts
-alias SQLCert
```

**Note:** The example uses the default Cognos Analytics installation location.

2. Edit the `install_location\bin64\cogconfig.bat` (Windows) or `install_location\bin64\cogconfig.sh` (Linux, UNIX) file by adding the following line after the line `set J_OPTS=%DD_OPTS% %J_OPTS%`:

Windows:

```
set J_OPTS="-Dcom.ibm.jsse2.overrideDefaultTLS=true" %J_OPTS%
```

Linux, UNIX:

```
JAVA_OPTS=$JAVA_OPTS -Dcom.ibm.jsse2.overrideDefaultTLS=true
```

3. Start IBM Cognos Configuration by double-clicking the `cogconfig` file that you modified in step 3.
4. Under **Data Access**, click the database name that you want to configure. For example, to configure the content store database, under **Content Manager**, click the database name.

Other databases that can be configured are **Notification**, **Mobile**, **Human Task and Annotation Services**, and **Logging**.

**Tip:** To configure the **Logging** database, go to **Environment > Logging**.

5. In the properties pane, click the **SSL Encryption Enabled** property, and set its value to **True**.
6. Test the connection, and save your configuration.
7. Start IBM Cognos Analytics. The full server name in SQL Server Configuration Manager must match the name in the certificate. For example, `mycomputer.canlab.ibm.com`, and not `localhost`.

## Enabling SSL for communications with Db2 and Informix databases

You can enable secure sockets layer (SSL) protocol for communications between IBM Cognos Analytics and IBM Db2 and Informix Dynamic Server databases.

The databases that can be configured are the **Content Manager**, **Notification**, **Mobile**, **Human Task and Annotation Services**, and **Logging** databases.

### Before you begin

Ensure that you enable SSL on your database server before you perform the steps in IBM Cognos Configuration.

### Procedure

1. Follow the documentation for your database version to enable SSL for the database server and to export the SSL certificate.
2. Obtain the root Certificate Authority (CA) certificate, as well as any intermediate certificate authority certificates, and copy them to the computer where Cognos Analytics is installed, in a location that's easy to access.
3. For each certificate that you copied to your computer, run this command:

```
installation_location\ibm-jre\jre\bin\keytool
-import -trustcacerts -file "certificate_location\certificate_name.crt"
-keystore C:\Progra~1\ibm\cognos\analytics\ibm-jre\jre\lib\security\cacerts
-alias alias
```

#### Notes:

- If you are importing more than one certificate, ensure that you specify a unique alias for each certificate.
- If you are prompted for a keystore password, type `changeit`, which is the default password for the JVM keystore.

#### Example

You want to import, to the root folder of your C drive, two certificates:

- a Root CA certificate, `rootca.crt`
- an Intermediate certificate, `myteam_int.crt` for use by your team

For the Root CA certificate, type the following:

```
C:\Progra~1\ibm\cognos\analytics\ibm-jre\jre\bin\keytool
-import -trustcacerts -file "c:\rootca.crt"
-keystore C:\Progra~1\ibm\cognos\analytics\ibm-jre\jre\lib\security\cacerts
-alias rootca
```

For the Intermediate certificate, type the following:

```
C:\Progra~1\ibm\cognos\analytics\ibm-jre\jre\bin\keytool
-import -trustcacerts -file "c:\myteam_int.crt"
-keystore C:\Progra~1\ibm\cognos\analytics\ibm-jre\jre\lib\security\cacerts
-alias myteam_int
```

4. Start IBM Cognos Configuration.
5. Under **Data Access**, click the database name that you want to configure. For example, to configure the content store database, under **Content Manager**, click the database name.

Other databases that can be configured are **Notification**, **Mobile**, **Human Task and Annotation Services**, and **Logging**.

**Tip:** To configure the **Logging** database, go to **Environment > Logging**.

6. In the properties pane, click the **SSL Encryption Enabled** property, and set its value to **True**.
7. Test the connection.

8. Save your configuration, and restart your IBM Cognos Analytics services.

## Enabling SSL for communications with Oracle databases

You can enable secure sockets layer (SSL) protocol for communications between IBM Cognos Analytics and Oracle databases.

The following databases can be configured: **Content Manager**, **Notification**, **Mobile**, **Human Task and Annotation Services**, and **Logging**.

To use secure sockets layer (SSL) with Oracle database connections in IBM Cognos Analytics, you must import the SSL certificate to the Java keystore.

### Before you begin

Ensure that you enable SSL on your database server before you perform the steps in IBM Cognos Configuration.

**Tip:** The database type must be **Oracle database (Advanced)**, not **Oracle database**.

### About this task

The configuration settings that you need to specify depend on the version of Oracle JDBC driver that is supported by your version of the Cognos Analytics server. Refer to [this article](http://www.ibm.com/support/pages/node/6989513) (www.ibm.com/support/pages/node/6989513) to view a list of supported JDBC drivers that are regularly tested with 12.0.x versions of Cognos Analytics. For information about specific versions of JDBC drivers, see the Oracle documentation.

### Procedure

1. Edit the `bootstrap_wlp_os_version.xml` file.

This file is used when you start Cognos Analytics as a service from IBM Cognos Configuration.

**Tip:** Using double quotation marks in the `bootstrap_wlp_linux38664.xml` file prevents IBM Java from starting, and causes Cognos startup to hang and fail.

- a) Go to the `install_location/bin64` directory, and open the `bootstrap_wlp_os_version.xml` file in a text editor.
- b) Under the `<process>`, `<start>`, `<spawn>` element, specify the Java system properties that are required by the Oracle JDBC driver version that is supported by your version of Cognos Analytics. For information about specific versions of JDBC drivers, see the Oracle documentation.

For example, you might add the following lines of code in `bootstrap_wlp_os_version.xml`:

```
<param>-Doracle.net.ssl_client_authentication=false</param>
<param>-Doracle.net.ssl_version=1.2</param>
<param>-Djavax.net.ssl.trustStore=/app/my_wallet/truststore.jks</param>
<param>-Djavax.net.ssl.trustStoreType=JKS</param>
<param>-Djavax.net.ssl.trustStorePassword=my_wallet_password</param>
```

**Tip:** This example works only for a specific version of Cognos Analytics and Oracle database. For your environment, you will likely need to specify different settings.

- c) Save and close the `bootstrap_wlp_os_version.xml` file.
2. Edit the `cogconfig` file.
    - a) From the `install_location/bin64` directory, open the `cogconfig.bat` (`cogconfig.sh` on UNIX or Linux) file in a text editor.
    - b) Add the Java system properties, as required by the Oracle JDBC driver version that is supported by your version of Cognos Analytics. For information about specific versions of JDBC drivers, see the Oracle documentation.

To continue with the example in step 1b, in the `cogconfig.bat` file, add the following lines of code below `set J_OPTS=%DD_OPTS% %J_OPTS% %DEBUG_OPTS%`:

```
set J_OPTS=-Doracle.net.ssl_client_authentication=false %J_OPTS%
set J_OPTS=-Djavax.net.ssl.trustStore=/app/my_wallet/truststore.jks %J_OPTS%
set J_OPTS=-Djavax.net.ssl.trustStoreType=JKS %J_OPTS%
set J_OPTS=-Djavax.net.ssl.trustStorePassword=my_wallet_password %J_OPTS%
set J_OPTS=-Doracle.net.ssl_version=1.2 %J_OPTS%
```

In `cogconfig.sh`, add the following lines:

```
JAVA_OPTS="$JAVA_OPTS -Doracle.net.ssl_client_authentication=false"
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStore=/app/my_wallet/truststore.jks"
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStoreType=JKS"
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStorePassword=my_wallet_password"
JAVA_OPTS="$JAVA_OPTS -Doracle.net.ssl_version=1.2"
```

- c) Save and close the `cogconfig` file.
3. Copy the required Oracle driver files to the Cognos Analytics *install\_location/drivers* directory.
4. Start IBM Cognos Configuration by double-clicking the `cogconfig` file that you modified in step 2.
5. Under **Data Access**, click the database name that you want to configure. For example, to configure the content store database, under **Content Manager**, click the database name.  
**Tip:** To configure the **Logging** database, go to **Environment > Logging**.
6. In the properties pane, click the **SSL Encryption Enabled** property, and set its value to **True**.
7. Test the connection.
8. Save your configuration, and restart your Cognos Analytics service.

## Configure JDBC data source connections for single sign-on using Kerberos

You can configure single sign-on using the Kerberos protocol for JDBC data source connections that are used for dynamic query mode (DQM).

Except for Microsoft SQL Server, single sign-on data source authentication is supported only for dynamic query mode.

Support for constrained delegation (a Microsoft extension to Kerberos), allows a service to obtain a ticket for another service on behalf of the user by presenting the user's service ticket to itself. The service ticket is either delegated from the user (Service for User to Proxy - S4U2Proxy), or generated by the service itself when user is authenticated by different means.

To configure a data source for single sign-on authentication using Kerberos, you must

- Create a Kerberos initialization file.
- Configure a service principal name (SPN) for the dynamic query mode data source.
- Create a keytab file.
- Configure the Kerberos login module.
- Configure data source connections.

Before you start, you must ensure that the following conditions are met:

1. The IBM Cognos service is configured for single sign-on using a Microsoft Active Directory namespace.
2. The database is configured to use the Kerberos protocol.
3. The Active Directory users are also configured on the database server.

4. If single sign-on is configured with constrained delegation, check the driver documentation to ensure the driver supports constrained delegation. Not all drivers that support Kerberos authentication also support constrained delegation.

Dynamic query supports Kerberos constrained delegation with the JDBC drivers for Netezza and Cloudera Impala. This capability requires JDBC drivers of the following versions or higher which have been enhanced to receive GSS credentials.: Netezza 7.2.0.9-P3 and 7.2.1.3-P3 (see <http://www-01.ibm.com/support/docview.wss?uid=swg21997658> for more information), and Cloudera Impala 2.5.36

IBM Cognos Analytics can be used with either an ORACLE or IBM JRE. The versions IBM requires are found in the [supported environments](#) page. Persons trying to use Cognos Analytics with an IBM JRE and Cloudera Impala JDBC would need to use IBM JRE 8.0.3.12 or above. See <https://developer.ibm.com/javasdk/downloads/sdk8/>.

## Using Kerberos authentication without single sign-on

If you don't configure Active Directory namespace, you still can configure your data source for Kerberos authentication. The dynamic query mode query service interprets the credentials that you provide (user name and password) as the credentials for obtaining a ticket granting ticket (TGT) from the Kerberos Distribution Center (Active Directory or another Kerberos implementation). These credentials can be provided through a signon or entered by the user when prompted for database credentials. In this case, configuration steps change as follows:

- You do not have to register an SPN.
- You do not have to create a keytab file.
- You **do not** have to configure the Kerberos Login Module.
- You have to supply a Kerberos initialization file.

## Editing the `bootstrap_wlp_*.xml` file for Oracle connections with Kerberos SSO

To use Kerberos single sign-on (SSO) with Oracle data server connections, you must add the Oracle JVM arguments to the IBM Cognos Analytics `bootstrap_wlp_os_version.xml` file before you configure the connection in the administration interface.

This file is used when you start IBM Cognos Analytics as a service from IBM Cognos Configuration.

### Procedure

1. From the `install_location/bin64` directory, open the `bootstrap_wlp_os_version.xml` file in a text editor.

The full file name depends on the operating system. For example, on Linux it's `bootstrap_wlp_linuxi38664.xml`, and on Windows it's `bootstrap_wlp_winx64.xml`.

**Tip:** Using double quotation marks in the `bootstrap_wlp_linux38664.xml` file prevents IBM Java from starting, and causes Cognos startup to hang and fail.

2. Under `<process>`, `<start>`, `<spawn>` elements, add the following lines after the memory-related `<param>` elements:

```
<param>-Djava.security.krb5.conf=/etc/krb5.conf</param>
<param>-Dsun.security.krb5.debug=true</param>
<param>-Doracle.net.kerberos5_mutual_authentication=true</param>
<param>-Doracle.net.authentication_services="(KERBEROS5)"</param>
```

The lines must be placed exactly as shown in the following snippet from the `bootstrap_wlp_*.xml` file:

```
<process name="wlp">
  <start>
    <spawn sync="1" wait_time="5">

      <path>${java_home}/bin/java</path>

      <param condName="${ip_protocol}" condValue="IPv6">-
Djava.net.preferIPv6Addresses=true</param>
      <param condName="${java_vendor}" condValue="IBM">-Xgcpolicy:gencon</param>
      <param condName="${java_vendor}" condValue="Sun">-XX:MaxNewSize=$
{dispatcherMaxMemoryBy2}m</param>
      <param condName="${java_vendor}" condValue="Sun">-XX:NewSize=$
{dispatcherMaxMemoryBy3}m</param>
      <param condName1="${java_vendor}" condValue1="Sun" condName2="${java_version}"
condValue2="1.8.0"
      condOp2="lt">-XX:MaxPermSize=128m</param>
      <param condName="${java_vendor}" condValue="Oracle">-XX:MaxNewSize=$
{dispatcherMaxMemoryBy2}m</param>
      <param condName="${java_vendor}" condValue="Oracle">-XX:NewSize=$
{dispatcherMaxMemoryBy3}m</param>
      <param condName1="${java_vendor}" condValue1="Oracle" condName2="${java_version}"
condValue2="1.8.0"
      condOp2="lt">-XX:MaxPermSize=128m</param>
      <param condName="${java_vendor}" condValue="IBM">-Xms512K</param>

      <!-- sso support -->
      <param>-Djava.security.krb5.conf=/etc/krb5.conf</param>
      <param>-Dsun.security.krb5.debug=true</param>
      <param>-Doracle.net.kerberos5_mutual_authentication=true</param>
      <param>-Doracle.net.authentication_services="(KERBEROS5)"</param>
      <!-- end sso support -->

      <param condName="${ip_protocol}" condValue="IPv4">-Djava.net.preferIPv4Stack=true</
param>
```

3. Save and close the file.
4. Go to the Cognos Analytics administration interface to continue configuring the Oracle data server for Kerberos SSO. For more information, see [“Configuring data source connections when using Kerberos” on page 219](#).

## Creating Kerberos initialization files

You must create a Kerberos initialization file and place it in a specific location on all computers with Application Tier Components installed. The Kerberos initialization file, `krb5.conf` is used by the JRE Kerberos protocol implementation.

For more information about Kerberos initialization files, see the [MIT Kerberos Documentation](http://web.mit.edu/kerberos/krb5-devel/doc/admin/conf_files/krb5_conf.html) ([web.mit.edu/kerberos/krb5-devel/doc/admin/conf\\_files/krb5\\_conf.html](http://web.mit.edu/kerberos/krb5-devel/doc/admin/conf_files/krb5_conf.html)).

### Procedure

On all computers where you have Application Tier Components installed, copy the `krb5.conf` file to the `JAVA_HOME/lib/security` directory.

On computers running UNIX, copy the `krb5.conf` file to the `/etc/krb5` directory.

On computers running Linux, copy the `krb5.conf` file to the `/etc` directory.

On computers running Microsoft Windows, copy the `krb5.conf` file to the `C:\Windows` directory, and rename it to `krb5.ini`



## Creating an SPN for the query service

You must create a service principal name (SPN) for the query service to use. The SPN must be configured with an Active Directory domain user that is trusted for delegation.

The SPN must be formatted as `spn@REALM`. The `spn` value is formatted as *service name/fully qualified domain name*. And `REALM` is the realm name that is configured in the Kerberos initialization file. For example, if `dqm` is the service name, `dqm/myserver.mydomain.com@MYWINDOWSDOMAIN.COM`.

If your Active Directory domain user is named `dqmuuser`, you would register the SPN by using the following command:

```
setspn -s dqm/myserver.mydomain.com mywindowsdomain\dqmuuser
```

You can use the **-L** and **-Q** parameters to verify that the SPN was created correctly. For example:

```
setspn -L mywindowsdomain\dqmuuser
```

```
setspn -Q dqm/myserver.mydomain.com
```

## Creating a keytab file

After you create the SPN, you must create a keytab file for the service. The keytab file allows the service to log in without a password. The keytab file must be re-created if the service account password changes.

### Procedure

Use the following command to create a keytab file:

```
ktpass -out krb5.keytab -princ SPN -mapUser username -mapOp set -pass password  
-pType KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

For example,

```
ktpass -out krb5.keytab -princ dqm/myserver.mydomain.com@mywindowsdomain.com  
-mapUser dqmuuser@mywindowsdomain -mapOp set -pass password -pType  
KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

## Configuring the Kerberos login module

You must configure the Kerberos login module to allow the IBM Cognos query service to log in to the Active Directory domain. To allow the log in the Java Authentication and Authorization Service (JAAS) package requires a configuration file.

There are two possible procedures in configuring the login modules.

To configure the login module for Kerberos with single sign-on (Active Directory):

1. In Cognos Configuration, select the Active Directory namespace in **Security > Authentication**.
2. In the **DQM Service Principal Name** property, enter the value exactly as it is listed in the keytab.  
Use the command **klist -k <keytab file>** to find the principal name.
3. Rename the keytab file to `ibmcognosba.keytab`, and place it in the `install_location/configuration` folder.

Cognos Analytics will dynamically create the necessary login configuration.

A configuration file must be included in the `java.security` file in the `JRE_HOME/lib/security` directory. You must include a line such as the following in the `java.security` file.

```
login.config.url.1=file:///{$java.home}/lib/security/jaas.conf
```

JAAS configuration examples are provided in the IBM Cognos installation. The example files are named `jaas-ibm.config` and `jaas-oracle.config`, and the files are in the `install_location/configuration` directory.

In the example files, you must replace the following values:

- *<principal name>* is the SPN that you created.
- *<keytab file specification>* is the path and file name of the keytab file that you created.

If you are not using a database connection that is configured for Kerberos authentication for modeling, then instead of modifying the `java.security` file, you can specify the JAAS login configuration file as an additional startup parameter for query service in IBM Cognos Administration. In IBM Cognos Administration, under **System**, expand your server, select **Query Service > Set Properties > Settings**, and enter the value in **Additional JVM arguments for the query service** in the form `-Djava.security.auth.login.config=<configuration file>`

## Verifying the Kerebos configuration

To verify the Java Authentication and Authorization Service (JAAS) configuration and the keytab file, you can run a command using the **java** command from the JRE that Cognos Analytics is using.

### Procedure

Run the following command from `install_location/webapps/p2pd/WEB-INF/lib`

```
java -cp xqeService.jar -Dcom.ibm.security.krb5.Krb5Debug=all  
-Dcom.ibm.security.jgss.debug=all com.cognos.xqe.util.KerberosSSOLoginHelper
```

The utility will attempt a login using the keytab file, and in the process will display the Kerberos debug output. At the end, it will display `Helper login successful` or `Helper Login failed <error message>`.

## Verifying the JDBC driver capabilities

Regardless of whether single sign-on is configured or not, DQM requires that the database driver can create connections using a pre-authorized subject. There is a utility that comes with the IBM Cognos Analytics installation which can help test the driver.

### Before you begin

The utility accepts **url**, **uid** and **password** as parameters. The driver must be installed in the `install_location/webapps/p2pd/WEB-INF/lib` folder.

### Procedure

From the `install_location/webapps/p2pd/WEB-INF/lib` folder, using the java command from the jre Cognos is using, run the following command:

```
java -cp xqeService.jar;<driver.jar>  
com.cognos.xqe.util.KerberosConnectionHelper <driver class name> <jdbc url>  
<user> <password>
```

where:

- *<driver.jar>* is the jar file containing the driver. If the driver has too many jar files, you can specify `"*"` for the classpath parameter.
- *<driver class name>* is the class name used to load the driver.
- *<jdbc url>* is the JDBC connection URL for the data source, including the driver-specific properties for Kerberos authentication.
- *<user>* is the Kerberos principal.
- *<password>* is the Kerberos principal password.

The utility tries to connect to the database using the supplied parameters, and outputs the Kerberos debug trace.

## Configuring data source connections when using Kerberos

Use the guidelines in this topic when configuring the connection strings for data source connections using Kerberos single sign-on.

### Procedure

1. In the Signon section, select **external namespace** and select the Active Directory namespace from the list. For dual tab (Native and JDBC) connection strings, the Signon section is on the Native tab.
2. In the **Connection properties** field, specify `ibmcognos.authentication=java_krb5`, and then add the properties required by the JDBC driver for Kerberos authentication, if any. For data source connections with dual tab (Native and JDBC), this field is on the **JDBC** tab and is called **JDBC Connection Parameters**.

If IBM Cognos Analytics is installed on a computer that are running Microsoft Windows operating systems, you do not have to specify `ibmcognos.authentication=java_krb5` for Microsoft SQL Server and Teradata data source connections.

3. Test the data source connection.

### Example

The following are examples for data source connection properties for some data sources:

- For Teradata data source connections:  
`ibmcognos.authentication=java_krb5;LOGMECH=KRB5;`
- For SAP-HANA data source connections:  
`ibmcognos.authentication=java_krb5;`
- For Microsoft SQL Server data source connections:  
`ibmcognos.authentication=java_krb5;authenticationScheme=JavaKerberos;`

## Configuring a repository for log messages

Log messages are an important diagnostic tool for investigating the behavior of IBM Cognos Analytics.

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 `install_location/logs` folder on every IBM Cognos Analytics computer that contains Content Manager or Application Tier Components. Because the log server uses a different port from the other IBM Cognos Analytics components, it continues to process events even if other services on the local computer, such as the dispatcher, are disabled.

The following workflow shows the tasks that are required to prepare for logging.

- During planning, determine the logging configuration that is suitable for your environment. For example, evaluate various log message repositories, such as remote log servers and log files, such as the UNIX or Linux syslog or the Windows NT Event log, in addition to the local log file. You can also send only audit logging information to a database. Consider security, such as methods available for protecting log files from system failures and user tampering.
- 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 Analytics computers. You can also enable certain logging features, such as user-specific logging.

- 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 more information, see the *IBM Cognos Analytics Manage Guide* and *IBM Cognos Analytics Administration and Security Guide*.

For information about using log messages to solve problems and resolving logging-related issues, see the *IBM Cognos Analytics Troubleshooting Guide*.

## Guidelines for creating a logging database

You can create a database to store log messages. Creating a logging database involves the following tasks:

- Create a logging database.

For IBM Db2, Oracle, Microsoft SQL Server, use the same procedure that was used to create the content store database. Use the instructions in [“Guidelines for creating the content store” on page 10](#).

**Note:** If you are using Db2, you cannot generate a script to create the notification database in the same way as you can the content store.

For Db2 on z/OS, use the instructions in [“Suggested settings for creating a logging database on Db2 on z/OS” on page 220](#).

- Set up the database connectivity.

Use the instructions in [“Database connectivity for the logging database” on page 221](#).

- Specify the log messages repository.

Use the instructions in [“Log message repositories” on page 223](#).

## Suggested settings for creating a logging database on Db2 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 on z/OS.

- \_\_\_ • Log on to the z/OS system as a user with administrator privileges on 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 on 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 a logging database on Db2 on z/OS” on page 220](#).

## Create tablespaces for a logging database on Db2 on z/OS

If you are using IBM Db2 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 6 characters. For more information, see the Db2 Knowledge Center.

## Procedure

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 `install_location/configuration/schemas/logging/db2zos` directory.

3. Open the `LS_tablespace_db2z0S.sql` script file and use the following table to help you to replace the generic parameters with ones appropriate for your environment.

Table 24. Tablespace parameter names and descriptions for a logging database on Db2 on z/OS	
Parameter Name	Description
IPFSCRIPT_DATABASE	The name of the logging database.
IPFSCRIPT_STOGROUP	The name of the storage group.
IPFSCRIPT_TABLESPACE	The name of the tablespace that contains the base tables in the logging database. This tablespace is not for Auxiliary tables.
IPFSCRIPT_LS_ID	The instance identifier for the audit database. This value must not be longer than two characters.
IPFSCRIPT_BP	The name of the 8 k buffer pool that is allocated for regular objects.
IPFSCRIPT_USERNAME	The user account that accesses the logging database.

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

4. Save and run the script.
5. Grant the IBM Cognos user rights to the tablespaces that were created when you ran the script file:
  - Open the `LS_rightsGrant_db2z0S.sql` script file.
  - 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_db2z0S.sql` script.

## Results

The logging database is created.

## 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, IBM Db2, Informix Dynamic Server as the database server.

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, and Db2, the appropriate JDBC driver and/or database client software is required only on the Application Tier Components computer with the remote log server that connects to the logging database.

## Microsoft SQL Server

If you use a Microsoft SQL Server database, the `JSQLConnect.jar` file is installed to the appropriate location by default. The only additional step is to ensure that the Microsoft SQL Server uses TCP/IP connectivity.

## Set up database connectivity for an IBM Db2 logging database

You must set up the database client software and the JDBC driver on all Application Tier Components computers with a connection to the logging database. You must set up the JDBC driver on the Content Manager computer, unless you are using the same type of database for the log messages as you use for the content store.

The driver version must be at least JCC 3.7 for a Linux or UNIX operating system, or for a Microsoft Windows operating system version 9.1 fix pack, or JCC 3.42 for a Linux, UNIX operating system, or for a Microsoft Windows operating system version 9.5 fix pack 2.

### Procedure

Copy the following files from *DB2\_installation\sqllib\java* directory to the *install\_location\drivers* directory:

- The universal driver file, *db2jcc4.jar*
- The license file:

For Db2 on Linux, UNIX, or Windows operating systems, use *db2jcc\_license\_cu.jar*.

For Db2 on z/OS, use *db2jcc\_license\_cisuz.jar*.

If you are connecting to Db2 on z/OS, use the driver version from Linux, UNIX, or Windows version 9.1 fix pack 5 or version 9.5 fix pack 2.

**Tip:** To check the driver version, run the following command:

```
java -cp path\db2jcc4.jar com.ibm.db2.jcc.DB2Jcc -version
```

## Set up database connectivity for an Oracle logging database

You must set up the JDBC driver on all Application Tier Components computers with a connection to the logging database. You must also set up the JDBC driver on the Content Manager computer, unless you are using the same type of database for the log messages as you use for the content store.

### Procedure

1. On the computer where the Oracle client is installed, go to the *ORACLE\_HOME/jdbc/lib* directory.
2. Copy the correct library file for your version of the Oracle client to the *install\_location\drivers* directory on the computer where Content Manager is installed and where notification is sent to an Oracle database.

If you are using Oracle version 12c Release 2, you must have the *ojdbc8.jar*.

If you are using Oracle version 12c Release 1, you must have the *ojdbc7.jar*.

If you are using Oracle version 11g Release 2, you must have the *ojdbc6.jar*.

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

## Set up database connectivity for an Informix logging database

You must set up the JDBC driver on all Application Tier Components computers with a connection to the logging database. You must also set up the JDBC driver on the Content Manager computer, unless you are using the same type of database for the log messages as you use for the content store.

### Procedure

1. On the computer where Informix is installed, go to the *Informix\_location/sqllib/java* directory.

2. Copy the following files to the *install\_location*\drivers directory on every computer where Content Manager is installed.
  - the universal driver file, db2jcc4.jar
  - the license file, db2jcc4\_license\_cisuz.jar

## Log message repositories

A local log server is automatically installed when you install Content Manager or the Application Tier Components. You can specify one or more repositories where the local log server sends log messages.

### Sending log messages to a remote log server

In a distributed installation, you can configure the log server on each IBM Cognos computer to send log messages to a single remote log server, which acts as a common log server. You can then configure the common log server to send the log messages to a local file or database on the same or different computer.

If the remote log server becomes unavailable, log messages are redirected to recovery files on the local computer in the *install\_location*/logs/recovery/remote directory. These recovery files have timestamp information in their file names, and are not readable like regular log files. When the remote log server becomes available, an automatic recovery process moves all log information to the remote log server and deletes the local log files.

### Saving log messages to a file

The log server is configured by default to send log messages to the *install\_location*/logs/cogaudit.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 *install\_location*/logs directory, you must ensure the path to the log file exists before starting the IBM Cognos service. For example, if you configure the log server to send messages to the /usr/lpp/logfiles/cognos.log file, IBM Cognos attempts to automatically create the cognos.log file in the /usr/lpp/logfiles folder. If this folder does not exist, IBM Cognos does not create the cognos.log file and no log messages can be recorded in it. Note that these log messages are not recorded in the default log file. Although IBM Cognos automatically creates the default log file even when another log file is configured, the default log file is not used as a backup.

### Saving log messages to a database

The log server can also send audit logs to a database on the same or another computer. Audit logs provide information about user and report activity.

The logging database has the same configuration and user account requirements as the content store database. After you configure IBM Cognos components to send messages to a logging database, and restart the IBM Cognos service, IBM Cognos components create the required tables and table fields. You can test the connection to the logging database before you restart the IBM Cognos service.

## Specify the Log Messages Repository for IBM Db2 on UNIX, Linux, or Windows

You can configure a type of repository for the log messages, and then configure properties for the specific repository. You can also configure more than one repository for log messages.

## Before you begin

Before you specify a database as a repository, ensure that you

- \_\_ • [created the logging database](#)
- \_\_ • [set up the database client](#)

## Procedure

1. On the computer where you installed Content Manager or the Application Tier Components, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Environment**, click **Logging**.
3. In the **Properties** window, use the following table to help set the log server properties.

Table 25. Log server properties	
Task	Action
Use TCP between IBM Cognos components on a computer and its local log server	Set the <b>Enable TCP</b> property to <b>True</b> .  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.
Change the number of threads available to the local log server	Type the value in the <b>Local log server worker threads</b> 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.

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

- Test the connection to the new database. In the **Explorer** window, under **Environment**, right-click **Logging** and click **Test**.

IBM Cognos components connect to the database. If you configured more than one database for logging messages, IBM Cognos components test all the databases.

10. Repeat steps 5 to 10 for each repository to which you want the log server to send messages.
11. From the **File** menu, click **Save**.
12. In the **Explorer** window, click **IBM Cognos services > IBM Cognos**.
13. From the **File** menu, click **Restart**.

If you selected a database as the repository, IBM Cognos components create the required tables and fields in the database that you created.

## Results

If the repository was a remote log server, configure and start the remote log server. Then restart the IBM Cognos service on the local computer.

If the repository was a database, you can use IBM Cognos components to run log reports from the database.

You can also set the logging level, which controls the amount of detail and type of messages that are sent to a log file or database. For instructions, see the *IBM Cognos Analytics Administration and Security Guide*.

## Specify the Log Messages Repository for IBM Db2 on z/OS

You can configure a type of repository for the log messages, and then configure properties for the specific repository. You can also configure more than one repository for log messages.

## Procedure

1. 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 26. Log server properties	
Task	Action
Use TCP between IBM Cognos components on a computer and its local log server	<p>Set the <b>Enable TCP</b> property to <b>True</b>.</p> <p>UDP provides faster communication with a lower risk of lost connections than TCP.</p> <p>TCP is used for communication between a local log server and a remote log server.</p>

Table 26. Log server properties (continued)	
Task	Action
Change the number of threads available to the local log server	Type the value in the <b>Local log server worker threads</b> 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.


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 [“Create tablespaces for a logging database on Db2 on z/OS”](#) on page 220.
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 icon .  
the edit icon
13. Click **Add**, and then add the configuration parameter names and values from the following table:

Table 27. Configuration parameter names and values	
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_LS_ID	The instance identifier for the audit database. This value must not be longer than two characters.

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.


## Specify the Log Messages Repository for Informix

You can configure a type of repository for the log messages, and then configure properties for the specific repository. You can also configure more than one repository for log messages.

### Procedure

1. In the **Explorer** window, under **Environment**, click **Logging**.
2. In the **Properties** window, use the following table to help set the log server properties.

Table 28. Log server properties	
Task	Action
Use TCP between IBM Cognos components on a computer and its local log server	Set the <b>Enable TCP</b> property to <b>True</b> .  UDP provides faster communication with a lower risk of lost connections than TCP.  TCP is used for communication between a local log server and a remote log server.
Change the number of threads available to the local log server	Type the value in the <b>Local log server worker threads</b> property.  Keep the default value of 10. The range is between 1 and 20. However, if you have a high number of log messages, you can allocate more threads to improve performance.

3. In the **Explorer** window, under **Environment**, right-click **Logging**, and click **New resource > Destination**.
4. In the **Name** box, type the name of the repository.
5. In the **Type** list, click **Database** and then click **OK**.
6. In the **Explorer** window, under **Logging**, right-click the database name, and click **New resource > Database**.
7. In the **Name** box, type the name of the repository.
8. In the **Type** list, click **Informix Dynamic Server database** and then click **OK**.
9. In the **Properties** window, type the values for **Database server and port number**, **User ID and password**, and **Database name**.
10. If you have multiple instances of an Informix logging database, create the advanced property IPFSCRIPTIDX and specify the account under which the instance runs:
  - In the **Explorer** window, click **Local Configuration**.
  - In the **Properties** window, click the **Value** column for **Advanced properties** and then click the edit icon .
  - In the **Value - Advanced properties** dialog box, click **Add**.
  - In the **Name** column, type **IPFSCRIPTIDX**
  - In the **Value** column, type the user ID of the account under which the instance of the logging database runs.  
  
Use a different user account for each instance of Informix logging database.
  - Repeat in every instance of IBM Cognos Configuration that uses an instance of an Informix logging database.
11. From the **File** menu, click **Save**.

12. Test the connection to the new database. In the **Explorer** window, under **Environment**, right-click **Logging** and click **Test**.

IBM Cognos components connect to the database. If you configured more than one database for logging messages, IBM Cognos components test all the databases.

## Changing Global Settings

---

By default, IBM Cognos components ensure that all locales, which may come from different sources and in various formats, use a normalized form. That means that all expanded locales conform to a language and regional code setting. Each computer has a default system locale and one user locale per user. The user locales may be different from the default system locale. If you change global settings on one Content Manager computer, you must make the same changes on the other Content Manager computers.

You change global settings

- [to customize language support for the user interface](#)
- [to customize currency support](#)
- [to customize content locale support](#)
- [to map the language used in the product user interface](#)
- [to map content locales](#)
- [to add fonts to your IBM Cognos environment](#)
- [to customize the default time zone](#)
- [to change the encoding for email messages](#)
- [to customize cookie settings](#)

## Customize Language Support to the User Interface

Use the Product Locales table to add or remove the user interface language support. For example, if you do not require a German user interface, you can remove the language from the list.

If you change the user interface language of the product, data is not affected.

### Before you begin

Ensure that you install the appropriate fonts to support the character sets and currency symbols you use. For Japanese and Korean currency symbols to appear correctly, you must install the additional fonts from the Supplementary Language Documentation disk.

### Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Product Locales** tab.

All supported locales are displayed.

4. Click **Add**.

**Tip:** To remove support, select the check box next to the **Supported Locale** and then click **Remove**.

5. In the second column, type the language portion of a locale.
6. Repeat steps 3 to 5 for other language support that you want to add.
7. Click **OK**.
8. From the **File** menu, click **Save**.

## Customizing Currency Support

If you require additional currencies or want to remove some from the user interface, you can update the list of supported currencies in the Currencies table. If you use Japanese or Korean currencies, you must configure support so that Japanese Yen and Korean Won characters display correctly.

By default IBM Cognos components show only a subset of supported currencies in the user interface. Currencies are identified by their ISO 4217 currency code. The complete list of supported currencies that can be added are listed in the `i18n_res.xml` file in the *install\_location/bin* directory.

Adding currencies to the IBM Cognos environment does not guarantee that your computer has a font with the required characters to display the currency. Ensure that you install the appropriate fonts to support the currency symbols you use. For example, to display the Indian currency symbol (rupee) correctly, you must install a font that contains that character. In addition, for Japanese and Korean currency symbols to appear correctly, you must install the additional fonts from the Supplementary Language Documentation disk.

### Add Currencies to the User Interface

You can add supported or unsupported currencies to the user interface. You add supported currencies in IBM Cognos Configuration. You add unsupported currencies to the `i18n_res.xml` file that is provided in IBM Cognos.

If you add a currency code that is not supported by IBM Cognos, you must manually add it to the `i18n_res.xml` file in the *install\_location/configuration* directory. Copy this file to each IBM Cognos computer in your installation.

### Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Currencies** tab.
4. Click **Add**.

**Tip:** To remove support, select the check box next to the supported item and then click **Remove**.

5. In the second column, type an appropriate value.

The value you add must comply with ISO 4217 codes for the representation of currencies and formats. Usually the value you add is a three-letter alphabetic code. The first two characters are letters representing the ISO 3166 country or region code for the country or region the currency is from. The additional letter represents the first letter of the currency.

6. Repeat steps 3 to 5 for other types of support that you want to add.
7. From the **File** menu, click **Save**.

## Customize content locale support

To ensure users see reports, data or metadata in their preferred language, or specific to their region, you can add partial locales (language) or complete locales (language-region) to the Content Locales table. This way, if content is available in different languages, or in different locales, it is rendered to users based on their user locale. By default, content locale overrides product locale in the portal for some content.

If you view reports in Thai language, digits are not supported.

### Before you begin

If a locale is not required, you can remove it from the list. You must leave at least one content locale in the list for the Application Tier Components to operate.

Adding incomplete locales (languages) to the IBM Cognos environment does not guarantee that your computer has a font that can display Web pages in your preferred languages. Ensure that you install the

appropriate fonts to support the character sets and currency symbols you use. For Japanese and Korean currency symbols to appear correctly, you must install the additional fonts from the Supplementary Language Documentation disk.

## Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Content Locales** tab.

All supported locales are displayed.

4. Click **Add**.

**Tip:** To remove support, select the check box next to the supported item and then click **Remove**.

5. In the second column, type an appropriate value.
  - To add language support for report data and metadata, type a partial local (language) setting.
  - To add support specific to a region, type a complete locale (language-region) setting.
6. Repeat steps 3 to 5 for each additional locale that you want to support.
7. From the **File** menu, click **Save**.

## Content Locales

Use the Content Locale Mappings table to map user locales to a complete (language-region) or partial (language) locale. You can also map a user's preferred language to another language if content is not available in the user's preferred language.

For example, if a report or scorecard is not available in a preferred language, for example Vietnamese, but is available in French and German, you can use the Content Mappings table to map the preferred language (Vietnamese) to another language (French or German). This way, you see the report or scorecard in the mapped language.

By default, the Content Locale Mappings table includes locales that do not contain the region. This allows you to use only the language portion of the locale when you specify locale settings and ensures that you always see the correct information. For example, in a multilingual database, data is usually available in different languages, such as French (fr), Spanish (es) and English (en), rather than being available in different locales, such as English Canada (en-ca), English United States (en-us), or French France (fr-fr).

The following examples show the method that IBM Cognos components use to determine which report or scorecard the user sees if the multiple language versions are available.

### Example 1

A report is available in Content Manager in two locales, such as en-us (English-United States) and fr-fr (French-France), but the user locale is set to fr-ca (French-Canadian). IBM Cognos uses the locale mapping to determine which report the user sees.

First, IBM Cognos checks to see if the report is available in Content Manager in the user's locale. If it is not available in the user's locale, IBM Cognos maps the user's locale to a normalized locale configured on the Content Locale Mapping tab. Because the user's locale is fr-ca, it is mapped to fr. IBM Cognos uses the mapped value to see if the report is available in fr. In this case, the report is available in en-us and fr-fr, not fr.

Next, IBM Cognos maps each of the available reports to a normalized locale. Therefore, en-us becomes en and fr-fr becomes fr.

Because both report and the user locale maps to fr, the user having the user locale fr-ca will see the report saved with the locale fr-fr.

## Example 2

The user's locale and the report locales all map to the same language. IBM Cognos chooses which locale to use. For example, if a user's locale is en-ca (English-Canada) and the reports are available in en-us (English-United States) and en-gb (English-United Kingdom), IBM Cognos maps each locale to en. The user will see the report in the locale setting that IBM Cognos chooses.

## Example 3

The report and the user locales do not map to a common language. IBM Cognos chooses the language. In this case, you may want to configure a mapping. For example, if a report is available in en-us (English-United States) and fr-fr (French-France), but the user locale is es-es (Spanish-Spain), IBM Cognos chooses the language.

## Map Content Locales

Use the Content Locale Mappings table to map user locales to a complete (language-region) or partial (language) locale. You can also map a user's preferred language to another language if content is not available in the user's preferred language.

### Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Content Locale Mapping** tab.
4. Click **Add**.
5. In the **Key** box, type the user locale:
  - To ensure all regions for a user locale see content in a specific language, type the language portion of the locale, followed by a dash (-) and an asterisk (\*).  
For example, type **fr-\***
  - To ensure a user locale (language-region) sees content in a specific language, type the complete locale.  
For example, type **fr-ch**
  - To map a preferred language to another language, type the preferred language portion of the locale.  
For example, type **zh**
6. In the **Locale Mapping** box, type the language portion of the locale.  
User locales specified in the **Key** box will see content in this language.
7. Repeat steps 3 to 5 for other mappings you want to do.
8. Click **OK**.
9. From the **File** menu, click **Save**.

## Map Product Locales

Use the Product Locale Mappings table to specify the language used in the user interface when the language specified in the user's locale is not available.

You can ensure that all regions for a locale use the same language, or that a specific, complete locale (language-region) uses a particular language.

By default, the user sees the product interface in the language that matches the language setting of the user locale.

## Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Product Locale Mappings** tab.
4. Click **Add**.
5. In the **Key** box, type the user locale:
  - To ensure all regions for a locale see the user interface in a specific language, type the language portion of the locale, followed by a dash (-) and an asterisk (\*).  
For example, type **es-\***
  - To ensure a complete locale (language-region) see the user interface in a specific language, type the complete locale.  
For example, type **es-es**
  - To map a preferred language to another language, type the preferred language portion of the locale.  
For example, type **zh**

**Tip:** To specify which locale to use as the default, use the wildcard character (\*) for the **Key** value and then, in the **Locale Mapping** box type the locale.
6. In the **Locale Mapping** box, type the language portion of the locale.  
User locales specified in the **Key** box will see content in this language.
7. Repeat steps 3 to 5 for other mappings you want to do.
8. Click **OK**.
9. From the **File** menu, click **Save**.

## Customize the Server Time Zone

You can customize the time zone used by Content Manager by selecting a different server time zone in IBM Cognos Configuration.

For UNIX installations that do not support a Java-based graphical user interface, you can view the list of acceptable time zones by opening IBM Cognos Configuration on the Windows computer where Framework Manager is installed.

Content Manager is configured to use the time zone of your operating system by default. All scheduled activities in IBM Cognos are set using this time zone. In addition, users in the portal use this time zone if they set their preferences for the default time zone. For more information about setting user preferences in the portal, see the *IBM Cognos Analytics Administration and Security Guide*.

## Procedure

1. Start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. In the **Global Configuration** window, click the **General** tab.
4. Click the **Value** column for **Server time zone** and select another time zone from the list.
5. From the **File** menu, click **Save**.

## Encoding for Email Messages

By default, IBM Cognos components use UTF-8 encoding in emails. This value sets the default encoding used by the delivery service in this instance for all email messages. You may have older email clients or send email from IBM Cognos to cell phones and PDAs that do not recognize UTF-8. If so, you can change the email encoding to a value that works on all your email clients (for example, ISO-8859-1, Shift-JIS). Each instance of IBM Cognos that has an available delivery service must be changed.



The specified encoding affects the entire message, including the subject, attachments, attachment names, and plain or HTML body text.

The encoding values are shown in the following table:

<i>Table 29. Supported encoding values</i>	
<b>Character set</b>	<b>Supported encoding value</b>
UTF-8	utf-8
Western European (ISO 8859-1)	iso-8859-1
Western European (ISO 8859-15)	iso-8859-15
Western European (Windows-1252)	windows-1252
Central and Eastern European(ISO 8859-2)	iso-8859-2
Central and Eastern European (Windows-1250)	windows-1250
Cyrillic (ISO 8859-5)	iso-8859-5
Cyrillic (Windows-1251)	windows-1251
Turkish (ISO 8859-9)	iso-8859-9
Turkish (Windows-1254)	windows-1254
Greek (ISO 8859-7)	iso-8859-7
Greek (Windows-1253)	windows-1253
Japanese (EUC-JP)	euc-jp
Japanese (ISO-2022-JP)	iso-2202-jp
Japanese (Shift-JIS)	shift_jis
Traditional Chinese (Big5)	big5
Simplified Chinese (GB-2312)	gb2312
Korean (EUC-KR)	euc-kr
Korean (ISO 2022-KR)	ISO 2022-KR
Korean (KSC-5601)	ksc_5601
Thai (Windows-874)	windows-874
Thai (TIS-620)	tis-620

## Change Encoding for Email Messages

You can change the email encoding to a value that works on all your email clients.

## Procedure

1. Start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. In the **Global Configuration** window, click the **General** tab.
4. Click the **Value** column for the **Email Encoding** property.
5. Scroll to the desired setting and click it.
6. From the **File** menu, click **Save**.

## Customizing 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 suggested in the following:

- For the Domain value, use the computer or server name alone. Specify this name without any dots. For example, mycompany
- The Domain value can also specify a suffix. Suffixes include .com, .edu, .gov, .int, .mil, .net, or .org. Include a prefix dot. For example, .mycompany .com
- Other levels can be used in a Domain value. Include a prefix dot. For example .accounts.mycompany .com
- A Path value can further restrict cookies. The most general path is /. A path of /payables restricts the cookie to all paths beginning with "payable" (and all subdirectories). A path of /payables/ restricts the cookie to the "payables" directory (and all subdirectories).

Additionally, for security, administrators can set the HTTPOnly attribute to block scripts from reading or manipulating the CAM passport cookie during a user's session with their web browser. For more information about this attribute, see the *IBM Cognos Analytics Administration and Security Guide*.

## Procedure

1. On each Content Manager computer, start IBM Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **General** tab.
4. Click in the **Value** column under **Cookie Settings** for each property that you want to change and specify the new value.

If you leave the **Domain** property blank, the dispatcher derives the domain from the host name of the request.

5. Click **OK**.

## Change the IP Address Version

IBM Cognos products support 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.

## Setting the IP version

Use IBM Cognos Configuration to select the IP version.

### Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. Click the **Value** box for **IP Version for Host Name Resolution** and click **Use IPv4 addresses** or **Use IPv6 addresses**.
4. From the **File** menu, click **Save**.
5. Close IBM Cognos Configuration.

## Manually configuring IBM Cognos Configuration to start with the IPv6 option

You can manually configure IBM Cognos Configuration to use the IPv6 option by specifying the option in the start command.

### Procedure

1. Go to the *install\_location/bin* or the *install\_location/bin64* directory.
2. Start IBM Cognos Configuration by including the IPv6 option in the command, as follows:
  - On Windows, type  
`cogconfig.bat -ipv6`
  - On UNIX or Linux, type  
`./cogconfig.sh -ipv6`
3. Edit the URI properties that use IPv6 format, specify the values, and then from the **File** menu, click **Save**.

## Configuring IBM Cognos Configuration to always start with the IPv6 option on Windows

You can configure IBM Cognos Configuration to always use the IPv6 option on Microsoft Windows operating systems by setting the option in the Start menu shortcut.

### Procedure

1. From the **Start** menu, right-click **IBM Cognos Configuration**, and select **Properties**.
2. On the **Shortcut** tab, in the **Target** box, type  
"install\_location\bin\cogconfigw.exe -ipv6"
3. Click **OK**.

## Configuring the Collaboration Discovery URI

---

You can configure IBM Cognos Analytics to use IBM Connections for collaborative decision-making. Integration with IBM Connections allows business users to collaborate while creating or viewing reports, performing analysis, or monitoring workspaces. Users have access to the IBM Connections homepage from within IBM Cognos Analytics.

The Collaboration discovery URI specifies the IBM Connections server to use as the collaboration provider. When a URI is specified, collaboration-related support is added to IBM Cognos Analytics as follows:

- a link is added to the IBM Cognos Analytics portal welcome page. If the user has access to the IBM Connections homepage, the link is named **Access my social network** and links the user to the homepage. If the user has access to IBM Connection activities, but not the homepage, the link is named **My Activities** and links the user to the activities page.
- a link to the IBM Connections homepage is added to the Launch menu in the portal.

### Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Dispatchers and Services** to view the list of dispatchers.
2. From the toolbar, click the set properties - configuration button.
3. Click the **Settings** tab.
4. For the **Environment** category, **Collaboration discovery URI**, specify the URI as follows:  
`http://server_name:port_number/activities/serviceconfigs`  
For example, `http://server_name:9080/activities/serviceconfigs`  
where *server\_name* represents the server name where IBM Connections is installed.
5. 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.

### Procedure

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

## Configuring IBM Cognos Analytics to Work with Other IBM Cognos Products

---

Some IBM Cognos products provide functionality that is not available in IBM Cognos Analytics.

You can continue to use these products in the same environment. Additional configuration tasks may be required to ensure that IBM Cognos Analytics can access objects that were created using other IBM Cognos products. Additional requirements for access depend on how you choose to run the two products.

### Enable Scheduled Reports and Agents for IBM Cognos Planning Contributor Data Sources

To run scheduled reports and agents, which are based on IBM Cognos Planning Contributor data sources, you must specify a shared, secret password. This helps to ensure secure communication between IBM Cognos Analytics servers and Contributor Data Server.

#### Procedure

1. On the Application Tier Components computer, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Data Access, IBM Cognos Planning, Contributor Data Server**.
3. In the **Properties** window, click the **Value** box next to the **Signature password** property and then click

the edit button  when it appears.

4. In the **Value - Signature Password** dialog box, type the password that will be digitally signed.

The password is case-sensitive and must match the **Signature password** property that you configure in IBM Cognos Series 7, Configuration Manager, **Cognos Planning/Cognos BI - Contributor Data Server/General** properties.

5. From the **File** menu, click **Save**.

#### Results

A digital signature, based on the password, is created. The digital signature is encoded by IBM Cognos Analytics and decoded by Contributor Data Server.

## Configuring the Software Development Kit

---

To use the IBM Cognos Software Development Kit, you must perform some configuration and set-up tasks.

To configure the Software Development Kit, follow this process:

- If you want to run the Framework Manager script player from outside the bin directory, configure the FM\_INI\_FILE\_PATH environment variable as a system variable on a Microsoft Windows operating system. The environment variable must point to the *Framework\_Manager\_location\configuration\fm.ini* directory.
- To allow the browsing or import of system objects such as tables, views, synonyms, stored procedures, or functions from a relational database in Framework Manager, edit the entry for ImportDatabaseSystemObjects in your fm.ini file.

By default, ImportDatabaseSystemObjects is set to FALSE. Users can see only the user tables in the import and expression editor dialog boxes. To allow browsing or import of system objects, set the preference to TRUE.

- Set up the samples for IBM Cognos Analytics and Framework Manager.

For more information, see the Installation and Configuration Guide for your IBM Cognos product.

- Set up the IBM Cognos software to use the Software Development Kit code samples.

For more information, see the *IBM Cognos Software Development Kit Developer Guide*.

- Set up the IBM Cognos software to use the Mashup Service samples.

For more information, see the *IBM Cognos Mashup Service Developer Guide*.

---

## Chapter 13. Configuring authentication providers

IBM Cognos components run with two levels of access: 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 must disable anonymous access. For more information, see [Disable anonymous access](#).

For authenticated logon, you must configure IBM Cognos Analytics 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.

### Classic and dynamic namespaces

You can configure two types of namespace in Cognos Analytics: *classic* namespaces and *dynamic* namespaces. Dynamic and classic namespaces function the same way. However, it is easier for the administrator to create dynamic namespaces than classic namespaces for these reasons:

- The administrator may not have direct access to the Cognos Analytics server and therefore cannot run Cognos Configuration.
- After creating a dynamic namespace, the administrator doesn't have to restart the Cognos Analytics service, which would interrupt current user sessions.

#### Tips:

- To configure classic namespaces using Cognos Configuration, click the links at the bottom of this topic.
- To configure dynamic namespaces using the Manage component, see "Creating a dynamic namespace" in the *IBM Cognos Analytics Managing Guide*.

If you upgraded from ReportNet and IBM Cognos detects a previously configured namespace that is no longer configured, the unconfigured namespace appears in the list of authentication providers in the Administration portal. You can configure the namespace if you still require the user account information. Otherwise, you can delete the namespace. Also, when upgrading from one version to another, you must use the same authentication namespace for both versions. Otherwise, the old secured content will not be available because the new version might not contain the same policies, users, roles, and groups.

IBM Cognos components support the following types of servers as authentication sources:

- Active Directory Server
- Custom Authentication Provider
- IBM Cognos Series 7 namespace
- LDAP
- OpenID connect
- SiteMinder
- SAP

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 an operating system it supports:

- IBM Cognos Series 7 namespace (Windows, Solaris, AIX)
- Active Directory Server (Windows only)
- SAP BW (All except Power PC, z/OS, z/Linux)

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. 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. However, "unknown" entries can also show up if you are not authenticated into all namespaces. In this scenario, do not delete "unknown" entries.

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 Analytics portal. You can hide Custom Java namespaces and SiteMinder namespaces from users. For more information, see [“Hide the Namespace from Users During Login”](#) on page 262.

## Disabling anonymous access

---

If you want to configure IBM Cognos Analytics for authenticated logon only, you need to disable anonymous access to the application.

By default, IBM Cognos components do not require user authentication. Users can log on anonymously.

### Procedure

1. On each computer where Content Manager is installed, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Security > Authentication**, click **Cognos**.  
The Cognos namespace stores information about IBM Cognos groups and roles, contacts, and distribution lists, and so on, and references to objects in other security namespaces.
3. In the **Properties** window, click the box next to the **Allow anonymous access** property and then select **False**.
4. From the **File** menu, click **Save**.

### Results

Now, you must configure a namespace so that users are required to provide logon credentials when they access IBM Cognos Analytics.

## Restricting user access to the Cognos namespace

---

You can configure access to IBM Cognos Analytics so that only users who are members of any group or role in the **Cognos** namespace can access the application.

Ensure that you are a member of the built-in **System administrator** role in the **Cognos** namespace before you enable this configuration.

### Procedure

1. On each Content Manager computer, 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**.

## What to do next

You must now remove the **Everyone** group from certain Cognos built-in groups and roles, and ensure that authorized users belong to at least one Cognos group or role. These tasks are performed by administrators in the Cognos Analytics administration interfaces. For more information, see the *IBM Cognos Analytics Managing Guide* or the *IBM Cognos Analytics Administration and Security Guide*.

## Configuring Lightweight Third-Party Authentication

---

You can configure IBM Cognos Analytics components to use IBM Lightweight Third-Party Authentication (LTPA). The practices that are described in this topic are based on Cognos Analytics 11.0.7 distributed environment with IBM Tivoli Directory Server LDAP or Microsoft Active Directory as authentication sources.

With LTPA, the user authenticates with the first server that is accessed, by using a user name and password. After authenticating, the user receives an LTPA token, which is valid for only one session. The token is used to identify the user on other servers within the same domain name system, where the servers are configured to use LTPA. Therefore, the user enters a user name and password only once, and the user directory is accessed only once to verify the identity of that user.

To implement LTPA, Cognos Analytics must be configured to use an authentication source that is configured in the WebSphere Liberty container that it runs in. You can configure single sign-on between Cognos Analytics and WebSphere Liberty using the identity mapping configuration in the Cognos namespace. For example, you can configure WebSphere Liberty to use an LDAP or Active Directory server for authentication, then configure Cognos Analytics to use the same LDAP or Active Directory, and set the identity mapping to use REMOTE\_USER.

For Cognos Analytics, this means that a user must be authenticated to an identity assigned to the HTTP session before accessing Cognos Analytics within the same session. Authentication is completed by presenting credentials to an external-to-Cognos security system. The security system might provide the identity and some sort of credential information suitable for achieving single sign-on to other systems, usually in the form of an SSO token. Typical candidates for such security systems are authentication proxies, such as IBM Tivoli WebSEAL, Oracle Oblix, Site Minder, or any other software or hardware solutions that can authenticate an HTTP session and persist that authentication in a token.

## Procedure

1. On a computer where the Cognos Analytics server is installed, start IBM Cognos Configuration.
2. In the **Explorer** window, expand the **Environment** category, and then the **IBM Cognos services** category.
3. Click the **IBM Cognos** service.
4. In the properties pane, click the **Enable IBM Lightweight Third Party Authentication (LTPA)** property, and change its value to **True**.
5. Save the configuration, and restart the **IBM Cognos** service.
6. Repeat these steps on all computers where the Cognos Analytics server is installed.

## What to do next

To use LTPA, open the `install_location/configuration/bi-services/bi-service.xml` file, and change the `special subject type` from `EVERYONE` to `ALL_AUTHENTICATED_USERS` in the following way:

```
<special-subject type="ALL_AUTHENTICATED_USERS"/>
```

Make this change on all computers where Cognos Analytics servers are installed.

## Configuring LTPA using an LDAP namespace

The following procedure describes how to set up LTPA for Cognos Analytics when using IBM Tivoli Directory Server LDAP as the authentication source.

For details about configuring LDAP, see [“Configuring IBM Cognos components to use LDAP” on page 263](#)

### Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource > Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, select **LDAP – General default values**.
5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
6. Specify the following properties:

#### **Host and port**

The fully qualified host and port of the LDAP server.

#### **Base distinguished name**

For example, `o=organization_name.com`

#### **User lookup**

For example, `uid=${userID},ou=people`

#### **Use External Identity**

True

#### **External identity mapping**

For example, `uid=${environment("REMOTE_USER")},ou=people`

7. If you want the LDAP authentication provider to bind to the directory server by using a specific **Bind user DN and password** when you perform 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 run under the authentication context of the user.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server using the following steps:

- Ensure that **Use external identity** is set to **False**.
- Set **Use bind credentials for search** to **True**.
- Specify the user ID and password for **Bind user DN and password**.

If you do not specify a user ID and password, and anonymous access is enabled, the search is done by using anonymous.

9. Check the mapping settings for the 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. Create an XML file named `local-server.xml` and place it in the `install_location/` configuration directory.

12. In the `local-server.xml` file, enter values that are appropriate for your environment:

```
<?xml version="1.0" encoding="UTF-8"?>
<server>
  <featureManager>
    <feature>ldapRegistry-3.0</feature>
    <feature>appSecurity-2.0</feature>
  </featureManager>
  <ldapRegistry id="id" realm="realm"
    host="host" port="port" ignoreCase="true"
    baseDN="o=basedn" ldapType="Custom" sslEnabled="false">
    <idsFilters
      userFilter="(uid=%v,ou=people)"
      userIdMap="*:uid"
      groupFilter='(objectclass=groupofnames)'
      groupIdMap="*:cn" />
  </ldapRegistry>
  <webAppSecurity allowFailOverToBasicAuth="true" displayAuthenticationRealm="true"/>
</server>
```

13. If Cognos Analytics is configured to use SSL, see [“Configuring the SSL protocol for IBM Cognos components”](#) on page 206 for more information.

14. To verify the configuration, log on to `http://host:port/bi` or `https://host:port/bi` for SSL enabled systems, where `host` is the fully qualified Cognos Analytics host domain.

You should not see the Cognos Analytics logon page. Instead, you should be prompted by the browser to log on.

## What to do next

If you want to configure single sign-on (SSO) between the Cognos Analytics application that was set up with LTPA authentication, and the application is deployed into a WebSphere instance, install the WebSphere key on each Cognos Analytics dispatcher where LTPA was set up, and update the `local-server.xml` file with the following `<ltpa>` element:

```
<ltpa keysFileName="yourLTPAKeysFileName.keys"
  keysPassword="keysPassword" expiration="120" />
```

For more information, see the [WebSphere Liberty documentation](#).

## Configuring LTPA using an Active Directory namespace

The following procedure describes how to set up LTPA for Cognos Analytics with Microsoft Active Directory as the authentication source.

### Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource > Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, select **LDAP - Default values for Active Directory** and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component. Default values are generated for you. Check them and make changes as needed.

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.

- For **User lookup**, enter `(sAMAccountName=${userID})`
- If you use single sign-on, for **Use external identity**, set the value to **True**.

- If you use single sign-on, for **External identity mapping**, enter (sAMAccountName=\${environment("REMOTE\_USER")})

If you want to remove the domain name from the REMOTE\_USER variable, enter (sAMAccountName=\${replace(\${environment("REMOTE\_USER")}, "domain\\", "")}).

**Important:** Ensure that you use only the variable REMOTE\_USER. Using another variable can cause a security vulnerability.

- For **Bind user DN and password**, enter **user@domain**.
  - For **Unique identifier**, enter objectGUID
7. Create an XML file named `local-server.xml` and place it in the *install\_location*/configuration directory.
  8. In the `local-server.xml` file, enter values that are appropriate for your environment:

```
<?xml version="1.0" encoding="UTF-8"?>
<server>
  <featureManager>
    <feature>ldapRegistry-3.0</feature>
    <feature>appSecurity-2.0</feature>
  </featureManager>
  <ldapRegistry id="id" realm="realm"
    host="host" port="port" ignoreCase="true"
    baseDN="DC=dc,DC=dc,DC=dc" bindDN="CN=doejohn,
      OU=Users,DC=dc,DC=dc,DC=dc"
    bindPassword="password" ldapType="Microsoft Active Directory" sslEnabled="false">
    <activeFilters
      userFilter="(&(sAMAccountName=%v)(objectcategory=user))"
      groupFilter="(&(cn=%v)(objectcategory=group))"
      userIdMap="user:sAMAccountName"
      groupIdMap="*:cn"
      groupMemberIdMap="memberOf:member">
    </activeFilters>
  </ldapRegistry>
  <webAppSecurity allowFailOverToBasicAuth="true" displayAuthenticationRealm="true"/>
</server>
```

9. If Cognos Analytics is configured to use SSL, see [“Configuring the SSL protocol for IBM Cognos components”](#) on page 206 for more information.
10. To verify the configuration, log on to `http://host:port/bi` or `https://host:port/bi` for SSL enabled systems, where `host` is the fully qualified Cognos Analytics host domain.

You should not see the Cognos Analytics logon page. Instead, you should be prompted by the browser to log on.

## What to do next

If you want to configure single sign-on (SSO) between the Cognos Analytics application that was set up with LTPA authentication, and the application is deployed into a WebSphere instance, install the WebSphere key on each Cognos Analytics dispatcher where LTPA was set up, and update the `local-server.xml` file with the following `<ltpa>` element:

```
<ltpa keysFileName="yourLTPAKeysFileName.keys"
  keysPassword="keysPassword" expiration="120" />
```

For more information, see the [WebSphere Liberty documentation](#). The root directory of the automatically generated LTPA keys file `${server.output.dir}/resources/security/ltpa.keys` that is mentioned in this document is `cognos_analytics_location/wlp/usr/servers/cognosserver`.

## OpenID Connect authentication provider

OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol. It is used for federated identity and authentication with multiple applications that use the same identity provider. OpenID

Connect is the preferred web-based authentication provider if you want to federate IBM Cognos Analytics with other applications.

OpenID Connect is a modern standard that incorporates the OpenID and OAuth 2.0 standards. It is supported for both on-premises and Cloud installations of Cognos Analytics.

Cognos Analytics supports the following types of OpenID Connect identity providers:

- ADFS (Active Directory Federation Services)
- Azure AD (Active Directory)
- Generic
- Google
- IBM Cloud Identity
- IBMid (IBM identity provider)
- MS Identity
- OKTA
- Ping
- Salesforce
- SiteMinder

**Tip:** Contact the identity provider administrator in your organization, or the sales and support organization, to find out which product version you should use.

## OpenID Connect Authentication Proxy

Cognos Analytics now provides another provider type, 'OpenID Connect Authentication Proxy' in Cognos Configuration. This menu offers the option to have Trusted Signon Provider (TSP) for OpenID connect. Similar to OpenID Connect entries, you will see the list of Identity Providers currently supported.

Additional configuration setting entries under Advanced Properties are now visible. You will need to configure the claim you want passed to the real provider as well as the namespace ID of the real provider.

- Identity claim name: Specifies the name of the claim that will be provided to the target namespace (for example. John Doe)
- Trusted environment name: Specifies the environment variable name that will be used to transfer the claim to the target namespace (for example. REMOTE\_USER)
- Redirect namespace ID: Specifies the namespace ID that will be invoked with the claim obtained from the OpenID identity provider (for example. LDAP)

## Leveraging the identity provider single sign-on

If your OpenID Connect identity provider supports single sign-on and two-factor authentication, Cognos Analytics can leverage this functionality.

If the identity provider does not support single sign-on, when a user makes an authentication request to Cognos Analytics, the user is redirected to the OpenID Connect identity provider logon page. After providing the required information, the user is redirected back to Cognos Analytics with an authorization code that is redeemed for an ID token that contains the identity of the user. The user can then access Cognos Analytics.

If the identity provider supports single sign-on, the user receives the ID token when making the authentication request to Cognos Analytics, and can immediately access the application.

## Federating IBMid with SAML 2.0 identity providers

IBMid is the IBM OpenID Connect identity provider. If your identity provider (IdP) does not support OpenID Connect, but supports SAML 2.0, you can use IBMid to configure an OpenID Connect namespace

as your authentication provider in Cognos Analytics. Simply, choose IBMId as your identity provider when configuring the OpenID Connect namespace.

With this namespace configuration, you can federate Cognos Analytics with most SAML 2.0 identity providers. As a result, when users log on to Cognos Analytics, they are redirected to the IBMId sign-on page where they type their email address. If the email address is recognized by IBMId, the users are redirected to their organization SAML 2.0 identity provider logon page. In this page, the users complete the authentication process by providing their credentials. Then, they can access Cognos Analytics.

## Configuring an OpenID Connect namespace

To use an OpenID Connect identity provider with IBM Cognos Analytics, you must configure an OpenID Connect namespace.

If you use IBMId as your OpenID Connect identity provider, see [Managing OpenID connect namespaces](#) for more information.

If users have authentication problems after you successfully configured your OpenID Connect namespace, use diagnostic logging in the **Manage** component of Cognos Analytics to troubleshoot issues. You need to create a new logging topic that is based on the predefined **AAA** topic. Modify the **AAA** logging topic by adding the following code to it:

```
{
  "loggerDefinitions": [
    {
      "loggerName": "com.ibm.cognos.camaaa.internal.OIDC",
      "level": "DEBUG",
      "additivity": true
    }
  ],
  "topicName": "OIDC"
}
```

For more information on diagnostic logging, see [Logging types and files](#).

### Procedure

1. Open IBM Cognos Configuration on your Content Manager computer.
2. Under **Security > Authentication**, right-click and select **New resource > Namespace**.
3. For **Type (Group)**, select **OpenID connect**.
4. For **Type**, select one of the identity providers from the drop-down list that includes the supported identity providers.
5. Type the namespace name in the **Name** field, and then click **OK**.

The new namespace is added in the **Explorer** pane under **Security > Authentication**, and its properties are displayed in the properties pane.

6. Specify values for the namespace properties.

**Tip:** Information about each property is displayed in the user interface when you click the property.

- The **Namespace ID** is used in the CAMID.
- Specify values for **Discovery Endpoint**, **Client Identifier**, and **OpenID Connect client secret**, as suggested by your OpenID Connect administrator.
- Update the **Return URL** with your gateway or dispatcher URL, as shown in the following example:

`http://mycompany:9300/bi/completeAuth.jsp`

If you use a load balancer in your environment, include the load balancer DNS entry in the **Return URL** in front of the gateway or dispatcher nodes, as shown in the following example:

`https://MyLoadbalancerDNS.mycompany.com:443/ibmcognos/bi/completeAuth.jsp`

In this example, the Cognos Analytics gateway is installed on the web server.

If you are using a set of dispatcher nodes behind the load balancer where the Cognos Analytics gateway is not installed on the web server, the **Return URL** might look as follows:

`https://MyLoadbalancerDNS.mycompany.com:9300/bi/completeAuth.jsp`

**Tip:** The **Multitenancy** properties do not need to be specified now.

7. Import the OpenID Connect root certificate authority certificate into the Cognos Analytics keystore by using the Third-Party Certificate Tool.

- On UNIX or Linux operating systems, type `ThirdPartyCertificateTool.sh -i -T -r cert.cer -p NoPasswordSet`
- On Windows operating systems, type `ThirdPartyCertificateTool.bat -i -T -r cert.cer -p NoPasswordSet`

**Tip:** Replace the `cert` variable with the name of the certificate file that is used by your OpenID Connect identity provider. For IBMid, the file name is `blueid.cer`.

The command imports the contents into the `CAMKeystore` file in the `certs` directory by using the specified password.

8. Perform the same configuration steps on your backup Content Manager computer.
9. Restart the IBM Cognos service on the Content Manager and the backup Content Manager computers.

## Results

All users who are registered with your OpenID Connect identity provider should now have access to Cognos Analytics.

## Generic OIDC provider type

If your OIDC identity provider type is not listed or you want more configuration flexibility, set the type to **Generic** when you configure your OpenID Connect namespace as your authentication provider. Additional information about the namespace is required.

You must perform two tasks:

- [Find out information about the OIDC namespace](#)
- [Configure OIDC values in Cognos Configuration](#).

### Finding out information about the OIDC namespace

Before you configure Cognos Configuration, gather information from your identity provider (IDP) administrator. For interactive user authentication, Cognos Analytics supports the authorization code flow, as defined in [OpenID Connect Core 1.0 specification](https://openid.net/specs/openid-connect-core-1_0.html) ([https://openid.net/specs/openid-connect-core-1\\_0.html](https://openid.net/specs/openid-connect-core-1_0.html)).

To obtain the necessary information, ask your IDP administrator these questions:

#### Does the IDP support OpenID Connect Discovery?

For more information, see [https://openid.net/specs/openid-connect-discovery-1\\_0.html](https://openid.net/specs/openid-connect-discovery-1_0.html)

If the answer is yes, obtain the discovery URL.

If the answer is no, obtain values for these settings:

- **Issuer**
- **Token Endpoint**
- **Authorization Endpoint**
- **JWKS Endpoint** (optional)

#### Does the IDP support JSON Web Key Sets (JWKS)?

The URL may be returned in the Discovery document. If it is not returned or your IDP does not support discovery, then ask your administrator to provide the JWKS URL.

If JWKS is not supported, ask your administrator to provide the public key used to sign the id\_token. The key must be provided in the form of a file that contains a single PEM-encoded X509 certificate.

### **How will the Cognos Analytics application authenticate to the IDP?**

The options are to use a client secret or a JWT signed with a private key. If you are using a private key, it must be provided as encrypted PKCS#8 in a PEM format.

In both cases, obtain the **Client ID**.

### **Which user property claims can be mapped to Cognos Analytics?**

Cognos Analytics maps user properties to claims in the OIDC id\_token and optionally also the user\_info endpoint. Your administrator can help determine which claims are available and if extra scope values are required for the required claims.

For more information, see [Table 1: Mapping of OIDC claim names to Cognos Configuration properties](#).

In addition, you can configure custom properties. If a property is not mapped to a claim or if the claim is sometimes empty the value is displayed as empty.

First, identify which claim uniquely identifies a user. Next, map this claim to one of the user properties or a custom property. The value of this property must never change and must be unique across all users in the namespace.

The sub claim is convenient, and guaranteed unique by the OIDC specification. However, it may make it more difficult to pre-register users in Cognos Analytics before they logon. It may also make migration to a different IDP more complicated if the value is proprietary. The preferred\_username attribute usually works well if supported by the IDP and does not change over time.

The rest of the user properties are optional. However, configuring at least the username is recommended so that it can be displayed in the audit logs.

### **Does the IDP support password grant/ROPC (Resource Owner Password Credentials)?**

If the answer is yes, are any additional URL parameters required?

### **What offline authentication methods are supported by the IDP?**

Cognos Analytics supports password grant, refresh\_token, and a proprietary fallback of "id token". Some IDPs require additional scope values for refresh tokens.

### **What is the Return URL?**

For security reasons, the OIDC protocol requires the application to pre-register its own URL with the IDP. The specification also requires that https protocol be used. At this time the URL must contain a port, and is usually 443 for https.

You must give your administrator the exact URL with the port.

## **Configuring OIDC values in Cognos Configuration**

1. Open IBM Cognos Configuration on your Content Manager computer.
2. Under **Security > Authentication**, right-click and select **New resource > Namespace**.
3. For **Type (Group)**, select **OpenID connect**.
4. For **Type**, select **Generic**.
5. Type the namespace name in the **Name** field, and then click **OK**.

The new namespace is added in the **Explorer** pane under **Security > Authentication**, and its properties are displayed in the properties pane.

6. Specify values for the namespace properties.

- The **Namespace ID** is used in the CAMID.

#### **If you are using a discovery URL:**

- Keep **Use Discovery endpoint?** set to **True** and configure **Discovery Endpoint**.
- Keep the following **Non-discovery endpoint configuration** properties empty:



- **Issuer**
- **Token Endpoint**
- **Authorization Endpoint**

**If you are not using a discovery URL:**

- Change the **Use discovery endpoint?** value to **False**.
- Leave **Discovery Endpoint** empty.
- Configure the **Non-discovery endpoint configuration** properties **Issuer**, **Token endpoint**, and **Authorization Endpoint** properties with the values that you obtained from the OIDC administrator.
- In the **Application configuration** section, specify values for **Client Identifier**, and **Return URL**, as suggested by your OIDC administrator.
- In the **Identity provider authentication** section:
  - For the **Scope for authorize endpoint** property, keep the value **openid**. Add any required additional scopes. Values are separated by spaces.
  - For the **Account claims** property, the default value is **ID token**.

**Tip:** Some IDPs require an extra call to the **Userinfo endpoint** property to resolve all needed claims. This causes an extra HTTP GET request to be sent to the IDP logon time. If your IDP requires this, you can change this setting.
- In the **Token endpoint authentication** section:
  - If you are using a client secret, enter its value. For the **Strategy** property, select **Client secret post** or **Client secret basic**, depending on what your IDP requires. Leave the private key parameters empty.
  - If you are using Private Key JWT authentication, select Private key JWT for the **Strategy** property and leave **Client secret** empty. Configure the path to the private key file and password. The file must contain a single, encrypted PKCS#8 key in a PEM format. If your IDP requires a kid parameter in the JWT header, enter it as the **Private key identifier**, otherwise leave it blank.
- For the **Token signature verification** section:
 

Usually, the JWKS URL is taken from the Discovery endpoint document and these sections defaults are appropriate.

However, you can manually configure the URL or certificate file, if needed. The **Location** drop down allows you to select which one to use. If you are using a file, it must contain a single PEM encoded X509 certificate.
- For the **Password grant** section:
  - If you are using password grant for offline authentication, the strategy lets you configure where the claims are gathered from.
  - **ID Token:** Only the ID token is considered.
  - **ID Token and User info endpoint:** both the ID token and the user info endpoint are used.
  - **User info endpoint.** For security reasons, the setting is now identical to **ID Token** and **User info endpoint** and is included for backward compatibility with previous versions.
  - **Unsupported** - Select this value if your IDP does not support password grant or if you do not wish Cognos Analytics to use it.
  - If your IDP requires that the scope not be sent, then you can configure this here. Same with additional URL parameters that may be required. Note that the parameters must start with **&** and the rest be URL-encoded. For example: **'&resource=https%3A%2F%2Fca.ibm.com'**.
- For the **Scheduling credentials** section:

This section is used to configure offline authentication or when interactive authentication is not possible. An example is a schedule that runs a report.

For offline authentication to be possible, an encrypted blob is stored in Content Manager while the user is logged on interactively, for example, when the schedule is created. Then later a trusted service can use this blob to create a session to perform work on behalf of a user.

The configured strategy controls what this encrypted blob contains:

- **ID Token:** store only the id\_token. Later the idtoken is used directly to establish the users identity. This is the most compatible setting but it prevents certain forms of Data Source authentication. Also the IDP is not contacted so the credentials will be valid until the user is disabled in Cognos Analytics.
  - **Credentials:** Cognos Analytics will prompt for a username and password. When needed, they are directly used to authenticate the user with the IDP using ROPC/password grant.
  - **Credentials and ID Token:** A combination of both. Password grant is used, and claims can come from either the old or new token. Use this if your IDP returns limited claims when using password grant.
  - **Refresh token:** The most secure setting. It is the default recommended setting if it is supported by your IDP. This setting usually requires the offline\_access scope, but check with your administrator to see if additional scopes are required.
- For the **Account mappings (Advanced)** section:

For historical reasons, the **Unique Identifier** must be the internal name that corresponds to the property name in Cognos Configuration. For more information, see [Table 1: Mapping of Cognos Configuration properties to internal names](#).

The rest of the properties must be OIDC claims. If the configured unique identifier is not configured correctly, the following error message appears when you log on:

Cannot create Account object. CAMID property value is null

If none of the Cognos user properties are appropriate for use as the unique identifier, a custom property can be configured to map to any claim.

Both the Cognos Analytics property names and the OIDC claim names are case-sensitive.

The following table lists the property names displayed in Cognos Configuration and the corresponding internal names to use for the unique identifier.

Table 30. Mapping of Cognos Configuration properties to internal names	
Property name in Cognos Configuration	Internal name to use for the unique identifier
Business phone	businessPhone
Content locale	contentLocale
Description	description
Email	email
Fax/Phone	faxPhone
Given name	givenName
Home phone	homePhone
Mobile phone	mobilePhone
Name	name
Pager phone	pagerPhone
Postal address	postalAddress

Table 30. Mapping of Cognos Configuration properties to internal names (continued)	
Property name in Cognos Configuration	Internal name to use for the unique identifier
Product locale	productLocale
Surname	surname
User name	username

**Member Of** is used for simple group configuration. The comma-separated list of claims is looked up in the user claims individually. The resulting array of strings is used to create groups.

Custom properties can be added. For example, use "subjectId: sub" to use the sub claim value as the value of the **subjectId** custom property. Custom properties are exposed in certain parts of the product and they can also be used for a user's **Unique Identifier** as mentioned above.

7. If your IDP is not using a well known certificate, you must import the root certificate authority certificate into the Cognos Analytics keystore using the Third-Party Certificate Tool. Proceed as follows:

- On UNIX or Linux operating systems, type `ThirdPartyCertificateTool.sh -i -T -r cert.cer -p NoPasswordSet`
- On Windows operating systems, type `ThirdPartyCertificateTool.bat -i -T -r cert.cer -p NoPasswordSet`

**Tip:** Replace the *cert* variable with the name of the certificate file that is used by your OpenID Connect identity provider.

The command imports the contents into the CAMKeystore file in the certs directory by using the specified password.

8. Perform the same configuration steps on your backup Content Manager computer.
9. Restart the IBM Cognos service on the Content Manager and the backup Content Manager computers.

## Configuring IBM Cognos Components to Use Active Directory Server

If you install Content Manager on a Microsoft Windows operating system computer, you can configure an Active Directory namespace as your authentication source.

If you install Content Manager on a UNIX-based computer, you must instead use an LDAP namespace to configure Active Directory as your authentication source. If you install Content Manager on a mix of Windows and UNIX computers, you must use an LDAP namespace to configure Active Directory for all Content Managers. When you use an LDAP namespace to authenticate against Active Directory Server, you are limited to LDAP features only. You do not have access to Active Directory features such as advanced properties for domains and single signon with Kerberos delegation.

If you install Content Manager on a Linux-based computer, the same restrictions apply as for UNIX. You must use an LDAP namespace to configure Active Directory as your authentication source.

If you want to use Microsoft SQL Server or Microsoft Analysis Server as a data source and use single signon for authentication, you must use Active Directory as your authentication source.

You cannot connect to the Active Directory Global Catalog, which is a caching server for Active Directory Server. If the connection uses port 3268, you must change it. By default, Active Directory Server uses port 389.

### Procedure

1. [Configure IBM Cognos components to use an Active Directory Server namespace](#)
2. [Enable secure communication to the Active Directory Server](#), if required

## Configuring an Active Directory Namespace

You can use Active Directory Server as your authentication provider.

You also have the option of making custom user properties from the Active Directory Server available to IBM Cognos components.

### Before you begin

For IBM Cognos to work properly with Active Directory Server, ensure that the Authenticated users group has Read privileges for the Active Directory folder where users are stored.

If you are configuring an Active Directory namespace to support single signon with a Microsoft SQL Server or Microsoft Analysis Server data source, ensure the following configuration:

- The IBM Cognos gateway is installed on an IIS web server that is configured for Integrated Authentication on Microsoft Windows operating system.
- The gateway is assigned to the local intranet website in your web browser.
- Content Manager is installed on a Windows 2008 or Windows 2012 server.
- Content Manager, Application Tier Components, IIS web server, and the data source server (Microsoft SQL Server or Microsoft Analysis Server) belong to the Active Directory domain.
- The data source connection for Microsoft SQL Server or Microsoft Analysis Server is configured for **External Namespace** and that namespace must be the Active Directory namespace.

For more information about data sources, see the *IBM Cognos Analytics Administration and Security Guide*.

### Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource > Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the appropriate namespace and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the Authentication component.

5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
6. Specify the values for all other required properties to ensure that IBM Cognos components can locate and use your existing authentication provider.
7. Specify the values for the **Host and port** property.

To support Active Directory Server failover, you can specify the domain name instead of a specific domain controller.

For example, use *mydomain.com:389* instead of *dc1.mydomain.com:389*.

8. If you want to search for details when authentication fails, specify the user ID and password for the **Binding credentials** property.

Use the credentials of an Active Directory Server user who has search and read privileges for that server.

9. From the **File** menu, click **Save**.
10. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

You are prompted to enter credentials for a user in the namespace to complete the test.

Depending on how your namespace is configured, you can enter either a valid user ID and password for a user in the namespace or the bind user DN and password.

## Results

IBM Cognos loads, initializes, and configures the provider libraries for the namespace.

## Make Custom User Properties for Active Directory Available to IBM Cognos Components

You can use arbitrary user attributes from your Active Directory Server in IBM Cognos components. To configure this, you must add these attributes as custom properties for the Active Directory namespace.

The custom properties are available as session parameters through Framework Manager. For more information about session parameters, see the *Framework Manager User Guide*

You can also use the custom properties inside command blocks to configure Oracle sessions and connections. You can use the command blocks can be used with Oracle light-weight connections and virtual private databases. For more information, see the *IBM Cognos Analytics Administration and Security Guide*.

## Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security > Authentication**, click the Active Directory namespace.
3. In the **Properties** window, click in the **Value** column for **Custom properties** and click the edit icon.
4. In the **Value - Custom properties** window, click **Add**.
5. Click the **Name** column and type the name you want IBM Cognos components to use for the session parameter.
6. Click the **Value** column and type the name of the account parameter in your Active Directory Server.
7. Repeat steps 4 to 6 for each custom parameter.
8. Click **OK**.
9. From the **File** menu, click **Save**.

## Enabling Secure Communication to the Active Directory Server

If you are using an SSL connection to the Active Directory Server, you must copy the certificate from the Active Directory Server to the Content Manager location.

## Procedure

1. In every Content Manager location, use your Web browser to connect to the Active Directory Server and copy the CA root certificate to the Content Manager location.
2. Add the CA root certificate to the certificate store of the account that you are using for the current IBM Cognos session:
  - If you are running the IBM Cognos session under a user account, use the same Web browser as in step 1 to import the CA root certificate to the certificate store for your user account.  
For information, see the documentation for your Web browser.
  - If you are running the IBM Cognos session under the local account, use Microsoft Management Console (MMC) to import the CA root certificate to the certificate store for the local computer.  
For information, see the documentation for MMC.
3. In IBM Cognos Configuration, restart the service:
  - In the **Explorer** window, click **IBM Cognos services, IBM Cognos**.

- From the **Actions** menu, click **Restart**.

## Include or Exclude Domains Using Advanced Properties

When you configure an authentication namespace for IBM Cognos, users from only one domain can log in. By using the Advanced properties for Active Directory Server, users from related (parent-child) domains and unrelated domain trees within the same forest can also log in. There is no cross-forest support; there must be a namespace for each forest.

If you set a parameter named `chaseReferrals` to true, users in the original authenticated domain and all child domains of the domain tree can log in to IBM Cognos. Users from a parent domain of the original authenticated domain or in a different domain tree cannot log in.

If you set a parameter named `MultiDomainTrees` to true, users in all domain trees in the forest can log in to IBM Cognos.

### Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security > Authentication**, click the Active Directory namespace.
3. In the **Properties** window, specify the **Host and port** property:
  - For users in one domain, specify the host and port of a domain controller for the single domain.
  - For users in one domain tree, specify the host and port of the top-level controller for the domain tree.
  - For users in all domain trees in the forest, specify the host and port of any domain controller in the forest.
4. Click in the Value column for **Advanced properties** and click the edit icon.
5. In the **Value - Advanced properties** window, click **Add**.
6. Specify two new properties, **chaseReferrals** and **MultiDomainTrees**, with the values from the following table:

<i>Table 31. Advanced properties settings</i>		
<b>Authentication for</b>	<b>chaseReferrals</b>	<b>MultiDomainTrees</b>
One domain	False	False
One domain tree	True	False
All domain trees in the forest	True	True

7. Click **OK**.
8. From the **File** menu, click **Save**.

## Enable single signon between Active Directory Server and IBM Cognos components

By default, the Active Directory provider uses Kerberos authentication. It integrates with the Microsoft Internet Information Services (IIS) web server for single signon if Windows authentication (formerly named NT Challenge Response) is enabled on the IIS web server.

If Windows authentication is enabled, you are not prompted to reenter authentication information when you access IBM Cognos content that is secured by the Active Directory namespace.

If you use Kerberos authentication, you can choose to use Service for User (S4U). S4U allows users to access IBM Cognos Analytics from computers not on the Active Directory domain. To enable S4U, you must use enable constrained delegation.

For example, you have users whose computers do not belong to the domain, but they do have the domain account. When they open their web browsers, they are prompted for their domain account. However, they get the Kerberos ticket with Identity privilege only, which prevents them from getting authenticated to IBM Cognos Analytics. To resolve this issue, you can use S4U.

If you do not want Kerberos authentication, you can configure the provider to access the environment variable **REMOTE\_USER** to achieve single signon.

**Important:** Ensure that you use only the variable **REMOTE\_USER**. Using another variable can cause a security vulnerability.

To enable single signon to use Kerberos authentication, you must ensure that you complete the following tasks:

1. Configure Windows authentication on your Microsoft IIS web server for the ibmcognos/cgi-bin application.
2. Install Content Manager on a computer that is part of the Active Directory domain, for the active and standby Content Managers.
3. Set up the computers, or the user account under which Content Manager runs, to be trusted.

For more information, see the following technote documents:

- [Enabling single sign-on to CRN or Cognos secured against Active Directory technote](http://www.ibm.com/support/docview.wss?uid=swg21341889) (www.ibm.com/support/docview.wss?uid=swg21341889)
- [When using Kerberos Single Sign-on \(SSO\) with Active Directory in Cognos, user is prompted for credentials technote](http://www.ibm.com/support/docview.wss?uid=swg21659267) (www.ibm.com/support/docview.wss?uid=swg21659267)

## Enabling single signon between Active Directory Server and IBM Cognos Components to use REMOTE\_USER

If you do not want Kerberos authentication, you can configure the provider to access the environment variable **REMOTE\_USER** to achieve single signon.

You must set the advanced property **singleSignonOption** to the value **IdentityMapping**. You must also specify bind credentials for the Active Directory namespace.

Microsoft IIS sets **REMOTE\_USER** by default when you enable Windows authentication. If Kerberos authentication is not used, single signon to Microsoft OLAP (MSAS) data sources is not possible.

When you define the **REMOTE\_USER**, you can also choose to save the **REMOTE\_USER** as a trusted credential. Saving as a trusted credential means that scheduled jobs authenticate the **REMOTE\_USER** with the **Binding Credential** privileges.

**Important:** Ensure that you use only the variable **REMOTE\_USER**. Using another variable can cause a security vulnerability.

### Procedure

1. On the computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security > Authentication**, and select the Active Directory namespace.
3. Click in the **Value** column for **Advanced properties** and then click the edit icon.
4. In the **Value - Advanced properties** dialog box, click **Add**.
5. In the **Name** column, type **singleSignonOption**
6. In the **Value** column, type **IdentityMapping**.
7. If you want to save the **REMOTE\_USER** as a trusted credential, in the **Value - Advanced properties** dialog box, click **Add**.
8. In the **Name** column, type **trustedCredentialType**.
9. In the **Value** column, type **IdentityMappingForTC**.

10. Click **OK**.
11. Click in the **Value** column for **Binding credentials**, and then click the edit icon.
12. In the **Value - Binding credentials** dialog box, specify a user ID and password and then click **OK**.

## Enabling single signon to use Kerberos authentication

If your IIS web server is configured for Windows authentication, you do not have to add any additional settings. Kerberos authentication is used as the default.

## Enabling single signon to use Kerberos authentication with constrained delegation

To be able to use constrained delegation, you must define the service principal names (SPN) for the users that are configured to run the IBM Cognos components and your Microsoft Internet Information Services (IIS) web server's application pool in your Active Directory domain.

If you use Kerberos with constrained delegation, you must add an **sAMAccountName** user for Content Manager when you configure your gateway. All active and stand by Content Managers must be configured to run under the same account.

If you are configuring single signon to your database servers, you must configure the **sAMAccountName** for the user who runs the Application Tier Components when you add the Active Directory namespace. All Application Tier Components must be configured to run under the same account.

The SPNs are the users that you enter in the **sAMAccountName** fields in IBM Cognos Configuration.

For example, assume that you have one user who runs the Content Manager component, another who runs the Application Tier Components, and another who runs your web server's application pool. The Content Manager user is CognosCMUser. The Application Tier Components user is CognosATCUser. The application pool user is IISUser. Each user is in the MyDomain domain.

1. You must set up IIS so that your MyDomain\IISUser is the application pool identity
2. Run the setspn command for the computer where IIS is running.

For example:

```
setspn -A http/IISServerName MyDomain\IISUser
setspn -A http/IISServerName.MyDomain.com MyDomain\IISUser
```

3. Run the setspn command for your IBM Cognos users.

For example:

```
setspn -A ibmcognosba/CognosCMUser MyDomain\CognosCMUser
setspn -A ibmcognosba/CognosATCUser MyDomain\CognosATCUser
```

In these commands, you must use ibmcognosba as shown in the examples. The user names and domains must match your environment.

**Note:** In this example, the **sAMAccountName** users you must enter are CognosCMUser and CognosATCUser.

4. If you are configuring single signon to your Microsoft SQL Server or Microsoft SQL Server Analysis Services database server, you must set up the SPN for the database server. For more information, see you database server documentation.
5. Finally, you must configure the constrained delegation in the Active Directory Users and Computers administration tool. On the **Delegation** tab for all users (IISUser, CognosCMUser, and CognosATCUser), you must select **Trust this user for delegation to specified services only** and **Use Kerberos only** to use Kerberos with constrained delegation. Select **Trust this user for delegation to specified services only** and **Use any authentication protocol** if you are using the S4U Kerberos extension.



And then you must add the required SPNs. For example, add `ibmcognosba` as a service type. And add `DomainController1` and `DomainController2` as service type `ldap`.

If you are configuring single signon for the datasource, add the `MSQLSVC` service.

## Procedure

1. On the computer where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security > Authentication**, and select the Active Directory namespace.
3. Click in the **Value** column for **Advanced properties** and then click the edit icon.
4. In the **Value - Advanced properties** dialog box, click **Add**.
5. In the **Name** column, type `singleSignonOption`.
6. In the **Value** column, enter one of the following values:
  - Enter `KerberosS4UAuthentication` if you want to use Kerberos authentication first. If Kerberos fails, Service For User (S4U) authentication is attempted. If S4U fails, the user is prompted for credentials.
  - Enter `S4UAuthentication` if you want to use S4U authentication first. If S4U fails, the user is prompted for credentials.
7. In the **Value - Advanced properties** dialog box, click **Add**.
8. In the **Name** column, type `trustedCredentialType`.
9. In the **Value** column, enter one of the following values:
  - Enter `CredentialForTC` if you want to save the user's credentials as a trusted credential. For example, if you want to use the credentials to run scheduled jobs.
  - Enter `S4UForTC` if you want to save only the authenticated user name as a trusted credential. The user name is saved in UPN format, and scheduled jobs can be run with the UPN without requiring the user's password.
10. Click **OK**.
11. Click in the **Value** column for **Application Tier Components sAMAccountName**, and enter the **sAMAccountName** of the user who runs the Application Tier Components.

**Important:** This value is required only if you are configuring single signon to your Microsoft SQL Server. If you are not configuring single signon to the database server, do not change this value.
12. Click **File > Save**.
13. Restart the IBM Cognos service.
14. On the computer where you installed the Gateway components, open IBM Cognos Configuration.
15. In the **Explorer** window, click **Environment**.
16. Click in the **Value** column for **Content Manager sAMAccountName**, and enter the **sAMAccountName** of the user who runs Content Manager.
17. Click **File > Save**.

## 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 are 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 Analytics. You must configure the namespace before you load the Transformer models.

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

You can configure IBM Cognos components to use multiple IBM Cognos Series 7 authentication providers. All IBM Cognos Series 7 namespaces must use the same primary IBM Cognos Series 7 Ticket Server. Otherwise, you can receive errors or be prompted for authentication more than one time. To maintain performance, also ensure that the ticket server is running.

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

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

## Procedure

1. [Configure a Series 7 namespace](#)
2. [Enable secure communication to the directory server used by the IBM Cognos Series 7 namespace, if required](#)
3. [Enable single signon between IBM Cognos Series 7 and IBM Cognos](#)

## Configuring an IBM Cognos Series 7 Namespace

You can configure IBM Cognos to use one or more IBM Cognos Series 7 namespaces for authentication.

### Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource > Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the appropriate namespace and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the Authentication component.

5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
6. Specify the values for all other required properties to ensure that IBM Cognos components can locate and use your existing authentication provider.

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

The host value can be a server name or an IP address. If you are publishing from PowerPlay Enterprise Server to IBM Cognos Analytics, you must use the same value format that is 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 Analytics.

7. If your namespace environment includes version 15.2 of the IBM Cognos Series 7 namespace, you must disable the **Series7NamespacesAreUnicode** setting.
  - In the **Properties** window, in the **Advanced Properties** value, click the edit icon.
  - In the **Value - Advanced properties** window, click **Add**.
  - In the **Name** box, type **Series7NamespacesAreUnicode**.
  - In the **Value** box, type **False**, and then click **OK**.
8. In the **Properties** window, under **Cookie settings**, ensure that the **Path**, **Domain**, and **Secure flag enabled** properties match the settings that are 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**.

You are prompted to enter credentials for a user in the namespace to complete the test.

Depending on how your namespace is configured, you can enter either a valid user ID and password for a user in the namespace or the bind user DN and password.

## Enabling Secure Communication to the Directory Server Used by the IBM Cognos Series 7 Namespace

If you are using an SSL connection to the Directory Server used by the IBM Cognos Series 7 namespace, you must copy the certificate from the Directory Server to each Content Manager location.

For more information, see the IBM Cognos Access Manager *Administrator Guide* and the documentation for your Directory Server.

## Enabling Single Signon Between IBM Cognos Series 7 and IBM Cognos

If your IBM Cognos Series 7 namespace has been configured for integration with your external authentication mechanisms for single signon, the IBM Cognos Series 7 provider will automatically use this configuration.

By configuring single signon, you are not prompted to reenter authentication information when accessing IBM Cognos content that is secured by the IBM Cognos Series 7 namespace.

### Procedure

1. Ensure that you configured IBM Cognos components to use an IBM Cognos Series 7 namespace as an authentication provider.
2. For IBM Cognos Series 7, start Configuration Manager.
3. Click **Open the current configuration**.
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 Analytics.
6. Save and close Configuration Manager.
7. If the IBM Cognos Series 7 namespace uses the Trusted Signon plug-in for single signon, you must now define the `SaferAPIGetTrustedSignonWithEnv` function.

### Results

You can now add IBM Cognos Upfront Series 7 NewsBoxes to IBM Cognos Analytics.

## 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

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 32. Parameters and description for the SaferAPIGetTrustedSignonWithEnv Function	
Parameter	Description
[in] envVar	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 <code>envVarName</code> and a null <code>envVarValue</code> . Note that the first time this API is called, the <code>envVar</code> array contains only the end of array marker.
[in] reqEnvVarList	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.

Table 32. Parameters and description for the SaferAPIGetTrustedSignonWithEnv Function (continued)	
Parameter	Description
[out] trustedSignonName	A sequence of bytes that identifies the currently authenticated user. This value does not need to be null-terminated. This value is mandatory.
[out] trustedSignonNameLength	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.
[out] trustedDomainName	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.
[out] trustedDomainNameLength	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.
[out] userType	<p>A value that indicates the type of user that Access Manager will authenticate. This value is mandatory.</p> <p>The following return values are required for Access Manager to successfully authenticate users:</p> <p><b>SAFER_NORMAL_USER</b> A named user. OS signons must exist and be enabled in the current namespace.</p> <p><b>SAFER_GUEST_USER</b> A guest user. A guest user account must exist and be enabled in the current namespace.</p> <p><b>SAFER_ANONYMOUS_USER</b> An anonymous user. An anonymous user account must exist and be enabled in the current namespace.</p>
[in/out] implementerData	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.

## Configuring IBM Cognos to Use a Custom Java 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 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 login.

For more information, see the Custom Authentication Provider *Developer Guide*.

## Configure a Custom Authentication Namespace

You can configure IBM Cognos components to use a custom authentication namespace. Any additional configuration for authentication source access, single signon, or custom attributes are dependent on the custom authentication provider implementation.

Ensure that the versions of Java runtime environment (JRE) and Java Software Development Kit that you use are compatible with each other. If you use supported versions of the JRE and Java Software Development Kit that are not compatible with each other, then the custom Java authentication provider that you configure will not appear in the list of namespaces in IBM Cognos Configuration.

### Procedure

1. In every location where Content Manager is installed, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and click **New resource > Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, select **Custom Java Provider** and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.

5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

**Tip:** Do not use colons (:) in the Namespace ID property.

6. Specify the values for all other required properties to ensure that IBM Cognos can locate and use your existing authentication provider.
7. From the **File** menu, click **Save**.
8. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

You are prompted to enter credentials for a user in the namespace to complete the test.

Depending on how your namespace is configured, you can enter either a valid user ID and password for a user in the namespace or the bind user DN and password.

### Results

IBM Cognos loads, initializes, and configures the provider libraries for the namespace.

## Hide the Namespace from Users During Login

You can hide namespaces from users during login. You can have trusted signon namespaces without showing them on the namespace selection list that is presented when users log in.

For example, you may want to integrate single signon across systems but maintain the ability for customers to authenticate directly to IBM Cognos without being prompted to choose a namespace.

### Procedure

1. In each location where you configured a custom Java authentication provider, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security > Authentication**, click the custom Java authentication provider.
3. In the **Properties** window, click the box next to **Selectable for authentication** and select **False**.
4. From the **File** menu, click **Save**.

## Results

The namespace is not shown on the selection list that is presented at login.

## Configuring IBM Cognos components to use LDAP

---

You can configure IBM Cognos components to use an LDAP namespace as the authentication provider. You can use an LDAP namespace for users that are stored in an LDAP user directory, Active Directory Server, IBM Directory Server, Novell Directory Server, or Oracle Directory Server.

You can also use LDAP authentication with IBM Db2 by specifying the LDAP namespace when you set up the data source connection. For more information, see the *IBM Cognos Analytics 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” on page 263](#).

### Procedure

1. [“Configuring an LDAP namespace” on page 264](#)
2. [Make custom user properties available to IBM Cognos components](#), if required
3. [Enable secure communication to the LDAP server](#), if required
4. [Enable single signon between LDAP and IBM Cognos components](#), if required

## LDAP mapping

To bind a user to the LDAP server, the LDAP authentication provider must construct the distinguished name (DN). If the Use external identity property is set to True, it uses the External identity mapping property to try to resolve the user's DN. If it cannot find the environment variable or the DN in the LDAP server, it attempts to use the User lookup property to construct the DN.

If users are stored hierarchically within the directory server, you can configure the User lookup and External identity mapping properties to use search filters. When the LDAP authentication provider performs these searches, it uses the filters that you specify for the User lookup and External identity mapping properties. It also binds to the directory server by using the value you specify for the Bind user DN and password property or by using anonymous if no value is specified.

When an LDAP namespace is configured to use the External identity mapping property for authentication, the LDAP provider binds to the directory server by using the Bind user DN and password or by using anonymous if no value is specified. All users who log on to IBM Cognos by 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 by using the bind user credentials or by using anonymous if no value is specified. When the property is disabled, which is the default setting, searches are performed by 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:** 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.

## Configuring 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 SiteMinder.

If you are configuring an LDAP namespace for a directory server other than LDAP, see the appropriate section:

- For Active Directory Server, see [Configure an LDAP Namespace for Active Directory Server](#).
- For IBM Directory Server, see [Configure an LDAP Namespace for IBM Directory Server](#).
- For Novell Directory Server, see [Configure an LDAP Namespace for Novell Directory Server](#).
- For Oracle Directory Server, see [Configure an LDAP Namespace for Oracle Directory Server](#).

You can also use LDAP authentication with IBM Db2 by specifying the LDAP namespace when you set up the data source connection. For more information, see the *IBM Cognos Analytics Administration and Security Guide*.

### Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource > Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the appropriate namespace and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the Authentication component.

5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
6. Specify the values for all other required properties to ensure that IBM Cognos components can locate and use your existing authentication provider.
7. If you want the LDAP authentication provider to bind to the directory server by using a specific **Bind user DN and password** when you perform 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 run under the authentication context of the user.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following step:

- 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 by using anonymous.

9. Check the mapping settings for the 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**.

You are prompted to enter credentials for a user in the namespace to complete the test.

Depending on how your namespace is configured, you can enter either a valid user ID and password for a user in the namespace or the bind user DN and password.

## Results

IBM Cognos loads, initializes, and configures the provider libraries for the namespace.

## Configuring an LDAP namespace for Active Directory Server

If you configure a new LDAP namespace for use with an Active Directory Server, default values are generated for you.

### Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource > Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, select **LDAP - Default values for Active Directory** and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component. Default values are generated for you. Check them and make changes as needed.

5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

**Tip:** Do not use colons (:) in the Namespace ID property.

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

The following settings are examples:

- For **User lookup**, enter (sAMAccountName=\${**userID**})
- If you use single signon, for **Use external identity**, set the value to **True**.
- If you use single signon, for **External identity mapping**, enter (sAMAccountName=\${environment("REMOTE\_USER")})

If you want to remove the domain name from the REMOTE\_USER variable, enter (sAMAccountName=\${replace(\${environment("REMOTE\_USER")}, "domain\\", "")}).

**Important:** Ensure that you use only the variable REMOTE\_USER. Using another variable can cause a security vulnerability.

- For **Bind user DN and password**, enter **user@domain**.
  - For **Unique identifier**, enter objectGUID
7. If you want the LDAP authentication provider to bind to the directory server by using a specific **Bind user DN and password** when you perform searches, then specify these values.

If no values are specified, the LDAP authentication provider binds as anonymous.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following steps:

- Ensure that **Use external identity** is set to **False**.
- Set **Use bind credentials for search** to **True**.
- Specify the user ID and password for **Bind user DN and password**.

9. 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**.

You are prompted to enter credentials for a user in the namespace to complete the test.

Depending on how your namespace is configured, you can enter either a valid user ID and password for a user in the namespace or the bind user DN and password.

## Results

IBM Cognos loads, initializes, and configures the provider libraries for the namespace.

## Configuring an LDAP namespace for IBM Directory Server

If you configure a new LDAP namespace for use with an IBM Directory Server, default values are generated for you.

### Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource > Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **LDAP - Default values for IBM Tivoli**, and then click **OK**.

The new authentication namespace resource appears in the **Explorer** window, under the **Authentication** component. Check them and make changes as needed.

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 by using a specific **Bind user DN and password** when you perform searches, then specify these values.

If no values are specified, the LDAP authentication provider binds as anonymous.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following steps:

- Ensure that **Use external identity** is set to **False**.
- Set **Use bind credentials for search** to **True**.
- Specify the user ID and password for **Bind user DN and password**.

9. From the **File** menu, click **Save**.

## Configuring an LDAP namespace for Novell Directory Server

If you configure a new LDAP namespace for use with a Novell Directory Server, you must modify the necessary settings and change the values for all properties of the Novell Directory objects.

### Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource > Namespace**.

3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type(Group)** list, click **LDAP**, then in the **Type** list, choose **LDAP - General default values**, and then click **OK**.

The new authentication namespace resource appears in the **Explorer** window, under the **Authentication** component.

5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.

**Tip:** Do not use colons (:) in the Namespace ID property.

6. Specify the values for all other required properties to ensure that IBM Cognos can locate and use your existing authentication namespace.

- For **User lookup**, specify (cn=\${userID})
- For **Bind user DN and password**, specify the base DN for an administration user, such as cn=Admin,o=COGNOS

7. If you want the LDAP authentication provider to bind to the directory server by using a specific **Bind user DN and password** when you perform searches, then specify these values.

If no values are specified, the LDAP authentication provider binds as anonymous.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following steps:

- Ensure that **Use external identity** is set to **False**.
- Set **Use bind credentials for search** to **True**.
- Specify the user ID and password for **Bind user DN and password**.

9. To configure the LDAP advanced mapping properties for use with Novell Directory Server objects, use the values specified in the following table.

Table 33. LDAP advanced mapping values for use with Novell Directory Server objects		
Mappings	LDAP property	LDAP value
Folder	Object class	organizationalunit,organization,container
	Description	description
	Name	ou,o,cn
Group	Object class	groupofnames
	Description	description
	Member	member
	Name	cn
Account	Object class	inetOrgPerson
	Business phone	telephonenumber
	Content locale	Language
	Description	description
	Email	mail

<i>Table 33. LDAP advanced mapping values for use with Novell Directory Server objects (continued)</i>		
<b>Mappings</b>	<b>LDAP property</b>	<b>LDAP value</b>
	Fax/Phone	facsimiletelephonenumber
	Given name	givenname
	Home phone	homephone
	Mobile phone	mobile
	Name	cn
	Pager phone	pager
	Password	(leave blank)
	Postal address	postaladdress
	Product locale	Language
	Surname	sn
	Username	uid

These mapping properties represent changes that are based on a default Novell Directory Server installation. If you modify the schema, you might have to make more 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 the portal, they must have permission to read the ou and o attributes.

10. From the **File** menu, click **Save**.

## Configuring an LDAP namespace for Oracle Directory Server

If you configure a new LDAP namespace for use with an Oracle Directory Server, default values are generated for you.

### Procedure

1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource > Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **LDAP - Default values for Oracle Directory Server** and then click **OK**.

The new authentication namespace resource appears in the **Explorer** window, under the **Authentication** component. Check them and make changes as needed.

5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.

**Tip:** Do not use colons (:) in the Namespace ID property.

6. Specify the values for all other required properties to ensure that IBM Cognos can locate and use your existing authentication namespace.

The following settings are examples:

- For **User lookup**, enter `(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:

```
(ntuserdomainid=$environment("REMOTE_USER"))
```

```
(uid=${environment("REMOTE_USER")})
```

**Important:** Ensure that you use only the variable REMOTE\_USER. Using another variable can cause a security vulnerability.

- For **Unique identifier**, type `nsuniqueid`
7. If you want the LDAP authentication provider to bind to the directory server by using a specific **Bind user DN and password** when you perform searches, then specify these values.

If no values are specified, the LDAP authentication provider binds as anonymous.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following steps:
  - Ensure that **Use external identity** is set to **False**.
  - Set **Use bind credentials for search** to **True**.
  - Specify the user ID and password for **Bind user DN and password**.

9. From the **File** menu, click **Save**.

## Making custom user properties for LDAP available to IBM Cognos components

You can use arbitrary user attributes from your LDAP authentication provider in IBM Cognos components. To configure this, you must add these attributes as custom properties for the LDAP namespace. The custom properties are available as session parameters through Framework Manager.

You can also use the custom properties inside command blocks to configure Oracle sessions and connections. You can use the command blocks with Oracle lightweight connections and virtual private databases. For more information, see the *IBM Cognos Analytics Administration and Security Guide*.

For more information about session parameters, see the *Framework Manager User Guide*.

### Procedure

1. In each location where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security > Authentication**, and select the LDAP namespace.
3. In the **Properties** window, click in the **Value** column for **Custom properties**, and click the edit icon.
4. In the **Value - Custom properties** window, click **Add**.
5. Click the **Name** column, and type the name that 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**.

## Enabling 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.

Go to the section that applies to your version of Cognos Analytics:

- [Release 11.2.2 or earlier](#)
- [Release 11.2.3 or later](#)

### Release 11.2.2 or earlier

#### Before you begin

IBM Cognos works with both the `cert8.db` and `cert7.db` versions of the client certificate database. You must use the `certutil` tool from Netscape Security Services (NSS) to create the certificate databases. IBM Cognos does not accept other versions of `cert8.db` files, including those files from the `certutil` tool that is provided with Microsoft Active Directory.

IBM Cognos includes the `certutil` tool on platforms where Netscape Security Services (NSS) is not listed as a system requirement. The `certutil.exe` file is located in the `installation_location/bin64` directory. You must add `/bin64` to your `LD_LIBRARY_PATH`.

For platforms where NSS is listed as a system requirement, please use that version of the `certutil` tool.

#### Procedure

1. Create a directory for the certificate database.
2. Create the certificate database by typing the following command:

```
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:

```
certutil -A -n certificate_name -d certificate_directory -i CA.cert -t C,C,C
```

- For a directory server certificate:

```
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 *install\_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.

**Important:** You can configure your namespace on-the-fly. That is, you do not have to restart the Cognos Analytics service after you configure the change. In this case, ensure that you configure the same value for every computer that is running the Content Manager service. Otherwise, the Content Manager service on the other computers will not start. Also, ensure that the database is copied to each Content Manager computer.

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 - 11 on every other location where Content Manager is installed.

## Release 11.2.3 or later

### Before you begin

As of release 11.2.3, the Cognos Analytics LDAP provider uses the same TLS subsystem as the rest of the product.

Before you enable secure communication with the LDAP server, do the following:

#### \_\_\_ • Verify the TLS protocol version settings:

In Cognos Configuration, check the values in **Security > Cryptography > SSL Protocol**

#### \_\_\_ • Verify the Supported Cipher Suites settings:

In Cognos Configuration, check the values in **Security > Cryptography > Cognos > Supported ciphersuites**

#### \_\_\_ • Import your CA certificate as a trusted certificate using the third-party certificate tool.


For more information, see [“ThirdPartyCertificateTool commands and usage examples”](#) on page 198.

**Note:** We recommend that you use the third-party certificate tool (see above) to update the keystore. However, you can instead update the keystore using a cert7.db or cert8.db file. Support for cert7.db and cert8.db may be removed in a later release.

### Procedure

On each Content Manager computer where you configured the LDAP namespace to use the directory server, follow these steps:

1. Start Cognos Configuration.
2. In the **Explorer** window, under **Security > Authentication**, click the LDAP namespace.

3. In the **Properties** window, for the **Host and port** property, change the port to the secure LDAPS port number.
4. Set the configuration item **Use TLS** to **true**.
5. If you are using a cert8.db file (*not recommended* - see [Note](#)), follow these steps:
  - a. Click **Advanced properties**,
  - b. Click the pencil icon .
  - c. Add the following name-value pairs:
    - useNSPRNetworking=true
    - sslCertificateDatabase=path to cert8.db
6. From the **File** menu, click **Save**.
7. From the **Actions** menu, click **Restart**.

## Enable 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. For an application server gateway or dispatcher entry that is 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 run time 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 by using the Bind user DN and password or by using anonymous if no value is specified. All users who log on to IBM Cognos by 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 by using the [replace operation](#).

## Replace operation

The replace operation returns a copy of the string with all occurrences of the old substring that is 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 34. Parameters and description for the Replace Operation	
Parameter	Description
str	The string to search.
old	The substring to be replaced by the new substring.
new	The substring that replaces the old substring.

### Examples

```
${replace}(${environment("REMOTE_USER")}, "NAMERICA\\", )}
```

```
${replace}(${environment("REMOTE_USER")}, "NAMERICA\\", "")}
```

## SiteMinder authentication provider

You can configure IBM Cognos Analytics to use a SiteMinder namespace as an authentication source.

The authentication provider uses the SiteMinder Software Development Kit to implement a custom agent. The custom agent deployment requires that you set the Agent Properties in the SiteMinder Policy server administration console to support 4.x agents.

### SiteMinder configuration requirements

Configure the following items in the CA SiteMinder Policy Server:

- Cognos Analytics requires the GET and POST verbs for its functionality. Enable these verbs in the CA SiteMinder Policy Server.
- Enable the encoding of characters or masking of methods by setting the **Is third party XSS Checking enabled?** property to True in Cognos Configuration. For more information, see [“Configuring IBM Cognos components to use IBM Cognos Application Firewall” on page 179](#).
- Customers who embed URLs in their reports should verify the characters passed in the URL parameters and ensure that CA SiteMinder does not treat these characters as **BadURLChars** or **BadCSSChars**. For more information, see the CA SiteMinder documentation.

### SiteMinder configured for more than one user directory

If your SiteMinder environment is configured for more than one user directory, you must use the **SiteMinder** namespace type in IBM Cognos Configuration.

After you configure the SiteMinder namespace in IBM Cognos Configuration, you must also add a corresponding LDAP or Active Directory Server namespace to IBM Cognos Configuration for each user directory that is defined in SiteMinder.

When you configure a corresponding LDAP namespace, ensure that the **External identity mapping** property is enabled and that you include the **REMOTE\_USER** token in property value. This does not mean that you must configure SiteMinder to set **REMOTE\_USER**.

When you configure a corresponding Active Directory namespace, ensure that the **singleSignonOption** property is set to **IdentityMapping**.

The **SiteMinder** namespace passes user information internally to the corresponding LDAP namespace using the **REMOTE\_USER** environment variable when it receives successful user identification from the SiteMinder environment.

For more information, see [“Enabling single signon between Active Directory Server and IBM Cognos Components to use REMOTE\\_USER”](#) on page 255.

**Important:** Ensure that you use only the variable **REMOTE\_USER**. Using another variable can cause a security vulnerability.

## SiteMinder configured with only one user directory

If your SiteMinder environment is configured with only one user directory, you do not have to use the **SiteMinder** namespace type in IBM Cognos Configuration.

In this case, you can use the user directory as your authentication source by configuring the appropriate namespace, or you can configure the **SiteMinder** with one user directory. For example, if the SiteMinder user directory is LDAP, you can configure IBM Cognos components with an LDAP namespace or with one **SiteMinder** namespace, referring to one user directory that is an LDAP namespace.

If the SiteMinder user directory is Active Directory, you can use an Active Directory namespace or an LDAP namespace that is configured for use with Active Directory.

If you want to use the user directory as your authentication source directly instead of configuring a **SiteMinder** namespace, you can configure the appropriate LDAP or Active Directory namespace. In this case, verify the Agent Configuration Object properties in SiteMinder Policy Server. Ensure that **SetRemoteUser** is activated.

When you configure the Active Directory namespace, ensure that the **singleSignonOption** property is set to **IdentityMapping**.

When you configure a corresponding LDAP namespace, ensure that the **External identity mapping** property is enabled and that you include the **REMOTE\_USER** token in property value.

For more information, see [“Enabling single signon between Active Directory Server and IBM Cognos Components to use REMOTE\\_USER”](#) on page 255.

**Important:** Ensure that you use only the variable **REMOTE\_USER**. Using another variable can cause a security vulnerability.

## Configuring a SiteMinder namespace

If you configured SiteMinder for more than one user directory, you must use the **SiteMinder** namespace type in IBM Cognos Configuration. After you add the SiteMinder namespace, you must also add a corresponding LDAP namespace for each user directory in your SiteMinder environment.

You can also use the **SiteMinder** namespace type if users are stored in an LDAP server or an Active Directory server.

You can hide namespaces from users during login. You can have trusted signon namespaces without showing them on the namespace selection list that is presented when users login. For example, you want to integrate single sign-on across systems but maintain the ability for customers to authenticate directly to IBM Cognos without being prompted to choose a namespace.

### Before you begin

To use the **SiteMinder** namespace, you must obtain the required SiteMinder library files, which are shown in the following table, and add the files to the appropriate library path for your operating system.

Table 35. SiteMinder library files	
Operating system	SiteMinder library file
AIX	libsmagentapi.so

Table 35. SiteMinder library files (continued)	
Operating system	SiteMinder library file
Microsoft Windows 64-bit	smagentapi.dll
	smerrlog.dll

## Procedure

- On the computer where you installed Content Manager, append the directory that contains the SiteMinder library file to the appropriate library path environment variable.
  - For AIX operating systems, **LIBPATH**
  - For Microsoft Windows operating systems, **PATH**
- Open IBM Cognos Configuration.
- 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, select the **SiteMinder** and then click **OK**.
- Select the namespace that you added.
- In the **Namespace ID** property, specify a unique identifier for the namespace.
 

**Tip:** Do not use a colon (:) in the identifier.
- Specify values for the other required properties.
 

**Tip:** If you do not want the users to see the namespace name when they log in, set the **Selectable for authentication** property to **False**.
- In the **Explorer** window, under **Security > Authentication**, right-click the namespace that you added, and click **New resource > SiteMinder Policy Server**.
- In the **Name** box, type a name for the policy server and click **OK**.
- In the **Properties** window, specify the **Host** property and any other property values you want to change.
- In the **Explorer** window, right-click the new SiteMinder policy server that you added and click **New resource > User directory**.
- In the **Name** box, type a name for the user directory and click **OK**.
 

**Important:** The name must match the name of the user directory that is found in the policy server.
- In the **Properties** window, type a value for the **Namespace ID reference** property.
- Configure a user directory for each user directory in the SiteMinder policy server.
- Click **File > Save**.
- Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.
 

You are prompted to enter credentials for a user in the namespace to complete the test.

Depending on how your namespace is configured, you can enter either a valid user ID and password for a user in the namespace or the bind user DN and password.
- Configure a corresponding LDAP or Active Directory namespace for each user directory.
 

Ensure that you use the same value for the **Namespace ID** property that you use for the **Namespace ID** property for the SiteMinder namespace.

## Configure IBM Cognos to use SAP

To use an SAP server as your authentication provider, you must use a supported version of SAP BW.

In SAP BW, you can assign users to user groups or roles or both. The SAP authentication provider uses only the roles.

The authorization rights required by the SAP user depend on who uses IBM Cognos components: users or administrators.

## SAP Authorization Settings for IBM Cognos Users

The authorization objects in the following table are required for any IBM Cognos user.

Table 36. SAP authorization settings for IBM Cognos users		
Authorization object	Field	Value
S_RFC Authorization check for RFC access	Activity	
	Name of RFC to be protected	RFC1 RS_UNIFICATION, SDTX, SH3A, SU_USER, SYST, SUSO
	Type of RFC to be protected	FUGR
S_USER_GRP User Master Maintenance: User Groups	Activity	03
	Name of user group	*

Some of the values shown, such as \*, are default values that you may want to modify for your environment.

## SAP Authorization Settings for IBM Cognos Administrators

If users perform administrative tasks and searches for users and roles, the values from the following table must be added to the S\_RFC authorization object in addition to the values for IBM Cognos users.

Table 37. SAP authorization settings for IBM Cognos administrators		
Authorization object	Field	Value
S_RFC Authorization check for RFC access	Activity	16
	RFC_NAME	PRGN_J2EE, SHSS, SOA3
	Type of RFC object to be protected	FUGR

Some of the values shown, such as \*, are default values that you might want to modify for your environment.

## Connectivity Between SAP BW and IBM Cognos on UNIX

To configure connectivity between SAP BW and IBM Cognos components on a UNIX operating system, ensure that you install the SAP shared library file (provided by SAP) and add it to the library path environment variable as follows:

- AIX

```
LIBPATH=$LIBPATH:<librfc.a_directory>
```

## Configure an SAP Namespace

You can configure IBM Cognos components to use an SAP server as the authentication source.

### Before you begin

If you installed your IBM Cognos product on a 64-bit server, you must also manually copy the SAP RFC library files to the IBM Cognos installation directory.

### Procedure

1. If running on a 64-bit server, do the following:
  - Go to the SAP installation directory on the 64-bit server.
  - Copy all 64-bit SAP RFC library files to *install\_location\bin64*.
  - Copy all 32-bit SAP RFC library files to *install\_location\bin*.
2. If running on a 32-bit server, copy all 32-bit SAP library files from the SAP installation directory to the *install\_location\bin64* directory.
3. In the location where you installed Content Manager, open IBM Cognos Configuration.
4. In the **Explorer** window, under **Security**, right-click **Authentication**, and click **New resource > Namespace**.
5. In the **Name** box, type a name for your authentication namespace.
6. In the **Type** list, click **SAP** and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the Authentication component.

7. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.

**Important:** Do not use colons (:) in the Namespace ID property.

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

Depending on your environment, for the **Host** property, you may have to add the SAP router string to the SAP host name.

9. If the SAP system encodes the contents of cookies, enable the decode tickets feature:
  - In the **Properties** window, for **Advanced properties**, click the Value and then click the edit icon.
  - Click **Add**.
  - Enter the name URLDecodeTickets and enter the value true
  - Click **OK**.

All SAP logon tickets will be decoded by the SAP namespace before establishing a connection.

10. From the **File** menu, click **Save**.
11. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

You are prompted to enter credentials for a user in the namespace to complete the test.

Depending on how your namespace is configured, you can enter either a valid user ID and password for a user in the namespace or the bind user DN and password.

## Enable Single Signon Between SAP and IBM Cognos

You can enable single signon between SAP Enterprise Portal and IBM Cognos components as well as when using the external namespace function of the SAP BW data source connections.

To do so, ensure that you set the following system parameters on the SAP BW server:

- **login/accept\_sso2\_ticket = 1**
- **login/create\_sso2\_ticket = 1**
- **login/ticket\_expiration\_time = 200**

## Delete an Authentication Provider

---

If they are no longer required, you can delete namespaces that you added, or unconfigure namespaces that IBM Cognos components detected.

You must not delete the Cognos namespace. It contains authentication data that pertains to all users and is required to save the configuration.

When you delete a namespace, you can no longer log on to the namespace. Security data for the namespace remains in Content Manager until you permanently delete it in the portal. For more information, see the *IBM Cognos Analytics Administration and Security Guide*.

### Procedure

1. In each location where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security > Authentication**, right-click the namespace and click **Delete**.
3. Click **Yes** to confirm.

The namespace disappears from the **Explorer** window and you can no longer log on to the namespace in that location.

4. From the **File** menu, click **Save**.
5. Repeat steps 1 to 4 for each location where you installed Content Manager.

You must now log on to the portal and permanently delete the data for the namespace. For more information, see the *IBM Cognos Analytics Administration and Security Guide*.

### Results

After you delete a namespace, it appears as Inactive in the portal.

---

## Chapter 14. Performance Maintenance

This section includes topics about using IBM Cognos Analytics and other tools and metrics to maintain the performance of your IBM Cognos Analytics environment.

### System Performance Metrics

---

IBM Cognos Analytics 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 the portal. For more information about monitoring system performance metrics, see the *IBM Cognos Analytics Administration and Security Guide*.

You can take a snapshot of the current system metrics so that you can track trends over time or review details about the state of the system at a particular time. For more information, see the topic about the metric dump file in the *IBM Cognos Analytics Troubleshooting Guide*.

You can also monitor system metrics externally to IBM Cognos Administration by using Java Management Extensions (JMX), a technology that supplies tools to manage and monitor applications and service-oriented networks.

### Monitoring System Metrics Externally

You can monitor system metrics outside of IBM Cognos Administration by using industry standard Java Management Extensions (JMX). First, you configure two JMX properties in IBM Cognos Configuration to enable secure access to the metrics in the Java environment. Then you use a secure user ID and password to connect to the metrics through a JMX connection tool.

#### Before you begin

You must install Oracle Java SE Development Kit or the Java Software Development Kit from IBM before you can use the external monitoring feature.

#### Procedure

1. In the location where Content Manager is installed, start IBM Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, under **Dispatcher Settings**, click **External JMX port**.
4. In the **Value** column, type an available port number.
5. Click **External JMX credential**.
6. In the **Value** column, click the edit icon, type a user ID and password, and then click **OK**.

The user ID and password ensure that only an authorized user can connect to the system metrics data in the Java environment, using the port specified in **External JMX port**.

7. Save the changes and restart the service.
8. To access the system metrics data, specify the following information in the JMX connection tool:

- the URL to connect to the system metrics data

For example,

```
service:jmx:rmi:///Content_Manager_server/jndi/rmi://  
monitoring_server:<JMXport>/proxyserver
```

where *JMXport* is the value that you typed for **External JMX port**, and *Content\_Manager\_server* and *monitoring\_server* are machine names. Do not use localhost, even if connecting locally.

- the user ID and password to secure the connection

Use the same values that you configured for **External JMX credential**.

9. To access the local metrics data, specify the following information in the JMX connection tool:

- the URL to connect to the local JMX server

For example,

```
service:jmx:rmi:///local_server_hostname/jndi/rmi:///
local_server_hostname:JMXport/server
```

where *JMXport* is the value that you typed for **External JMX port**, and *local\_server\_hostname* is the local computer name.

- 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 Analytics services are not required in your environment, you can disable them to improve the performance of other services.

For example, to dedicate a computer to running and distributing reports, you can disable the presentation service on an Application Tier Components computer. When you disable the presentation service, the performance of the Application Tier Components will improve.

### Note:

- The Presentation service must remain enabled on at least one computer in your IBM Cognos Analytics 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 Analytics components are not installed on a computer, you should disable the services associated with the missing components. Otherwise the IBM Cognos Analytics components will randomly fail.

## IBM Cognos services

After you install and configure IBM Cognos Analytics, one dispatcher is available on each computer by default. Each dispatcher has a set of associated services, listed in the following table.

Table 38. IBM Cognos services	
Service	Purpose
Agent service	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.
Batch report service	Manages background requests to run reports and provides output on behalf of the monitor service.
Content Manager cache service	Enhances the overall system performance and Content Manager scalability by caching frequent query results in each dispatcher.



Table 38. IBM Cognos services (continued)

Service	Purpose
Content Manager service	<ul style="list-style-type: none"> <li>• Performs object manipulation functions in the content store, such as add, query, update, delete, move, and copy</li> <li>• Performs content store management functions, such as import and export</li> </ul>
Delivery service	Sends emails to an external SMTP server on behalf of other services, such as the report service, job service, or agent service
Event management service	Creates, schedules, and manages event objects that represent reports, jobs, agents, content store maintenance, and deployment imports and exports.
Graphics service	Produces graphics on behalf of the Report service. Graphics can be generated in 4 different formats: Raster, Vector, Microsoft Excel XML or PDF.
Human task service	Enables the creation and management of human tasks. A human task such as report approval can be assigned to individuals or groups on an ad hoc basis or by any of the other services.
Job service	Runs jobs by signaling the monitor service to run job steps in the background. Steps include reports, other jobs, import, exports, and so on.
Log service	<p>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:</p> <ul style="list-style-type: none"> <li>• security events</li> <li>• system and application error information</li> <li>• selected diagnostic information</li> </ul>
Metadata service	Provides support for data lineage information displayed in Cognos Viewer, Reporting, Query Studio, and Analysis Studio. Lineage information includes information such as data source and calculation expressions.
Migration service	Manages the migration from IBM Cognos Series 7 to IBM Cognos Analytics.

Table 38. IBM Cognos services (continued)

Service	Purpose
Mobile service	<p>Manages activities related to IBM Cognos Analytics Mobile Reports client:</p> <ul style="list-style-type: none"> <li>• Transforms reports and analyses for mobile consumption.</li> <li>• Compresses report and analysis content for fast distribution over-the-air to the mobile devices and access from those devices.</li> <li>• Pushes report and analysis content to the mobile devices.</li> <li>• Facilitates incoming and outgoing report-related and analysis-related requests between the mobile device and the environment to search, browse, or run reports.</li> <li>• Synchronizes the mobile content store on the server with the mobile database on the mobile device.</li> <li>• Translates Simple Object Access Protocol (SOAP) messages into wireless-friendly messages.</li> <li>• Communicates with the mobile device.</li> </ul>
Monitor service	<ul style="list-style-type: none"> <li>• Manages the monitoring and execution of tasks that are scheduled, submitted for execution at a later time, or run as a background task</li> <li>• 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.</li> <li>• Creates history objects within the content manager and manages failover and recovery for executing entries</li> </ul>
PowerPlay service	Manages requests to run PowerPlay reports.
Presentation service	<ul style="list-style-type: none"> <li>• Transforms generic XML responses from another service into output format, such as HTML or PDF</li> <li>• Provides display, navigation, and administration capabilities</li> </ul>
Query service	Manages Dynamic Query requests and returns the result to the requesting batch or report service.
Relational metadata service	Used by Framework Manager and CubeDesigner to import metadata from relational databases. It may also be used by Dynamic Query Analyzer at runtime.

Table 38. IBM Cognos services (continued)

Service	Purpose
Report data service	Manages the transfer of report data between IBM Cognos Analytics and applications that consume the data, such as IBM Cognos for Microsoft Office and IBM Cognos Analytics Mobile Reports.
Report service	Manages interactive requests to run reports and provides output for a user.
Repository service	Manages requests to retrieve archived report output from an archive repository or object store.

## Tuning a IBM 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 the application server that IBM Cognos Analytics uses by default. If you want to configure IBM Cognos Analytics to run on another application server, do not use IBM Cognos Configuration to configure the resources. Instead, configure the resources within that application server environment.

The IBM Cognos service is available only on the computers where you installed Content Manager or the Application Tier Components.

### Procedure

1. Start IBM Cognos Configuration.
2. In the **Explorer** window, expand **Environment** > **IBM Cognos services**, and then click **IBM Cognos**.
3. In the **Properties** window, change the value for **Maximum memory in MB**.
  - To reduce the startup time, memory footprint, and resources that are used, use the default setting of 8192 MB.
  - This value can be adjusted based on available system resources.

4. From the **File** menu, click **Save**.

## 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 Analytics Administration and Security Guide*.

To resolve this problem, increase the wait timeout.

### Procedure

1. Go to the following directory:  
`install_locationwebapps/p2pd/WEB-INF/services/`.
2. Open the `reportservice.xml` file in a text editor.
3. Change the `async_wait_timeout_ms` parameter to 120000.
4. Save the file.
5. Restart the service.

---

## Chapter 15. Manually configuring Cognos Analytics on UNIX and Linux operating systems

The console attached to the UNIX or Linux operating system computer on which you are installing IBM Cognos Analytics may not support a Java-based graphical user interface.

You must perform the following tasks manually:

- \_\_\_ • Change default configuration settings by editing the `cogstartup.xml` file, located in the `install_location/configuration` directory.
- \_\_\_ • Change language or currency support, or locale mapping by editing the `coglocale.xml` file, located in the `install_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 Analytics works in your environment. If you distribute IBM Cognos Analytics 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 Analytics by editing the `cogstartup.xml` file to change property values. You can also use sample files that enable IBM Cognos Analytics to use resources that already exist in your environment.

---

### Manually change default configuration settings

If the console attached to your UNIX or Linux operating system computer does not support a Java-based graphical user interface, you must edit the `cogstartup.xml` to configure IBM Cognos Analytics to work in your environment.

**Important:** Some configuration settings are not saved in the `cogstartup.xml` file unless you use the graphical user interface. For example, the server time zone is not set for your IBM Cognos components when you modify the `cogstartup.xml` file directly and then run IBM Cognos Configuration in silent mode. In this case, other user settings that rely on the server time zone may not operate as expected.

If you want IBM Cognos Analytics to use a resource, such as an authentication provider that already exists in your environment, you can add a component to your configuration. You do this by copying the required XML code from the sample files into the `cogstartup.xml` file and then edit the values to suit your environment.

By default, the `cogstartup.xml` file is encoded using UTF-8. When you save the `cogstartup.xml` file, ensure that you change the encoding of your user locale to match the encoding used. The encoding of your user locale is set by your environment variables.

When you edit the `cogstartup.xml` file, remember that XML is case-sensitive. Case is important in all uses of text, including element and attribute labels, elements and values.

Before you edit the `cogstartup.xml` file, ensure that you

- make a backup copy
- create the content store on an available computer in your network
- review the configuration requirements for your installation type

#### Procedure

1. Go to the `install_location/configuration` directory.
2. Open the `cogstartup.xml` file in an editor.

3. Find the configuration setting you want to change by looking at the help and description comments that appear before the start tag of the `<crn:parameter>` elements.
4. Change the value of the `<crn:value>` element to suit your environment.  
**Tip:** Use the type attribute to help you determine the data type for the configuration property.
5. Repeat steps 3 to 4 until the configuration values are appropriate your environment.
6. Save and close the file.

## Results

You should now use a validating XML editor to validate your changes against the rules in the `cogstartup.xsd` file, located in the `install_location/configuration`.

## Adding a component to your configuration

---

The `cogstartup.xml` file contains configuration settings used by IBM Cognos Analytics and by default components. You can change the components that IBM Cognos Analytics 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 Analytics can use only one instance at a time of the following elements:

- The database for the content store
- A cryptographic provider
- A configuration template for the IBM Cognos service

You should be familiar with the structure of XML files before you start editing them.

## Procedure

1. Go to the `install_location/configuration/samples` directory.
2. Choose a sample file to open in an editor:
  - To use Oracle, or IBM Db2 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 Analytics process uses, open the `CognosService_language_code.xml` file.
3. Copy the elements that you need.

**Tip:** Ensure that you copy the code including the start and end tags for the `<crn:instance>` element.

For example, look for the (Begin of) and (End of) comments:

```
<!--
(Begin of) Db2 template
-->
<crn:instance ...>
...
</crn:instance>
<!--
End of) Db2 template
-->
```

4. Go to the `install_location/configuration` directory.

5. Open the `cogstartup.xml` file in an editor.
6. Paste the code from the sample file to the `cogstartup.xml` file and replace the appropriate `<crn:instance>` element.
7. Change the values of these new elements to suit your environment.

For the `<crn:instance>` element, do not change the class attribute. You can change the name attribute to suit your environment.

For example, if you use an Oracle database for the content store, change only the name attribute to suit your environment.

```
<crn:instance class="Oracle" name="MyContentStore">
```

8. Save and close the file.
9. Run IBM Cognos Configuration in silent mode by typing the following command:

```
./cogconfig.sh -s
```

This ensures that the file is valid and that passwords are encrypted.

## Changing manually encrypted settings

---

You can manually change encrypted settings, such as passwords and user credentials, in the `cogstartup.xml` file.

To prompt IBM Cognos Configuration to save an encrypted setting, you change the value and then set the encryption flag to false.

### Procedure

1. Go to the `install_location/configuration` directory.
2. Open the `cogstartup.xml` file in an editor.
3. Find the encrypted setting you want to change by looking at the help and description comments that appear before the start tag of the `<crn:parameter>` elements.
4. Change the value of the `<crn:value>` element to suit your environment.

**Tip:** Use the type attribute to help you determine the data type for the configuration property.

5. Change the encryption value to false.

For example,

```
<crn:value encrypted="false">
```

6. Repeat steps 3 to 5 until the configuration values are appropriate for your environment.
7. Save and close the file.
8. Type the following configuration command:

```
./cogconfig.sh -s
```

### Results

The new settings are saved and encrypted.

## Global settings on UNIX and Linux operating systems

---

If the console attached to your UNIX or Linux operating system computer does not support a Java-based graphical user interface, you must manually edit the `coglocale.xml` file.

You can change global settings

- to specify the language used in the user interface when the language in the user's locale is not available
- to specify the locale used in reports when the user's locale is not available

- to add currency or locale support to report data and metadata
- to add language support to the user interface

By default, IBM Cognos Analytics components ensure that all locales, which may come from different sources and in various formats, use a normalized form. That means that all expanded locales conform to a language and regional code setting.

Before you can add language support to the user interface, you must install the language files on all computers in your distributed installation. For more information, contact your support representative.

### Example 1

A report is available in Content Manager in two locales, such as en-us (English-United States) and fr-fr (French-France), but the user locale is set to fr-ca (French-Canadian). IBM Cognos uses the locale mapping to determine which report the user sees.

First, IBM Cognos checks to see if the report is available in Content Manager in the user's locale. If it is not available in the user's locale, IBM Cognos maps the user's locale to a normalized locale configured on the Content Locale Mapping tab. Because the user's locale is fr-ca, it is mapped to fr. IBM Cognos uses the mapped value to see if the report is available in fr. In this case, the report is available in en-us and fr-fr, not fr.

Next, IBM Cognos maps each of the available reports to a normalized locale. Therefore, en-us becomes en and fr-fr becomes fr.

Because both report and the user locale maps to fr, the user having the user locale fr-ca will see the report saved with the locale fr-fr.

### Example 2

The user's locale and the report locales all map to the same language. IBM Cognos chooses which locale to use. For example, if a user's locale is en-ca (English-Canada) and the reports are available in en-us (English-United States) and en-gb (English-United Kingdom), IBM Cognos maps each locale to en. The user will see the report in the locale setting that IBM Cognos chooses.

### Example 3

The report and the user locales do not map to a common language. IBM Cognos chooses the language. In this case, you may want to configure a mapping. For example, if a report is available in en-us (English-United States) and fr-fr (French-France), but the user locale is es-es (Spanish-Spain), IBM Cognos chooses the language.

## Changing manually the global settings on UNIX and Linux operating systems

Use the following steps to change global settings on UNIX and Linux operating systems using the coglocale file.

### Procedure

1. On every computer where you installed Content Manager, go to the *install\_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 39. Tags for global settings		
Type of element	Start tag	End tag
Language	<supportedProductLocales>	</supportedProductLocales>
Content Locales	<supportedContentLocales>	</supportedContentLocales>
Currency	<supportedCurrencies>	</supportedCurrencies>
Product Locale Mapping	<productLocaleMap>	</productLocaleMap>
Content Locale Mapping	<contentLocaleMap>	</contentLocaleMap>
Fonts	<supportedFonts>	</supportedFonts>
Cookie settings, archive location for reports	<parameter name="setting">	</parameter>

**Tip:** To remove support, delete the element.

4. Save and close the file.

## Results

**Tip:** Use a validating XML editor to validate your changes against the rules in the `cogstartup.xsd` file, located in the `install_location/configuration`.

If you add a currency code that is not supported, you must manually add it to the `i18n_res.xml` file in the `install_location/bin/` directory. Copy this file to each IBM Cognos computer in your installation.

## Starting and stopping Cognos Analytics in silent mode on UNIX and Linux operating systems

You run IBM Cognos Configuration in silent mode to apply the configuration settings and start the services on UNIX or Linux operating system computers that do not support a Java-based graphical user interface.

Before you run the configuration tool in silent mode, you should ensure the `cogstartup.xml` file is valid according to the rules defined in the `cogstartup.xsd` file. The `cogstartup.xsd` file is located in the `install_location/configuration` directory.

## Starting Cognos Analytics in silent mode on UNIX and Linux operating systems

Use the following steps to start the IBM Cognos Analytics software in silent mode.

### Procedure

1. Ensure that the `cogstartup.xml` file, located in the `install_location/configuration` directory, has been modified for your environment.

For more information, see [“Manually change default configuration settings” on page 285](#).

2. Go to the `install_location/bin64` directory.

3. Type the following command

```
./cogconfig.sh -s
```

**Tip:** To view log messages that were generated during an unattended configuration, see the `cogconfig_response.csv` file in the *install\_location/uninstall/logs* directory.

## Results

IBM Cognos Configuration applies the configuration settings specified in the `cogstartup.xml` file, encrypts credentials, generates digital certificates, and if applicable, starts the Cognos service or process.

## Stopping Cognos Analytics in silent mode on UNIX and Linux operating systems

Use the following steps to stop the IBM Cognos Analytics software in silent mode.

### Procedure

1. Go to the *install\_location/bin64* directory.
2. Type the following command  
`./cogconfig.sh -stop`

---

## Chapter 16. Uninstalling IBM Cognos Analytics

It is important to use uninstall programs to completely remove all files and modifications to system files. To uninstall IBM Cognos Analytics, you uninstall server components and modeling tools.

If you are running IBM Cognos Analytics 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 Analytics 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 Analytics components, complete the steps in this section to uninstall on UNIX and Microsoft Windows operating systems.

**Tip:** If monitoring tools such as Process explorer, MMC (Microsoft Management Console) are running during the uninstall, they will interfere with the deletion of the services. This applies to all services in general. For example, after uninstalling Cognos Analytics, product services such as ApacheDS, IBM Cognos, and Informix will not be fully removed, but instead they will show in the services panel as stopped and disabled. To avoid this, do not have any monitoring tools running while running the uninstall. Shutting down these monitoring tools after the uninstall will also complete the removal of the services.

**Important:** Do not delete the configuration and data files if you are upgrading to a new version of IBM Cognos Analytics and you want to use the configuration data with the new version.

**Important:** The Application and associated services must be stopped for the uninstall process to complete. Note that stopping of the services can take up to 15 minutes to complete.

---

### Uninstall IBM Cognos Analytics on UNIX or Linux operating systems

---

If you no longer require IBM Cognos Analytics or if you are upgrading on your UNIX or Linux operating system, uninstall IBM Cognos Analytics.

Uninstalling does not remove any files that changed since the installation, such as configuration and user data files. Your installation location remains on your computer, and you retain these files until you delete them manually.

#### Procedure

1. If the console attached to your computer does not support a Java-based graphical user interface, determine the process identification (pid) of the IBM Cognos Analytics process by typing the following command:

```
ps -ef | grep cogbootstrapservice
```

2. Stop the IBM Cognos Analytics 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 Analytics, go to the *install\_location/uninstall* directory and type the appropriate command:

- If you use XWindows, type  

```
./Uninstall_IBM_Cognos_Analytics
```
- If you do not use XWindows, do a silent uninstallation (see [Use an silent uninstallation](#)).

4. Follow the prompts to complete the uninstallation.
5. Delete all temporary Internet files from the Web browser computers.

# Uninstall Cognos Analytics on Microsoft Windows operating systems

---

If you no longer require IBM Cognos Analytics or if you are upgrading, uninstall all IBM Cognos Analytics 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 Analytics 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 Analytics. 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 Analytics and you want to use the configuration data with the new version.

## Procedure

1. In the **Start** menu list of programs, find the IBM Cognos Analytics application. Right-click the application name, and click **Uninstall**.

If you can't access the **Start** menu, go to the *install\_location*\uninstall directory, and run the Uninstall\_IBM Cognos Analytics.exe 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.

## Recovering from an unsuccessful uninstall

---

If an uninstall is unsuccessful, files, registry entries, and services may remain that should have been deleted. This topic provides guidelines for both Easy and Custom installations.

## Procedure

1. For an Easy, first install:

- a) Remove Informix by executing the Informix uninstall command:

```
install_location\informix\bin\ifxdeploy.exe -u install_location\informix -delifx
```

- a) Remove the following registry key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Informix\Online\ol\_cognoscm

- b) Remove the installation folder *install\_location*

- c) If this is the only InstallAnywhere-based install on your machine, you can remove the InstallAnywhere registry file: %PROGRAM FILES%\Zero G Registry\.com.zerog.registry.xml

2. For all other installations:

- a) Remove the installation folder *install\_location*

- b) If this is the only InstallAnywhere-based install on your machine, you can remove the InstallAnywhere registry file :

On Windows (hidden directory): %PROGRAM FILES%\Zero G  
Registry\.com.zerog.registry.xml

On UNIX: registry file: .com.zerog.registry.xml located:

- If logged in as root, the global registry is located in /var
- If logged in as a user, it is located in the user's home directory.

If you are not sure about the status of InstallAnywhere installations, you can simply rename this file in order to keep a copy of it.



---

## Chapter 17. IBM Cognos content archival

Storing archived content in your external repository provides you with the ability to adhere to regulatory compliance requirements, and can enhance the scalability and performance of IBM Cognos products by reducing the size of content in the content store.

Administrators create a data source connection to an external repository to allow content to move from the content store to the repository. Users can then view the archived content in the external repository. By providing search results for recent and archived content, users can make critical comparisons between current data and historical data. This efficient mechanism allows your company to meet corporate and government requirements while providing a seamless user experience.

The content archived in the external repository is not managed in IBM Cognos environment. For example, if you delete reports in IBM Cognos Analytics, the archived outputs are not deleted in your external repository.

For information about administering your archives, see the *IBM Cognos Analytics Administration and Security Guide*.

There are two workflow scenarios for archiving your content. The first workflow allows administrators archive packages and folders after installing IBM Cognos Content Archival software. The second workflow allows administrators to create repository connections for new packages and folders.

### **Workflow 1: Archiving content after installing connectivity software**

Administrators can archive saved report output for specific packages and folders or all packages and folders after installing or upgrading IBM Cognos Analytics. This workflow only needs to be completed once since all of your content is currently located in your content store.

- Create a data source connection to the external repository.
- Select repository connections for the packages and folders that need to be archived.
- Create and run a content archival maintenance task to select folders and packages to archive in the external repository.

Once you set a repository connection for packages and folders, any new report output is automatically archived, which means that there is no need to run the content archival maintenance task again.

### **Workflow 2: Creating repository connections for new packages and folders**

Administrators can create repository connections for new packages and folders by completing these tasks:

- Create a data source connection to the external repository.
- Select repository connections for the packages and folders that need to be archived.

### **Using content archival content maintenance tasks**

The content archival content maintenance task creates a reference to the report versions in the folders and packages that you select and configure. Selecting folders and packages marks the content within and allows it to remain in the content store until it is archived in your external repository.

It is important to note that this task does not move your content from the content store to the external repository. You must select repository connections for your packages and folders first. Report versions in folders and packages that are not marked for archiving are available for deletion from the content store.

Once the content is marked, the content archival task is complete. A background task in Content Manager finds the marked items and then copies and saves them in the external repository.

Importing content into a folder or package that is configured for archiving to an external repository does not automatically move and archive the imported content into the repository. An administrator must run a content archival content maintenance task for this folder or package to archive the imported content.

## Background tasks

The background XML tasks used to move content from the content store to the external repository are `archiveTask.xml` and `deleteTask.xml`. The `archiveTask.xml` file moves marked content to an external repository. You can also use this file to set thread execution times and archive outputs of selected formats. The `deleteTask.xml` file is a configuration file that retrieves and deletes marked version objects from the queue. You should not modify this file.

## Preserve content IDs before you archive

If required, you can preserve content IDs before report output is archived.

Objects in the content store have content IDs that are deleted and replaced with new IDs by default when you run an import deployment and move content to a target environment. However, there may be situations when you must preserve content IDs, for example, when moving report output to a external report repository.

## Configure content archival

---

You must configure your environment for content archival. For the configuration changes to take effect you must stop and start your IBM Cognos services.

## Creating a file location for a file system repository

To archive reports or report specifications to an IBM Cognos content archival file system repository, you must create an alias root that points to a file location on a local drive or network share.

### Before you begin

You must be an administrator and have access to the file location. Content Manager and Application Tier Components must be able to access this location by using a file URI.

### Procedure

1. If running, stop the IBM Cognos service.
2. Start IBM Cognos Configuration.
3. Click **Actions** > **Edit Global Configuration**.
4. On the **General** tab, select **Alias Roots**, click inside the value field, click the edit button, and when the **Value - Alias Roots** dialog box appears, click **Add**.
5. In the **Alias root name** column, type a unique name for your file system repository.

**Note:** There is no limit to the number of aliases you can create.

6. Type the path to your file system location, where file-system-path is the full path to an existing file location:
  - On Windows, in the **windowsURI** column, type `file:///` followed by the local path, for example, `file:///c:/file-system-path` or type `file://` followed by the server name and share path, for example `file://server/share`.
  - On UNIX or Linux, in the **unixURI** column, type `file:///` followed by the local path, for example, `file:///file-system-path`.

**Note:** Relative paths, such as `file:///../file-system-path`, are not supported.



In a distributed installation, both the Content Manager and Application Tier Components computers must have access to the file location. Use both URIs only in a distributed installation. The UNIX URI and the Windows URI in an alias root must point to the same location on the file system.

7. Click **OK**.

8. Restart the IBM Cognos service. This might take a few minutes.

## Results

Use this file system repository name to create a data source connection to use with the Cognos content archival software. For more information, see the *IBM Cognos Administration and Security Guide*.

## Importing custom classes definitions and properties into IBM Content Manager 8

To use IBM Cognos content archival with IBM Content Manager 8, you must import a set of custom classes and properties files. You must also update the CMIS configuration file with the IBM Cognos folder types.

Custom classes definitions and properties include IBM Content Manager 8 specific metadata. You can install custom classes and properties files at any time.

As there is no Resource Manager that is defined during the installation process, there are conflict error messages during the import process.

### Before you begin

You must have IBM Content Manager 8 installed with an IBM Content Manager 8 CMIS version 1.1 external repository.

### Procedure

1. Open the Content Manager 8 **System Administration Client**.
2. From the main menu, click **Tools > Import XML**.
3. From the **Import XML Options** window, **File to import** section:
  - In the **Data model file** field, click **Browse**, and select the `CMECMIntegrationTypes_RMImport_Manifest.xsd` file from which you want to import the objects.
  - In the **Administrative objects file** field, click **Browse**, and select the `CMECMIntegrationTypes_RMImport_MimeTypes.xml` file to import the Administrative objects file.

The default location is `install_location/configuration/repository/contentManager8/New` directory.
4. To view conflicts, from the **Import XML Options** window, under **Processing options**, select **Process interactively**.
5. Click **Import** to begin the import process.
  - a) From the **Import Preprocessor Results** window, expand **Item Types**, and double-click an item type that indicates a conflict.
  - b) From the **Details of Import Definition and Target Definition** window, in the **Resulting Target** column, select the names for the **Resource Manager** and **Collection** created when you installed Content Manager 8, and click **Accept**.
  - c) Repeat steps a and b for each item type that indicates a conflict.
6. After you resolve all the conflicts, from the **Import Preprocessor Results** window, click **Continue**.
7. From the **Confirm Import Selection** window, click **Import**.
8. After the import is complete, click **OK**.

9. To update the CMIS configuration file to detect the IBM Cognos folder types, run the CMIS for Content Manager 8 configuration program to create a profile.
10. Open the `cmpathservice.properties` file in the IBM CMIS for Content Manager configuration profiles folder.

For UNIX, the default file path is: `/opt/IBM/CM_CMIS/profiles/profile1`

For Windows, the default file path is: `C:\Program Files\IBM\CM_CMIS\profiles\profile1`

- a) Locate the `folderTypes` line.
- b) Add the IBM Cognos folders types `COGNOSREPORT` and `REPORTVERSION` in uppercase. Separate each folder type by a comma.

```
For example,  
folderTypes = C1bFolder,COGNOSREPORT,REPORTVERSION
```

- c) Save and close the file.
11. Run the CMIS for Content Manager 8 configuration program and select the option to redeploy the CMIS configuration file automatically.

**Note:** For more information about manually deploying CMIS, see [Manually deploying IBM CMIS for Content Manager](http://pic.dhe.ibm.com/infocenter/cmgmt/v8r4m0/topic/com.ibm.installingcmcmis.doc/cmsde001.htm) (<http://pic.dhe.ibm.com/infocenter/cmgmt/v8r4m0/topic/com.ibm.installingcmcmis.doc/cmsde001.htm>).

12. From the WebSphere Application Server Liberty Profile administrative console, restart the **CMIS for Content Manager Application**.

## Specifying an available time to run the archival process

To maintain high system performance during peak hours, you can configure a blackout period to specify when the archive or delete tasks run.

A blackout period is a temporary period in which the movement of data is denied. By default, a blackout period is not defined when the software is installed.

### Procedure

1. Go to the `install_location/webapps/p2pd/WEB-INF/cm/tasks/manager` directory.
2. Using an XML text editor, open the `tasksManager.xml` file.
3. For example, to specify a weekly blackout period from 8.00 a.m. to 5 p.m., Tuesday through Friday, add the following `<blackoutPeriods>` element as a child element of the `backgroundTasksManager` element.

- `start time = <hour>08</hour>`
- `stop time = <hour>17</hour>`
- `days =`

```
<day>Tuesday</day>  
<day>Wednesday</day>  
<day>Thursday</day>  
<day>Friday</day>
```

4. If required, decrease the number of threads available to the archiving and deletion processes. The maximum number of threads is 7.
5. Save and close the file.
6. Restart background activities on the Content Manager service.

## Specifying thread execution time

You can use threads to schedule operating system processing time.

The archive and delete background tasks use threads to move content. Threads are units of processing time that are scheduled by the operating system.

### Procedure

1. Go to the *install\_location/webapps/p2pd/WEB-INF/cm/tasks/config* directory.
2. Using an XML text editor, open the `archiveTask.xml` file.
3. For example, to configure three threads that execute from midnight to 8.00 a.m., one thread that executes from 8.00 a.m. to 5.00 p.m., no threads that execute from 5.00 p.m. to midnight, and all threads that run every day of the week, add the following `<executionPeriods>` XML element as a child element of the `backgroundTask` element.

```
<executionPeriods>
<executionPeriod>
  <threads>3</threads>
  <startTime>
    <hour>00</hour>
    <minute>00</minute>
  </startTime>
  <stopTime>
    <hour>08</hour>
    <minute>00</minute>
  </stopTime>
  <days>
    <day>Monday</day>
    <day>Tuesday</day>
    <day>Wednesday</day>
    <day>Thursday</day>
    <day>Friday</day>
    <day>Saturday</day>
    <day>Sunday</day>
  </days>
</executionPeriod>
<executionPeriod>
  <startTime>
    <hour>08</hour>
    <minute>00</minute>
  </startTime>
  <stopTime>
    <hour>17</hour>
    <minute>00</minute>
  </stopTime>
  <days>
    <day>Monday</day>
    <day>Tuesday</day>
    <day>Wednesday</day>
    <day>Thursday</day>
    <day>Friday</day>
    <day>Saturday</day>
    <day>Sunday</day>
  </days>
</executionPeriod>
</executionPeriods>
```

4. Save and close the file.

## Archiving selected formats of report outputs

You can limit archiving to limit archiving to specific output formats. By default outputs of any given format, including PDF, XML, HTML and Excel, are archived.

You can limit archiving of specific output formats to the repository.

### Procedure

1. Go to the *install\_location/webapps/p2pd/WEB-INF/cm/tasks/config* directory.
2. Using an XML text editor, open the `archiveTask.xml` file.

3. For example, to define the archiving of only PDF report output versions, add the following `<outputFormats>` XML element as a child element of the `runOptions` XML element.

```
<outputFormats>
  <outputFormat>PDF</outputFormat>
</outputFormats>
```

You can use the existing sample `outputFormats` element and modify the list to specify output formats to be archived.

You cannot selectively archive multiple file report output versions, for example HTML with graphics.

Save and close the file.

## Specifying that report specifications are not archived

By default, report specification output is archived. Report specifications describe how data was generated within a report.

To turn off the archiving of report specifications, you must modify two files: `CM.xml` and `CM_CM8.xml`.

### Procedure

1. Go to the `install_location/webapps/p2pd/WEB-INF/repositories/config` directory.
2. Using an XML text editor, open the `CM.xml` file.
3. Comment out or remove the following line: `<property name="specifications" metadataPropertyName="specification" useTempFile="true"`
4. Save and close the file.
5. Go to the `install_location/webapps/p2pd/WEB-INF/repositories/config` directory.
6. Open the file named `CM.xml` in a text editor.
7. Comment out or remove the following element:

```
<property repositoryName="REPORTEXECUTIONSPECIFICATION"
  repositoryType="ASSOCIATED"
  metadataPropertyName="specification">
  <associatedObjectTypes>
    <objectType name="VERSIONSPECIFICATION">
      <properties>
        <property repositoryName="cmis:name"
          repositoryType="STRING"
          metadataPropertyName="reportVersionDefaultName" valueHandler="com.cognos.cm.
            repositoryPluginFramework.
            PropertyValueAppendStringHandler" valueHandlerArgument="_specification"/>
      </properties>
    </objectType>
  </associatedObjectTypes>
</property>
```

**Note:** In the `CM.xml` file, the `objectType` name value is `<objectType name="$t!-2_VERSIONSPECIFICATIONv-1">`.

8. Restart background activities on the Content Manager service. For more information, see the *IBM Cognos Analytics Administration and Security Guide*.

## Appendix A. IBM Cognos Configuration command-line options

Use command-line options with the configuration command to modify the behavior of IBM Cognos Configuration when it starts.

Table 40. Command line options and descriptions	
Option	Descriptions
-h	Displays commands for IBM Cognos Configuration.
-s	<p>Runs IBM Cognos Configuration in silent mode.</p> <p>Uses property values specified in the <code>cogstartup.xml</code> file to configure installed components and then starts all services.</p> <pre>./cogconfig.sh -s cogconfig.bat -s</pre>
-stop	<p>Stops all IBM Cognos services.</p> <pre>./cogconfig.sh -stop cogconfig.bat -stop</pre>
-startupfile <i>path/filename.xml</i>	<p>Runs IBM Cognos Configuration using a file other than the <code>cogstartup.xml</code> file in the <code>install_location/configuration</code> directory.</p>
-test	<p>Uses property values specified in the <code>cogstartup.xml</code> file to test configuration settings.</p> <pre>./cogconfig.sh -test cogconfig.bat -test</pre>
-notest	<p>Starts IBM Cognos Configuration with the automatic testing tasks disabled.</p> <pre>./cogconfig.sh -notest cogconfig.bat -notest</pre> <p>This option should not be used for the first time you start the product or if you are making configuration changes.</p>
-utf8	<p>Saves the configuration in UTF-8 encoding.</p> <pre>./cogconfig.sh -s -utf8 cogconfig.bat -s -utf8</pre>

Table 40. Command line options and descriptions (continued)

Option	Descriptions
-l <i>language ID</i>	<p>Runs IBM Cognos Configuration using the language specified by the language identifier.</p> <p>To run the configuration tool in silent mode using Simplified Chinese</p> <pre>./cogconfig.sh -l zh-cn cogconfig.bat -l zh-cn</pre>
-e <i>filename.xml</i>	<p>Exports the current configuration settings to the specified file.</p> <pre>./cogconfig.sh -e filename.xml cogconfig.bat -e filename.xml</pre>
-log	<p>Creates a <code>cogconfig.timestamp.log</code> error log file in the <code>cognos_location/logs</code> directory.</p> <pre>./cogconfig.sh -log cogconfig.bat -log</pre> <p>The log file, <code>cogconfig.log</code>, will be created by default without the <code>-log</code> option in the <code>cognos_location/logs</code> directory.</p>
-d	<p>Enables debug logging in the log file. You need to use it in conjunction with the <code>-log</code> option.</p> <p>The log file, <code>cogconfig.log</code>, will be created by default. You can use the <code>-d</code> option without using <code>-log</code> option.</p>
-config	<p>Saves the IBM Cognos Configuration in silent mode. Loads property values specified in the <code>cogstartup.xml</code> file into IBM Cognos Configuration, then saves it in silent mode without starting the services.</p> <pre>./cogconfig.sh -config cogconfig.bat -config</pre>

You can use more than one command-line option at a time. For example, you can run IBM Cognos Configuration in silent mode and send all error messages to a log file.

---

## Appendix B. About this guide

This document is intended for use with IBM Cognos Analytics. IBM Cognos Analytics is a Web product with integrated reporting, dashboarding, analysis, and event management features.

This guide contains instructions for installing, upgrading, configuring, and testing IBM Cognos Analytics.

### Audience

To use this guide, you should be familiar with

- reporting concepts
- database and data warehouse concepts
- security issues
- basic Windows or UNIX administration skills
- existing server environment and security infrastructure in your organization

### Finding information

To find product documentation on the web, including all translated documentation, access [IBM Knowledge Center](http://www.ibm.com/support/knowledgecenter) (<http://www.ibm.com/support/knowledgecenter>). Release Notes are published directly to IBM Knowledge Center and include links to the latest technotes and APARs.

You can also read PDF versions of the product online help files by clicking the PDF links at the top of each HTML page, or access the PDFs from the [IBM Cognos product documentation web page](http://www.ibm.com/support/docview.wss?uid=swg27047187) ([www.ibm.com/support/docview.wss?uid=swg27047187](http://www.ibm.com/support/docview.wss?uid=swg27047187)).

### Forward-looking statements

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

### Samples disclaimer

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





---

# Index

## A

agent service [280](#)  
audience of document [303](#)

## B

batch report service [280](#)

## C

CA SiteMinder  
    cross-script checking in IBM Cognos Application Firewall [179](#)  
Cognos Analytics portal [62](#)  
Cognos Workspace approved domains [179](#)  
collaboration  
    using IBM Connections [179](#)  
components  
    Cognos Analytics portal [62](#)  
    content store [64](#)  
    data sources [64](#)  
    Event Studio [62](#)  
    Framework Manager [63](#)  
    IBM Cognos Administration [62](#)  
    IBM Cognos Configuration [62](#)  
    Reporting [62](#)  
    Transformer [63](#)  
Content Manager  
    active and standby [186](#)  
    replication [186](#)  
Content Manager service [280](#), [281](#)  
content store  
    component description [64](#)  
    connection management [106](#)  
cross-script checking  
    configuring in IBM Cognos Application Firewall [179](#)

## D

data source connections  
    setting [106](#)  
data sources  
    component description [64](#)  
database client  
    requirements for Transformer [69](#)  
database connection strings  
    IBM Db2 [106](#)  
    Microsoft SQL Server [106](#)  
    Oracle [106](#)  
database connections [106](#)  
databases  
    logging [223](#)  
delivery service [281](#)  
deployment archives  
    importing [88](#)

domains  
    approved for Cognos Workspace [179](#)

## E

enabling  
    IBM Cognos Application Firewall [179](#)  
event logs [223](#)  
event management service [281](#)  
Event Studio  
    component description [62](#)

## F

Framework Manager  
    component description [63](#)

## G

graphics service [281](#)

## H

human task service [281](#)

## I

IBM Cognos Administration  
    component description [62](#)  
IBM Cognos Analytics  
    dispatchers [282](#)  
    services [282](#)  
IBM Cognos Analytics for Microsoft Office [62](#)  
IBM Cognos Application Firewall  
    configuring [179](#)  
IBM Cognos Configuration  
    component description [62](#)  
IBM Cognos Controller  
    data access in IBM Cognos Analytics [71](#)  
IBM Cognos Planning - Analyst  
    data access in IBM Cognos Analytics [70](#)  
IBM Cognos Planning - Contributor  
    data access in IBM Cognos BI [70](#)  
IBM Cognos Series 7 PowerCubes  
    requirements for successful language conversion [71](#)  
IBM Connections [179](#)  
IBM Db2  
    creating connection strings [106](#)  
importing  
    deployment archives [88](#)

## J

JDBC  
    Kerberos single sign-on [214](#), [216](#), [218](#)  
job service [281](#)

## K

Kerberos single sign-on  
JDBC [214](#), [216](#), [218](#)

## L

Linux  
log messages [223](#)  
log messages  
enabling for IBM Cognos Application Firewall [179](#)  
logging  
database [223](#)  
remote log servers [223](#)  
using files [223](#)  
logs  
service [281](#)

## M

Metadata service [281](#)  
Microsoft Office  
report data service [283](#)  
Microsoft SQL Server  
creating connection strings [106](#)  
Migration service [281](#)  
mobile service [282](#)  
modeling [63](#)  
monitor service [282](#)

## O

Oracle  
creating connections strings [106](#)

## P

Planning Analytics [72](#)  
PowerCubes  
access in IBM Cognos Analytics [71](#)  
requirements for successful language conversion [71](#)  
presentation service [282](#)

## Q

query databases [64](#)  
query service [282](#)

## R

relational metadata service [282](#)  
remote log servers [223](#)  
report data service [283](#)  
report services [283](#)  
Reporting  
component description [62](#)  
reporting needs  
for Transformer users [69](#)  
repository services [283](#)  
role-based servers  
considerations for Transformer [69](#)

## S

Series 7 PowerCubes  
requirements for successful language conversion [71](#)  
service  
graphics [281](#)  
human task [281](#)  
services  
agent [280](#)  
batch report [280](#)  
Content Manager [280](#), [281](#)  
delivery [281](#)  
event management [281](#)  
IBM Cognos Analytics [282](#)  
job [281](#)  
log [281](#)  
Metadata [281](#)  
Migration [281](#)  
mobile [282](#)  
monitor [282](#)  
presentation [282](#)  
query [282](#)  
relational metadata [282](#)  
report [283](#)  
report data [283](#)  
repository [283](#)  
syslog  
destination for log messages [223](#)

## T

Transformer  
component description [63](#)  
data access in IBM Cognos Analytics [71](#)

## U

UNIX  
log messages [223](#)

## W

Windows event log  
destination for log messages [223](#)



