IBM Cognos Analytics
Version 11.1

Administration and Security Guide

©

Product Information

This document applies to IBM Cognos Analytics version 11.1.0 and may also apply to subsequent releases.

Copyright

Contents

Introduction

This information is intended for use with IBM® Cognos® Administration, the administrative component of IBM Cognos software.

This information contains step-by-step procedures and background information to help you administer IBM Cognos software.

Finding information

To find product documentation on the web, including all translated documentation, access IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter).

Accessibility Features

IBM Cognos Administration has accessibility features that help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products. The availability of accessibility features can vary however, if other pages and components that do not support accessibility are added to the Cognos Administration user interface.

For information on accessibility features that are available in IBM Cognos Administration, see Appendix A, “Accessibility features,” on page 379.

IBM Cognos HTML documentation has accessibility features. PDF documents are supplemental and, as such, include no added accessibility features.

Forward-looking statements

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

Samples disclaimer

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

Chapter 1. IBM Cognos Software Administration

After IBM Cognos software is installed and configured, you can perform server administration, data management, security and content administration, activities management, and services administration.

You can also perform the following administrative tasks:

- automating tasks
- setting up your environment and configuring your database for multilingual reporting
- installing fonts
- setting up printers
- configuring web browsers
- allowing user access to Series 7 reports
- restricting access to IBM Cognos software

Aside from the typical administrative tasks, you can also customize the appearance and functionality of different IBM Cognos components.

For information about potential problems, see the *IBM Cognos Analytics Troubleshooting Guide*.

IBM Cognos Administration

You must have the required permissions to access **IBM Cognos Administration**.

For more information, see Chapter 13, “Capabilities,” on page 185.

Table 1. Types of administration tools

Administrative Area	Tab	Use
Activities	**Status**	To manage current, past, upcoming, and scheduled IBM Cognos entries.
Content Manager computers	**Status**	To manage Content Manager computers.
Content store	**Configuration**	To perform content store maintenance tasks.
Data sources	**Configuration**	To create and manage data sources connections.
Deployment	**Configuration**	To deploy IBM Cognos , to export from a source environment and then import in a target environment.
Dispatchers and Services	**Status**	To manage dispatchers and services.
Printers	**Configuration**	To create and manage printers.

Table 1. Types of administration tools (continued)

Administrative Area	**Tab**	**Use**
Security	**Security**	To control access to specific product functions, such as administration and reporting, and features within the functions, such as bursting and user-defined SQL.
System, dispatcher, server, and service administration	**Status**	To monitor system performance using system metrics and administer servers.
Server tuning	**Status**	To optimize the speed and efficiency of IBM Cognos software.
Users, groups, and roles	**Security**	To create and manage users, groups, and roles.

Enabling system-wide accessible report output

You can specify system-wide settings for accessible report output that apply to all entries, including reports, jobs, and scheduled entries.

Accessible reports contain features, such as alternate text, that allow users with disabilities to access report content using assistive technologies, such as screen readers.

Accessibility settings in the user preferences and report properties can overwrite the system-wide settings in IBM Cognos Administration.

Accessible reports require more report processing and have a larger file size than non-accessible reports. Consequently, accessible reports affect performance. By default, support for accessible report output is disabled.

Accessible report output is available for the following formats: PDF, HTML, and Microsoft Excel.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Dispatchers and Services**.
2. From the **Configuration** page toolbar, click the set properties button ▤.
3. Click the **Settings** tab.
4. From the **Category** drop-down list, click **Administrator Override**.
5. For the **Administrator Override** category, next to **Accessibility support for reports**, in the **Value** column, click **Edit**.
6. In the **Accessibility support for reports** page, select one of the following options:

Option	**Description**
Disable	Accessible report output is not available to users.
Make mandatory	Accessible report output is always created.

Option	Description
Allow the user to decide	Accessible report output is specified by the user. If you set this option to **Not selected**, then accessible report output is not created automatically. This is the default. If you set this option to **Selected**, then accessible report output is created by default.

Automating Tasks

Virtually everything you can do with the product, you can achieve using the appropriate API, URL interface, or command line tool, as illustrated in the table below.

Table 2. Automating tasks

Goal	Automation interface	Information
Modify a model, or republish it to UNIX or Microsoft Windows operating systems.	Script Player tool	*IBM Cognos Framework Manager Developer Guide* and *IBM Cognos Framework Manager User Guide*
Modify an unpublished model using the updateMetadata and queryMetadata methods.	BI Bus API	*IBM Cognos Software Development Kit Developer Guide*
Retrieve the query items available in the published package using the getMetadata method.	BI Bus API	*IBM Cognos Software Development Kit Developer Guide*
Grant capabilities to users.	BI Bus API	*IBM Cognos Software Development Kit Developer Guide*
Administer and implement security.	BI Bus API	*IBM Cognos Software Development Kit Developer Guide*
Run, view, and edit reports through a hyperlink in an HTML page. Use URLs to view, edit, and run reports.	URL Interface	*IBM Cognos Software Development Kit Developer Guide*
Manipulate objects in the content store. Manage content manager.	BI Bus API	*IBM Cognos Software Development Kit Developer Guide*
Administer reports.	BI Bus API	*IBM Cognos Software Development Kit Developer Guide*
Administer servers and manage dispatchers.	BI Bus API	*IBM Cognos Software Development Kit Developer Guide*
Modify or author reports.	BI Bus API and report specification	*IBM Cognos Software Development Kit Developer Guide*

Setting up a multilingual reporting environment

You can set up a multilingual reporting environment.

You can create reports that show data in more than one language and use different regional settings. This means that you can create one report that can be used by report consumers anywhere in the world.

The samples databases provided with IBM Cognos software store a selection of text fields, such as names and descriptions, in more than 25 languages to demonstrate a multilingual reporting environment.

Here is the process for creating a multilingual reporting environment:

- Use multilingual metadata.

  The data source administrator can store multilingual data in either individual tables, rows, or columns.
- Create a multilingual model.

  Modelers use Framework Manager to add multilingual metadata to the model from any data source type except OLAP. They add multilingual metadata by defining which languages the model supports, translating text strings in the model for things such as object names and descriptions, and defining which languages are exported in each package. If the data source contains multilingual data, modelers can define queries that retrieve data in the default language for the report user.

  For more information, see the *IBM Cognos Framework Manager User Guide*.
- Create multilingual maps.

  Administrators and modelers use a Microsoft Windows operating system utility named Map Manager to import maps and update labels for maps in Reporting. For map features such as country or region and city names, administrators and modelers can define alternative names to provide multilingual versions of text that appears on the map.

  For more information, see the *IBM Cognos Map Manager Installation and User Guide*.
- Create a multilingual report.

  The report author uses Reporting to create a report that can be viewed in different languages. For example, you can specify that text, such as the title, appears in German when the report is opened by a German user. You can also add translations for text objects, and create other language-dependent objects.

  For more information, see the *IBM Cognos Analytics - Reporting User Guide*.
- Specify the language in which a report is viewed.
  - Define multilingual properties, such as a name, screen tip, and description, for each entry in the portal.
  - Specify the default language to be used when a report is run.

    Tip: You can specify the default language on the run options page, in the report properties, or in your preferences.
  - Specify a language, other than the default, to be used when a report is run.

The data then appears in the language and with the regional settings specified in

- the user's Web browser options
- the run options
- the IBM Cognos Analytics preferences

Any text that users or authors add appears in the language in which they typed it.

Configuring Your Database For Multilingual Reporting

IBM Cognos Analytics is a Unicode product capable of querying data in many languages and encoding.

IBM Cognos Analytics typically queries the database using the native data encoding of the database (Latin-1, Shift-JIS, Unicode, and so on). IBM Cognos Analytics translates this data to Unicode as required.

When querying databases with two or more data encodings, Reporting requests the data in Unicode. Certain databases require specific configuration of the client or server software to enable this capability. For more information, see your database vendor documentation.

Note: For information on round trip safety issues when characters are converted from Unicode to Shift-JIS and back, see the information on the Round Trip Safety Configuration utility in Appendix B, "Round Trip Safety Configuration of Shift-JIS Characters," on page 385.

Installing Fonts

IBM Cognos software uses fonts to display HTML reports and pages in browsers, to render PDF reports on the IBM Cognos server, and to render charts used in PDF and HTML reports.

To display output correctly, fonts must be available where the report or chart is rendered. In the case of charts and PDF reports, the fonts must be installed on the IBM Cognos server. For example, if a Reporting user selects the Arial font for a report, Arial must be installed on the IBM Cognos server to properly render charts and PDF files. If a requested font is not available, IBM Cognos software substitutes a different font.

Because HTML reports are rendered on a browser, the required fonts must be installed on the personal computer of each IBM Cognos software user who will read the HTML report. If a requested font is not available, the browser substitutes a different font.

When creating reports, you must select fonts that your IBM Cognos server or users have installed. Microsoft delivers a broad selection of fonts with different language packs, so this will likely not be an issue in Microsoft Windows operating system. However, UNIX servers rarely have fonts installed. You should be prepared to purchase and install the fonts you need on both the server and browser clients.

For information about PDF file settings, see "PDF File Settings" on page 63. For information on using PDF format in reports, see "Report formats" on page 325. For information about configuring fonts and about mapping substitute fonts, see the *IBM Cognos Analytics Installation and Configuration Guide*.

IBM Cognos Default Font

If a requested font is not found, the IBM Cognos server renders PDF files and charts using a default font.

Andale WT, part of the sans serif font family, is the default font because of its wide support of Unicode characters. However, it is not necessarily complete for all languages and may not be considered as attractive as purchased fonts. Also, this font has no Glyph Substitution (GSUB) and Ligature support in most languages.

Reporting Fonts

Reporting is an HTML and JavaScript application that runs in a browser.

Because of the browser design, Reporting operates within the browser security sandbox and has no access to the list of fonts installed on the local computer. Instead, Reporting uses fonts configured in the IBM Cognos global configuration.

For more information, see the *IBM Cognos Analytics Installation and Configuration Guide*.

Setting up printers

To make printers available to users when they distribute reports, you can create entries for printers and save them in the IBM Cognos content store.

When users want to print a report, they can select a printer that you set up without needing to know its network address details.

When you create a printer entry, ensure that the printer you define is set up on the computer where IBM Cognos is installed.

To set up printers, you must have the required capabilities to access **IBM Cognos Administration** functionality. You must have write permissions for the Cognos namespace, see Chapter 13, “Capabilities,” on page 185.

To avoid possible errors, ensure that the following conditions are met before you try printing:

- Ensure that Adobe Reader is installed on each computer where IBM Cognos servers are installed.
- Ensure that the IBM Cognos server is started using an account that has access to the network printer.

  Sometimes, system accounts may not have access to network printers.
- If IBM Cognos is installed on a UNIX operating system, ensure that the command **lpstat -v**, returns a configured printer and that a printer variable is defined.
- When you define the network address for the printer, use the following syntax:

  For Microsoft Windows operating system, use \\server_name\printer_name.

  For a UNIX operating system use *printer_name*, which is the print queue name displayed by the `lpstat -v` command.
- The network name must match the print queue name in lp.
- Ensure that IBM Cognos users have the correct access permissions to the printer.

The role Directory Administrators must have all access permissions granted, and the group Everyone must have read, execute, and traverse permissions granted.

Tip: To check or assign access permissions for a printer, in the **Actions** column, click the set properties button for the printer, and then click the **Permissions** tab.

Procedure

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

   A list of printers appears.

   Tip: To remove a printer, select the check box for the printer and click the delete button.
2. On the toolbar, click the new printer button .
3. Type a name and, if you want, a description for the printer.

   Tip: Use a name that provides details about the printer, such as Color Printer - 4th Floor.
4. Type the network address of the printer by using the format \\server_name\printer_name for a network printer on a Windows installation and *printer_name* for a UNIX operating system installation or for a local printer on Windows.
5. Click **Finish**.

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 3. Enabled browser settings

Browser	**Setting**
All browsers	Allow pop-ups for all Cognos Analytics pages

Table 3. Enabled browser settings (continued)

Browser	Setting
Internet Explorer Edge	Allow Cookies Active Scripting Allow META REFRESH Run ActiveX controls and plug-ins Script ActiveX controls marked safe for scripting Binary and script behaviors Allow programmatic clipboard access User data persistence
Firefox	Allow Cookies Enable Java™ 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

Reporting and Query Studio use the native Microsoft Internet Explorer XML support, which is a component of the browser. ActiveX support must be enabled because Microsoft applications implement XML using ActiveX. Cognos Analytics does not provide or download ActiveX controls. Only the ActiveX controls that are installed as part of Internet Explorer are enabled through this configuration.

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

Cookies used by Cognos Analytics components

Cognos Analytics uses the following cookies to store user information.

Table 4. 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

Table 4. Cookies used by Cognos Analytics components (continued)

Cookie	**Type**	**Purpose**
Cam_passport	Session temporary	Stores a reference to a user session stored on the Content Manager server. Administrators can set the HTTPOnly attribute to block scripts from reading or manipulating the CAM passport cookie during a user's session with their web browser.
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 users
CRN_RS	Persistent	Stores the choice that the user makes for the view members folder in Reporting
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
pp_session	Session temporary	Stores session information that is specific to PowerPlay® Studio
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.
FrameBorder PageOrientation PageSize PDFLayerDimension PDFOPTS	Session temporary	These cookies store the preferences for export to PDF.

Table 4. Cookies used by Cognos Analytics components (continued)

Cookie	Type	Purpose
DimTreeToolbarVisible	Persistent	Stores the setting that determines whether to show or hide the dimension viewer toolbar.
cea-ssa	Session temporary	Stores the setting that determines whether the user session information is shared with other Cognos Analytics components.
BRes	Session temporary	Stores information used to determine the screen resolution to use to render charts.
XSRF (Cross-Site Request Forgery)	Session temporary	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. Prevents a web page loaded from domain X from making requests to domain Y, assuming that the user is already authenticated to domain Y. 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.

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

Allow User Access to Series 7 Reports

If IBM Cognos software is configured properly to use the IBM Cognos Series 7 namespace, you can allow users to access NewsIndexes and NewsBoxes of the Series 7 version of IBM Cognos Upfront.

We recommend that IBM Cognos Analytics and IBM Cognos Series 7 use the same Web server if Upfront is set up to use relative URLs. If IBM Cognos Analytics and IBM Cognos Series 7 use different Web servers, configure Series 7 to use fully qualified URL. This allows users to use the Web browser back button to navigate from Upfront back to IBM Cognos Analytics.

For information about configuring Series 7, see *IBM Cognos Series 7 Configuration Manager User Guide*.

Procedure

1. In IBM Cognos Configuration, configure IBM Cognos to use your IBM Cognos Series 7 namespace. For more information, see the *IBM Cognos Analytics Installation and Configuration Guide*.

2. In the **Properties** window, under **Cookie Settings**, ensure that the **Secure Flag Enabled** property is set to **false**.
3. From the **File** menu, click **Save** and close IBM Cognos Configuration.
4. Ensure that the ticket server for IBM Cognos Series 7 namespace is running.
5. Ensure that the timeout value of the Series 7 ticket server is set to the same value or to a higher value than the IBM Cognos passport timeout value.
6. On the computer where IBM Cognos software is installed, open the `install_location/templates/ps/system.xml` file in an editor.

   Ensure that your editor supports saving files in UTF-8 format.
7. Find and edit (with an XML editor) the `series7` parameter as follows:

   ```
   <!-- Series 7 Integration parameters -->
   <param name="series7">
     <enabled>true</enabled>
     <!-- character encoding used by series7 -->
     <encoding>series7_character_encoding</encoding>
     <!-- host and port to connect to Upfront server -->
     <host>Upfront_host_name</host>
     <port>Upfront_dispatcher_port_number</port>
     <!-- Upfront gateway location -->
     <gateway>Upfront_gateway_location</gateway>
     <!-- If required, specify the prefix for IBM Cognos
   back URLs when linking to Series 7 content. (eg. http://ibmcognos_computer)
   otherwise relative URL's will be used -->
     <back-prefix>http://Series 7_server</back-prefix>
   </param>
   ```

   To view the character encoding used by Series 7, in Series 7 Configuration Manager, on the **Properties** tab, click **IBM Cognos Shared**, click **Locale**, and then click the **Encoding** property.
8. Save the system.xml file in UTF-8 format.
9. Using IBM Cognos Configuration, stop and then restart IBM Cognos Analytics.

   For more information about stopping IBM Cognos Analytics, see the *IBM Cognos Analytics Installation and Configuration Guide*.

Restricting Access to IBM Cognos Software

You may not want all users that exist in an authentication source to have access to IBM Cognos software.

To secure IBM Cognos software, configure the product so that only users who belong to a specific group or role in your authentication source, or in the Cognos namespace, are allowed access.

We recommend using the Cognos namespace because it contains pre-configured groups and roles that help you to secure IBM Cognos software quickly. One of the pre-configured groups is Everyone. By default, the group Everyone belongs to several built-in groups and roles in the Cognos namespace. If you decide to use the Cognos namespace, you must remove the Everyone group from all built-in groups and roles and replace it with groups, roles, or users authorized to access IBM Cognos software.

To restrict access to IBM Cognos software, do the following:

- In IBM Cognos Configuration, enable the required properties to restrict access.

  For more information, see the *IBM Cognos Analytics Installation and Configuration Guide*.
- In **IBM Cognos Administration**, remove the Everyone group from all built-in groups and roles.

  Replace it with groups, roles, or users that are authorized to access the different functional areas of IBM Cognos software. For more information, see Chapter 15, “Initial security,” on page 201.
- Set up access permissions for individual entries, such as folders, packages, reports, pages, and so on. For more information, see Chapter 12, “Access Permissions and Credentials,” on page 173.

For more information about the security concepts implemented in IBM Cognos software, see Chapter 10, “Security Model,” on page 161.

Chapter 2. Building IBM Cognos Analytics applications

You use the IBM Cognos Analytics components to build reporting and analysis applications.

The lifetime of an IBM Cognos Analytics application can be months, or even years. During that time, data may change and new requirements appear. As the underlying data changes, authors must modify existing content and develop new content. Administrators must also update models and data sources over time. For more information about using data sources, see the *IBM Cognos Analytics Administration and Security Guide* and the *IBM Cognos Framework Manager User Guide*.

Before you begin

In a working application, the technical and security infrastructure and the portal are in place, as well as processes for change management, data control, and so on. For additional information, see the IBM Cognos Solutions Implementation Methodology toolkit, which includes implementation roadmaps and supporting documents. Information about the toolkit is available on the IBM Support Portal (www.ibm.com/support/entry/portal/support).

When you use IBM Cognos Analytics to build applications across all of your IBM Cognos Analytics components, you locate and prepare data sources and models, build and publish the content, and then deliver the information. The following graphic provides an overview of the workflow.

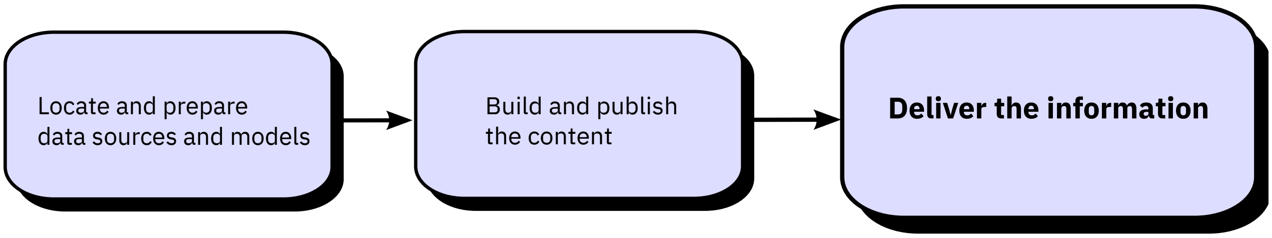

Locate and prepare data sources and models
Build and publish the content
Deliver the information

Figure 1. Using Cognos Analytics to build applications

Procedure

1. Locate and prepare data sources and models.

   IBM Cognos Analytics can report from a wide variety of data sources, both relational and dimensional. Database connections are created in the Web administration interface, and are used for modeling, for authoring, and for running the application.

   To use data for authoring and viewing, the studios need a subset of a model of the metadata (called a package). The metadata may need extensive modeling in Framework Manager.
2. Build and publish the content.

   Reports, scorecards, analysis, workspaces and more are created in the studios of IBM Cognos Analytics. Which studio you use depends on the content, life span, and audience of the report, and whether the data is modeled dimensionally or relationally. For example, self-service reporting and analysis are done through IBM Cognos Query Studio, and IBM Cognos Analysis Studio, and scheduled reports are created in IBM Cognos Analytics - Reporting. Reporting reports and scorecards are usually prepared for a wider audience, published, and scheduled for bursting, distribution, and so on. You can also use Reporting to prepare templates for self-service reporting.
3. Deliver and view the information.

   You deliver content from the IBM Cognos portal and view information that has been saved or delivered by other mechanisms. You can also run reports, analyses, scorecards, and more from within the studio in which they were created.

For information about tuning and performance, see the *IBM Cognos Analytics Administration and Security Guide* and the IBM Support Portal (www.ibm.com/support/entry/portal/support).

Chapter 3. Setting up logging

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.

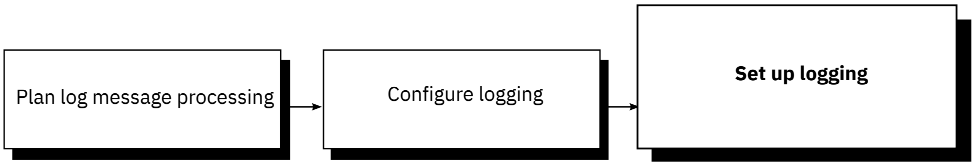


Figure 2. The workflow for implementing logging

- 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.

  For information about configuring logging, see the *IBM Cognos Analytics Installation and Configuration Guide*.
- When setting up logging, specify the level of detail to log to focus messages on the information that is relevant in your organization. Audit reports may also be set up to track user and report activity.

  For information about setting up logging, see the *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*.

Log messages

You can specify the location of log messages and the size and number of log files. You can also configure the log server properties.

By default, log messages are saved to the `cogaudit.log` file located in the `install_location/logs` directory. The log messages can also be saved in a database. For more information, see the *IBM Cognos Analytics Installation and Configuration Guide*.

Use log messages for troubleshooting only. If you want to track report, dashboard, or story usage, use audit reports. For more information, see “Audit reporting” on page 16.

For more information about the log service, see “Dispatchers and Services” on page 37.

Logging levels

You set logging levels to specify the events and messages to record in the log file or in the log database.

An event is an occurrence in your IBM Cognos environment that is significant enough to be tracked, such as starting or stopping a service.

You can set a different logging level for each dispatcher service. You can do this for each dispatcher or for all dispatchers in the same folder. By setting different logging levels for different services you can reduce the amount of irrelevant logging information. For example, if you must troubleshoot the batch report service, you can select a detailed logging level for just that service, keeping log messages to a minimum. The logging level for a service applies to all its components.

Tip: The log service does not have logging levels associated with it.

The following table indicates the details that each logging level logs.

Table 5. Logging levels

Details	**Minimal**	**Basic**	**Request**	**Trace**	**Full**
System and service startup and shutdown, runtime errors	X	X	X	X	X
User account management and runtime usage		X	X	X	X
Use requests		X	X	X	X
Service requests and responses			X		X
All requests to all components with their parameter values				X	X
Other queries to IBM Cognos components (native query)				X	X

You can maintain system performance by managing the amount of logging performed by the server. Since extensive logging affects server performance, increasing the logging level may negatively affect the performance of IBM Cognos software.

The default logging level is Minimal. Use Full logging and Trace levels only for detailed troubleshooting purposes, under the guidance of customer support. They may significantly degrade server performance.

If you are using audit reporting, refer to "Setting up audit reporting" on page 17 for guidelines on setting the logging level. For information on setting logging levels for audit reports, see "Audit reporting" on page 16.

Report validation levels and logging levels

You can collect information about report validation levels by setting the corresponding logging level. Report validation messages can be included in system log messages.

You can use the validation information in different ways. If the system is delivering a generally poor response, you can set logging to a higher level. The additional information can help you determine which reports are at fault and why. If you see warning messages in the logs, this may mean that users are receiving questionable results. You can alert the owners of the offending reports.

There are four report validation levels and five logging levels. The following table shows the correspondence between them.

Table 6. Report validation levels and logging levels

Report validation level	**Logging level**
Error	Minimal, Basic
Warning	Request
Key Transformation	Trace
Information	Full

The higher you set the logging level, the more it degrades system performance. Normally, you set the level to Minimal or Basic to collect errors, or to Request to collect errors and warnings.

For information about reports and report validation, see the *IBM Cognos Analytics - Reporting User Guide*.

Native query logging

If you want to create audit reports that include the queries that are run against your reporting data source, you must enable native query logging. You can use native query logging to learn what kinds of information users want or whether a report is running efficiently. For information on creating audit reports, see "Audit reporting" on page 16.

To enable native query logging in Dynamic Query Mode (DQM), set **Audit logging level for query service** to **Request** or higher when you set up audit reporting . However, if you are using audit reports, you can enable native query logging independently from Request level logging, as described in "Setting logging levels" on page 16.

Report execution options logging

You can log report execution options to your logging system. The report execution options include: prompt parameters, run options, and report specifications.

This functionality is disabled by default. You can enable this functionally using the following advanced parameters of the report service and batch report service:

RSVP.PARAMETERS.LOG
When this parameter is set to true, the run options and prompt parameters are logged.

Default: false

RSVP.REPORTSPEC.LOG
When this parameter is set to true, the report specifications are logged.

Default: false

For information about setting these parameters for the report service and batch report service, see "Configuring advanced settings for specific services" on page 464.

Setting logging levels

You set logging levels to specify the events and messages to record in the log file or in the log database.

An event is an occurrence in your IBM Cognos environment that is significant enough to be tracked, such as starting or stopping a service.

Logging levels that you set for the system apply to all dispatchers and services. Logging levels that you set at the dispatcher level apply to all services that are associated with the dispatcher. Logging levels that you set for individual services apply to the service across all dispatchers.

Logging levels that are set for dispatchers override logging levels that are set for the system. Logging levels that are set for services override logging levels that are set for dispatchers or the system.

If you are using logging for troubleshooting purposes, see "Logging levels" on page 14 for guidelines on setting the logging levels. If you are using audit reports, see "Setting up audit reporting" on page 17.

Before you begin

You must have the required permissions to access **IBM Cognos Administration** functionality. For more information, see Chapter 13, "Capabilities," on page 185.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **All dispatchers** or **Services**, depending on where you want to set logging levels.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. For the item whose logging levels you want to set, from its **Actions** menu, click **Set properties**.
4. Click the **Settings** tab.
5. To filter the list, from the **Category** menu, click **Logging**.
6. In the list, find the service that you want and from the **Value** menu, select the logging level you want for the service.
7. If native query logging is available for the service and you want to use it, select the **Audit the native query for batch report service** check box.

   For more information, see "Native query logging" on page 15.
8. Click **OK**.

Audit reporting

Use audit reports to view information about the report, dashboard, and story activities in the logging database.

Audit reports provide information about access to reports, dashboards, and stories. This information is recorded in the logging database when a report, dashboard, or story is created, run, or modified. It includes the name and location of the report, dashboard, or story, name of the user who ran or modified it, and the time and date when this happened.

The possible uses of audit information include:

- Capacity planning
- Licensing conformance
- Performance monitoring
- Identifying unused content

IBM Cognos Analytics extended samples include sample audit reports. For more information, see the *Samples for IBM Cognos Analytics Guide*.

Setting up audit reporting

Before you can create audit reports or use the sample audit reports that come with IBM Cognos software, you must set up audit reporting.

To enable audit reporting, set the logging level for all or selected IBM Cognos services to **Basic** (auditing enabled) or **Request**. If you set the logging level to **Minimal**, auditing is disabled. Use **Full** logging and **Trace** levels only for detailed troubleshooting purposes, under the guidance of customer support. They might significantly degrade the server performance.

Procedure

1. Set up a logging database in the database system that is used by your organization.

   For more information, see the guidelines for creating a logging database in the *IBM Cognos Analytics Installation and Configuration Guide*.
2. In IBM Cognos Configuration, under **Environment** > **Logging**, configure log messages to be sent to the database that you created in step 1.
3. In **Cognos Administration**, set the appropriate logging levels for the Cognos services.
   a) Go to **Manage** > **Administration console**.

   b) On the **Status** tab, select **System**.

   c) In the **Scorecard** pane, select the **All dispatchers** view.

   d) From your dispatcher actions menu, click **Set properties**, and click the **Settings** tab.

   e) From the **Category** drop-down list, select **Logging**.

   f) Set the logging level to **Basic** for the following services: Content Manager Cache service, Content Manager service, query service. You can enable audit logging for other services, depending on your organization requirements, or even for all services if you are not concerned about the impact on server performance.

   g) To enable native query logging in Compatible Query Mode (CQM), select both of these check boxes:

   - **Audit the native query for batch report service**
   - **Audit the native query for report service**

   h) To enable native query logging in Dynamic Query Mode (DQM), set **Audit logging level for query service** to **Request** or higher.

   i) Click **OK**.
4. In Cognos Configuration, restart the **IBM Cognos** service.

View Full Details for Secure Error Messages

You can view full error details, which may contain sensitive information.

Some IBM Cognos error messages may contain sensitive information such as server names. By default, the IBM Cognos Application Firewall secure error messages option is enabled. Users are presented with information that indicates only that an error has taken place.

If you have the appropriate permissions, you can retrieve full error details. You may also want to see log messages, refer to "Log messages" on page 13.

Procedure

1. Find the error code ID in the user error message. For example, the error number in the following message is secureErrorID:2004-05-25-15:44:11.296-#9:

An error has occurred. Please contact your administrator. The complete error has been logged by CAF with SecureErrorID:2004-05-25-15:44:11.296-#9

2. Open the `cogaudit.log` file in the in *install_location*/`logs` directory.
3. Search for the error code ID to locate the applicable error message.

Disable the creation of core dump files

Core dump files are created for serious problems, such as an unhandled exception or an abnormal termination of an IBM Cognos process.

If such a problem occurs, you receive the following error message:

```
Report Server not responding.
```

Since core dump files are big and a new one is created each time the problem recurs, you may want to disable them. You can enable core dump files again if you encounter problems that require it.

You may also want to delete any existing core dump files from the `\bin` directory of the IBM Cognos server installation, if they are not required for troubleshooting purposes. In a Microsoft Windows environment, core dump files have a .dmp extension and the file name *processID*.dmp, such as BIBusTKServerMain_seh_3524_3208.dmp. In a UNIX environment, the files are named core. In a Linux environment, the files are named `core.`*processID*.

Procedure

1. On the server where IBM Cognos Analytics is installed, open the `cclWinSEHConfig.xml` file from the *install_location*`\configuration` directory.
2. In the configuration element, change the value of the environment variable setting to 0 (zero) so that it reads

   ```
   <env_var name="CCL_HWE_ABORT" value="0"/>
   ```

3. Save the file.

Using logging to diagnose a problem for a specific user

You can use logs to diagnose a problem that is occurring for one or more specific users.

You temporarily set logging to occur for the specified users only. After the problem is resolved, you disable the user-specific logging and resume normal logging without interfering with existing logging settings.

You enable and disable logging for specific users by using the Remote Process service for Java Management Extensions (JMX), a technology that supplies tools to manage and monitor applications and service-oriented networks. You connect to the JMX Remote Process service using the jconsole executable that is provided with the Java JDK. By default, output from the user-specific logging is saved in the *install_location*`\logs` directory.

Before you begin

You must first enable user-specific logging for IBM Cognos Analytics. For more information, see the *IBM Cognos Analytics Installation and Configuration Guide*.

Procedure

1. Connect to the JMX Remote Process service by launching the `jconsole` executable and specifying the following information:

   - The URL to connect to the data. For example,

service:jmx:rmi://*Content_Manager_server*/jndi/rmi://
monitoring_server:<*JMXport*>/proxyserver

where *JMXport* is the value from **External JMX port** in IBM Cognos Configuration, and *Content_Manager_server* and *monitoring_server* are computer names. Do not use the name localhost, even if connecting locally.

- The user ID and password to secure the connection.
- The values from **External JMX credential** in IBM Cognos Configuration.

2. In the remote process server connection window, expand **com.cognos**, **Metrics**, **camAsyncAA**, http://*server_name*:*port_number*/p2pd and select the **Operations** node.
3. Copy the user's CAMID into the **enableDyeTrace** field and click the **enableDyeTrace** button.

   Tip: In IBM Cognos Administration, you can find the CAMID by doing the following:

   - Click the **Security** tab and then click **Users, Groups, and Roles**.
   - Click **Set properties** for the user and then click **View the search path, ID and URL**

   You must have the required permissions to access **IBM Cognos Administration**. For more information, see Chapter 13, “Capabilities,” on page 185.
4. To verify that you enabled the user correctly, navigate to **Attributes** and view the contents of the **DyeTracedUsers** setting.

Running logging for a specific user by editing component specific ipf files

You can start logging for a specified user and implement dye tracing by editing component specific ipf files.

Procedure

1. Add a `<filter>` element to an existing `<appender>` definition or add a new `<appender>` definition.

   You need to ensure that categories make reference to an `<appender>` definition which uses the `<filter>` element.
2. In cases where an `<appender>` definition specifies a log server, change the port values to your configured log server port.

Running logging for a specific user by using selected categories

To start logging for a specified user, implement dye tracing and customize the output by using selected categories and distributing output to one or more appender definitions.

Procedure

1. In the *install_location*\configuration directory, locate the `ipf` trace file for the component that you want to trace. The files are named ipf*component*clientconfig.xml.sample. For example, `ipfAAAclientconfig.xml`.
2. Create a copy of the identified ipf*component*clientconfig.xml.sample file using the name `ipfclientconfig.xml.off`.
3. Using a text editor, open the `ipfclientconfig.xml.off` file and make the following changes:

   - Add or change the log level of the `<categories>` you require.
   - Perform one of the following two actions:

     Add a new `<appender>` section below the last existing `<appender>` element, as follows:

```
<appender name="DyeTraceOutput" class="org.apache.log4j.RollingFileAppender">
        <param name="File" value="../logs/dyetrace_output.log"/>
        <param name="MaxBackupIndex" value="1"/>
        <param name="MaximumFileSize" value="10485760"/>
        <layout class="org.apache.log4j.PatternLayout"/>
```

```
      <param name="ConversionPattern" value="%m%n"/>
   </layout>
   <filter class="com.cognos.indications.LogIPFDyeTraceFilter"/>
</appender>
```

or modify one of the existing appender definitions by adding the line

```
<filter class="com.cognos.indications.LogIPFDyeTraceFilter"/>
```

before closing the `</appender>` tag.

4. For the `<categories>` sections that you want to apply the dye trace filter to, edit the `<appender-ref>` property to refer to the DyeTraceOutput appender or to the appender which had the filter added to it. For example:

```
<category name="Audit.RTUsage.CAM.AAA" class="com.cognos.indications.
LogTypedLogger" additivity="false">
   <level value="debug"/>
   <appender-ref ref="DyeTraceOutput"/>
</category>
```

5. Save the `ipfclientconfig.xml.off` file.
6. To activate this file, rename it to`ipfclientconfig.xml`
7. You can disable user-specific logging and resume normal logging by renaming the `ipfclientconfig.xml` file back to `ipfclientconfig.xml.off`. Reset the users you applied DyeTracing to after restarting the product.

Results

Within 60 seconds, user-specific logging is automatically activated and output is generated. For the appender described here, the output is stored in the *install_location*`\logs\dyetrace_output.log` file. For other appenders, it will be the destination configured for that appender. When an authenticated session is established with IBM Cognos, only actions by the specified user are logged.

You might receive some indications that are not related to the specified user. For example, this might occur when you start the product or when indications are logged before the user's authentication is complete. You can change the log level of categories to avoid an overwhelming number of indications.

Disabling logging for a specific user

You can disable logging for a specific user.

Procedure

Delete the `ipfclientconfig.xml` file that you created in "Using logging to diagnose a problem for a specific user" on page 18.

Results

Normal logging of all users resumes. It could take up to 30 seconds for the user-specific logging to stop.

Chapter 4. System Performance Metrics

You can monitor system performance using metrics in IBM Cognos Administration, which allows you to diagnose and fix problems quickly.

For example, you may want to know if there are more than 50 items in a queue or if any item has been waiting in a queue for longer than a specified amount of time.

You must have the required permissions to access **IBM Cognos Administration** Chapter 13, “Capabilities,” on page 185.

Using metrics, you can assess the status of the system as a whole, along with the status of individual servers, dispatchers, and services. You can view the attributes for each metric score, set the threshold values that are used to calculate metric scores, and reset metrics. You may want to refresh report service connections if a PowerCube has been rebuilt.

You can also perform functions such as starting and stopping dispatchers or services “Stopping and starting dispatchers and services” on page 40, and unregistering dispatchers “Removing dispatchers from the environment” on page 43.

You can use log files to analyze long-range performance and usage Chapter 3, “Setting up logging,” on page 13.

You can create a metric dump file for troubleshooting purposes.

How Metric Data is Gathered

Data for metrics is gathered differently depending on the metric change type, time scope, and gathering time associated with the metric.

For more information on how these apply to individual metrics, see “System Metrics” on page 22.

Metric Change Type

The value that is displayed for a metric depends on the change type, as shown in the following table.

Table 7. Metric change types

Change Type	Description
Counter	The value is a sum that increases with each change. For example, number of requests is a counter change type.
Gauge	The value may increase or decrease over time, depending on events. For example, the number of processes running at any time is a gauge change type.

Metric Time Scope

The interval over which a metric value is gathered differs by metric, as shown in the following table.

Table 8. Metric time scopes

Time Scope	Description
Point in time	The value is gathered at a specific point in time, such as when you reset a metric group or restart a service
Since reset	The value is gathered over the interval since the last reset of the metric

Metric Gathering Time

The time at which a metric value is gathered differs by metric, as shown in the following table.

Table 9. Metric gathering times

Gathering Time	Description
On change	The value is collected when a change occurs, such as when the number of requests changes
On demand	The value is gathered when you select a new item in the Scorecard pane, or reset a metric group. For more information, see "Panes on the Status System Page" on page 31 and "Resetting metrics" on page 34.
Unknown	The gathering time is unknown

System Metrics

There are a wide variety of metrics available to help you monitor the performance of your IBM Cognos software installation.

For more information, see "How Metric Data is Gathered" on page 21.

Some metrics are reset when the service restarts. You can also reset some metrics manually "Resetting metrics" on page 34.

At the system and server levels, the metrics include all associated dispatchers. At the dispatcher level, metrics include all associated services. For server groups, metrics are for all the dispatchers in the group.

Session Metrics

You can use session metrics to monitor user sessions. This is useful for monitoring system trends such as usage patterns by time of day and day of week. Session metrics are also useful for understanding the context of other metrics. For example, if the number of sessions is extraordinarily high, it could account for the queue length metrics being higher than normal. For more information, see "Queue Metrics" on page 23

The following session metrics are available:

- **Number of sessions**

  Specifies the number of currently active user sessions.

Table 10. Number of sessions

Entry	Change Type	Time Scope	Gathering Time
System	Gauge	Point in time	On demand

- **Number of sessions high watermark**

  Specifies the maximum number of active user sessions since the last reset.

Table 11. Number of sessions high watermark

Entry	Change Type	Time Scope	Gathering Time
System	Gauge	Since reset	On change

- **Number of sessions low watermark**

  Specifies the minimum number of active user sessions since the last reset.

Table 12. Number of sessions low watermark

Entry	Change Type	Time Scope	Gathering Time
System	Gauge	Since reset	On change

Queue Metrics

You can use queue metrics to determine if the system is keeping up with demand. For example, if requests spend too much time in a queue, you may not have enough resources to meet demand.

Queue metrics are available for services that use queues, such as the report service and report data service.

At the system level, queue metrics are available for the following entries:

- Job

  Job queue contains metrics related to the internal queue used by all event management services.
- Task

  Task queue contains metrics related to the internal queue used by all monitor services. This queue contains tasks until they are successfully completed.
- SMTP

  SMTP queue contains metrics related to the internal queue used by all delivery services. This queue contains e-mail messages until they are sent.

Some of the metrics available for these queue metric groups must be enabled to be displayed. For more information, see "Enabling job, SMTP, and task queue metrics" on page 83.

The following queue metrics are available:

- **Latency**

  Specifies the average amount of time that requests have spent in the queue (in seconds).

Table 13. Latency

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Service	Gauge	Since reset	On change

- **Number of queue requests**

  Specifies the number of requests that have passed through the queue.

Table 14. Number of queue requests

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Service	Counter	Since reset	On change

- **Queue length**

  Specifies the number of items currently in the queue.

Table 15. Queue length

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Service	Gauge	Point in time	On demand

- **Queue length high watermark**

  Specifies the maximum number of items in the queue since the last reset.

Table 16. Queue length high watermark

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Service	Gauge	Since reset	On change

- **Queue length low watermark**

  Specifies the minimum number of items in the queue since the last reset.

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Service	Gauge	Since reset	On change

- **Time in queue**

Specifies the cumulative amount of time that requests have spent in the queue (in days, hours, minutes, and seconds).

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Service	Counter	Since reset	On change

- **Time in queue high watermark**

  Specifies the maximum length of time that a request waited in the queue (in days, hours, minutes, and seconds).

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Service	Gauge	Since reset	On change

- **Time in queue low watermark**

  Specifies the minimum length of time, in days, hours, minutes, or seconds, that a request waited in the queue.

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Service	Gauge	Since reset	On change

JVM Metrics

You can use JVM metrics to monitor the Java Virtual Machine and the associated heap size, which specifies the amount of memory that is currently in use. For example, if a dispatcher has been running for a long time and heap usage is high, you may want to restart the dispatcher. The maximum heap size metric tells you if you have allocated a suitable amount of memory to the JVM based on the amount of hardware memory available. The current heap size, in relation to the maximum heap size, lets you know if available memory is being used. If current heap size is close to the maximum heap size, you may want to adjust tuning settings to reduce the load on a particular JVM. The current heap size may vary widely depending on the current load on the system.

For more information on tuning, see "Tuning server performance" on page 56.

The following JVM metrics are available:

- **Current heap size (bytes)**

  Specifies the current size of the JVM heap (in bytes).

Entry	Change Type	Time Scope	Gathering Time
Dispatcher	Gauge	Point in time	On demand

- **Initially requested heap size (bytes)**

Specifies the initial amount of memory that the JVM requests from the operating system during startup (in bytes).

Entry	Change Type	Time Scope	Gathering Time
Dispatcher	Gauge	Point in time	On demand

- **Maximum heap size (bytes)**

  Specifies the maximum amount of memory that can be used by the JVM (in bytes).

Entry	Change Type	Time Scope	Gathering Time
Dispatcher	Gauge	Point in time	On demand

- **Up time**

  The length of time that the JVM has been running (in days, hours, minutes, and seconds.

  At the system, server, and server group levels, this is the highest value from all associated dispatchers.

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Dispatcher	Counter	Point in time	On demand

- **Committed heap size**

  Specifies the amount of memory that is guaranteed to be available for use by the JVM (in bytes).

Entry	Change Type	Time Scope	Gathering Time
Dispatcher	Gauge	Point in time	On demand

Request Metrics

You can use request metrics to monitor volume of requests, operational status of services, response times, and processing times. General request metrics include data for all services and are a consolidation of metrics for all dispatchers. Request metrics specific to a service include only data for that service.

At the system, server, and server group levels, the metrics include data from all associated dispatchers. At the dispatcher level, metrics include all associated services.

The following request metrics are available:

- **Current time**

  Specifies the current date and time used by the service to interpret time values.

  Use only if the service has no clock synchronization mechanism.

Entry	Change Type	Time Scope	Gathering Time
Service	Counter	Point in time	On demand

- **Last response time**

  Specifies processing time for the most recent successful or failed request (in days, hours, minutes, and seconds).

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Dispatcher Service	Gauge	Point in time	On change

- **Number of failed requests**

  Specifies the number of service requests that failed (a fault was returned).

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Dispatcher Service	Counter	Since reset	On change

- **Number of processed requests**

  Specifies the number of processed requests.

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Dispatcher Service	Counter	Since reset	On change

- **Number of successful requests**

  Specifies the number of service requests that succeeded (no fault was returned).

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Dispatcher Service	Counter	Since reset	On change

- **Percentage of failed requests**

  Specifies the percentage of processed requests that failed.

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Dispatcher Service	Gauge	Since reset	On change

- **Percentage of successful requests**

Specifies the percentage of processed requests that succeeded.

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Dispatcher Service	Gauge	Since reset	On change

- **Response time high watermark**

  Specifies the maximum length of time taken to process a successful or failed request (in days, hours, minutes, and seconds).

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Dispatcher Service	Gauge	Since reset	On change

- **Response time low watermark**

  Specifies the minimum length of time taken to process a successful or failed request (in days, hours, minutes, and seconds).

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Dispatcher Service	Gauge	Since reset	On change

- **Seconds per successful request**

  Specifies the average length of time taken to process a successful request (in seconds).

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Dispatcher Service	Gauge	Since reset	On change

- **Service time**

  Specifies the time taken to process all requests (in days, hours, minutes, and seconds).

Entry	Change Time	Time Scope	Gathering Time
System Server/Server group Dispatcher Service	Counter	Since reset	On change

- **Service time failed request**

  Specifies the time taken to process all failed service requests (in days, hours, minutes, and seconds).

Entry	Change Time	Time Scope	Gathering Time
System Server/Server group Dispatcher Service	Counter	Since reset	On change

- **Service time successful requests**

  Specifies the time taken to process all successful service requests (in days, hours, minutes, and seconds).

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Dispatcher Service	Counter	Since reset	On change

- **Successful requests per minute**

  Specifies the average number of successful requests processed in one minute.

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Dispatcher Service	Gauge	Since reset	On change

Process Metrics for Report and Batch Report Service and Metadata Service

The following process metrics are available for report service and batch report service and metadata service:

- **Number of processes**

  Specifies the number of processes currently running.

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Report service and Batch report service Metadata service	Gauge	Point in time	On demand

- **Number of configured processes**

  Specifies the same value that was configured for the following properties of affected services:

  - "Maximum number of processes for the [service_name] during peak period"
  - "Maximum number of processes for the [service_name] during non-peak period" to be a non-default value

  This value cannot be reset.

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Report service and Batch report service Metadata service	Gauge	Point in time	On demand

- **Number of processes high watermark**

  For system, server, and server group, the total of all Number of processes high watermark metrics for all associated resources is specified.

  For services, the maximum number of processes that ran at any one time since the last reset is specified.

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Report service and Batch report service Metadata service	Gauge	Since reset	On change

- **Number of processes low watermark**

  For system, server, and server group, the total of all Number of processes low watermark metrics for all associated resources is specified.

  For services, the minimum number of processes that ran at any one time since the last reset is specified.

Entry	Change Type	Time Scope	Gathering Time
System Server/Server group Report service and Batch report service Metadata service	Gauge	Since reset	On change

Panes on the Status System Page

The System page has three panes, Scorecard, Metrics, and Settings, that you use to evaluate system status.

You can sort some columns by clicking on the title. By default, columns are sorted in ascending order. To sort in ascending order, click once. To sort in descending order, click again. To return to default order, click a third time. You can refresh each pane independently.

Scorecard Pane

The **Scorecard** pane lists entries: system, servers, server groups, dispatchers, and services. For each entry, it shows a metric score and operational status so that you can assess system performance. For more information, see "Assess System Performance" on page 32.

Each metric score is represented by one of the following icons:

- a green circle for good 🟢
- a yellow diamond for average 🔶
- a red square for poor 🟥

You must set metric thresholds before metric scores appear. For more information, see "Setting metric threshold values" on page 33.

If a service is disabled in IBM Cognos Configuration, it is not listed.

The metric score for each entry is based on the performance of individual child entries. The status that is displayed for each entry is the lowest status of the child entries. For example, if all the metrics for a dispatcher are good, but one service on that dispatcher has a poor metric, the metric score shown for the dispatcher is poor.

Status is one of the following:

- **Available** if all components are available
- **Partially available** if at least one component is available and at least one component is unavailable or partially unavailable.
- **Unavailable** if all components are unavailable

The Group actions menu lets you perform functions, such as starting and stopping dispatchers or services "Stopping and starting dispatchers and services" on page 40, unregistering dispatchers "Removing dispatchers from the environment" on page 43, and testing dispatchers "Testing dispatchers" on page 47. Each entry also has an Actions menu associated with it, which you access by clicking the arrow next to the entry.

You use the **Scorecard** pane to navigate to the entry that you want to view. You can select the view that you want from the Change view menu in the upper-left corner. You can click on entries to select them and display the next level of entries. For example, click a server to see associated dispatchers, or click a dispatcher to see associated services.

You can maximize the **Scorecard** pane to see a consolidated view of information that is displayed in the **Scorecard** pane and important metrics from the **Metrics** pane. The consolidated view includes the following information:

- For servers and server groups: metric score, operational status, up time, service time, number of processed requests and percentage of successful requests.
- For dispatchers: metric score, operational status, number of processes, service time, current heap size (bytes), number of processed requests, and percentage of successful requests.
- For services the information depends on the service.

Metrics Pane

The **Metrics** pane shows the metrics for the selected entry. You can expand metric groups to see the individual metric scores and values. You can reset each metric group independently "Resetting metrics" on page 34.

To choose the metrics that you want to display, select one or more check boxes for good, average, poor, or **No metric score** values. By default, all metrics are displayed. Metrics with no metric score include ones that you cannot set thresholds for and ones that you have not yet set metric thresholds for. For the latter, you must display them by clicking the **No metric score** check box before you can set them.

Settings Pane

The **Settings** pane shows settings associated with the selected entry in view only mode. To change the settings, click the set properties button ▤.

For more information on the settings in the **Settings** pane, see Chapter 5, "Server administration," on page 37.

Assess System Performance

To evaluate how IBM Cognos software is performing, you can view metric scores that are based on thresholds that you set. You can also view the operational status of system components.

You must set metric thresholds before metric scores appear. For more information, see "Setting metric threshold values" on page 33. If dispatchers and services are not performing as they should, you can tune server performance "Tuning server performance" on page 56. For more information on logging settings, see Chapter 3, "Setting up logging," on page 13.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.

   The metric score icon for the **System** entry, shows overall system status. The metric score icon for each server shows the status of that server. In the **Metrics** pane, individual metrics are listed.
2. In the **Scorecard** pane, from the change view menu of the current view, click **All servers**, **All server groups**, **All dispatchers**, or **Services**.

   If you choose **All server groups**, display dispatchers that are not grouped by server by clicking **Default server group**.
3. To view the metrics for a displayed item, click the entry.
4. To view the children of a displayed entry, click the entry.

   Tip: You can refresh individual panes by clicking the refresh button in the pane.
5. To view or change the properties of an entry, click the actions menu button next to the entry, and then click **Set properties**.
6. To see the consolidated view, click the maximize button on the **Scorecard** pane.

Tip: To return to the previous view, click the restore button.

Viewing attributes for metric scores

You can view the last time a metric was reset and updated. You can also view the current threshold setting for each metric score for which a threshold is set. For metrics that are collected at regular intervals, you can also view the period of time to which the value applies.

Before you begin

For more information on threshold settings, see "Setting metric threshold values" on page 33.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click the view that you want.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. In the **Metrics** pane, expand ⊞ the metric group that you want to view.
4. In the **Value** column of the **Metrics** pane, pause your pointer over the value for the metric that you want to view.

   The name of the metric is displayed.
5. To view more information about some metrics, click **More**.

Setting metric threshold values

You can set threshold values that are used for some metric scores.

Acceptable threshold values depend on your operating environment. When a threshold is crossed, the state of the metric score changes.

For example, you determine that the maximum acceptable queue length is 50 items. You select **Low values are good**. You set the upper value to 50 and the lower value to 40. If the queue remains below 40 items in length, the metric score is green (good). If the queue length goes above 40 items, the metric score is yellow (average). If the queue length goes above 50 items, the metric score is red (poor).

Or for percentage of successful requests, you select **High values are good**. You set the upper value to 98 and the lower value to 95. If the percentage of successful requests goes below 95 percent, the metric score is red (poor). If the percentage of successful requests is between 95 and 98 percent, the metric score is yellow (average). If the percentage of successful requests remains above 98, the metric score is green (good).

Changes to thresholds are effective immediately.

There are no threshold defaults. You must set thresholds for metric scores to display.

Before you begin

Log entries Chapter 3, "Setting up logging," on page 13 occur in the following circumstances:

- when metric thresholds are violated
- when enumerated metrics, such as operational status, change

Logs are not generated when metric values change but remain in the same range.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click the view that you want.

Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.

3. To change the threshold for a metric, in the **Metrics** pane, click the Edit thresholds button ✎ for the metric.
4. Click the performance pattern that you want: **High values are good**, **Middle values are good**, or **Low values are good**.
5. To specify a threshold value, click in the threshold box and enter the threshold number you want.
6. Click the arrow for the threshold value to specify which range the value itself falls into.

   For example, if your maximum value is 50 and you want values of 50 to fall into the average category rather than the poor category, click the arrow to move the threshold value into the average category.
7. Click **OK.**

Resetting metrics

You can reset a group of metrics at any time.

When you reset a group of metrics, all the metrics in the group are reset. For example, for a server, you can reset the Queue - Report service group of metrics.

Some metrics cannot be reset. For example, JVM metrics cannot be reset because they were recalculated after the last reset.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click the view that you want.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. In the **Metrics** pane, click the reset button ↻ for the group of metrics that you want to reset.

Resetting metrics for the system

You can reset all metrics for the system at the same time.

Some metrics cannot be reset. For example, JVM metrics cannot be reset because they were re-calculated after the last reset.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, click **Actions**, **Reset all metrics of the system**.

Refreshing report service connections

If a PowerCube has been rebuilt, you can update the connection information without affecting current users.

You must first update the connection information to the rebuilt PowerCube, and then refresh the report servers to use the rebuilt PowerCube for new connections.

For more information, see “Deploying updated PowerCubes” on page 138.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.

2. With all servers displayed, click the check box for the servers you want, and from the Group actions menu, click Refresh report service connections.

   Tip: You can also do this from the Actions menu next to System, servers, and dispatchers. You can also click the Configuration tab, and then click Dispatchers and Services, and then click the **Refresh Report Service Connections - Configuration** button.
3. When the **View the results** page appears, ensure that the operation has been successful and then click Close.

Chapter 5. Server administration

Server administration includes managing and maintaining your IBM Cognos system, and tuning the system performance.

You should be familiar with the IBM Cognos components and with how they are installed and configured. If you installed IBM Cognos servers or components on more than one computer, all functionality can be controlled through system administration. For information about the IBM Cognos environment, see the *IBM Cognos Analytics Installation and Configuration Guide*.

For some server administration tasks, you use the administration components and must have the required permissions to the access administration functionality Chapter 13, “Capabilities,” on page 185.

Dispatchers and Services

The dispatcher is the entry point for IBM Cognos service requests sent by a Web server gateway or other software. The dispatcher handles the routing requests and balances the load of user requests to the various IBM Cognos services.

You can have more than one dispatcher in your IBM Cognos environment. In such distributed installations one dispatcher is configured for every instance of the Content Manager or Application Tier Components that are installed and configured in your environment.

After you install and configure IBM Cognos software, one dispatcher is available on each computer by default. Each dispatcher has a set of associated services, listed in the following table.

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 17. 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.
Annotation service	Enables the addition of commentary to reports via the IBM Cognos Workspace. These comments persist across versions of the report.
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.
Content Manager service	• Performs object manipulation functions in the content store, such as add, query, update, delete, move, and copy • Performs content store management functions, such as import and export

Table 17. IBM Cognos services (continued)

Service	**Purpose**
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.
Interactive Discovery Visualization service	Used by Cognos Workspace to provide visualization recommendations.
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	Records log messages generated by the dispatcher and other services. The log service can be configured to record log information in a file, a database, a remote log server, Windows Event Viewer, or a UNIX system log. The log information can then be analyzed by customers or by Cognos Software Services, including: • security events • system and application error information • selected diagnostic information
Metadata service	Provides support for data lineage information displayed in Cognos Viewer, 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 17. IBM Cognos services (continued)

Service	**Purpose**
Mobile service	Manages activities related to IBM Cognos Analytics Mobile Reports client: • Transforms reports and analyses for mobile consumption. • Compresses report and analysis content for fast distribution over-the-air to the mobile devices and access from those devices. • Pushes report and analysis content to the mobile devices. • Facilitates incoming and outgoing report-related and analysis-related requests between the mobile device and the environment to search, browse, or run reports. • Synchronizes the mobile content store on the server with the mobile database on the mobile device. • Translates Simple Object Access Protocol (SOAP) messages into wireless-friendly messages. • Communicates with the mobile device.
Monitor service	• Manages the monitoring and execution of tasks that are scheduled, submitted for execution at a later time, or run as a background task • Assigns a target service to handle a scheduled task. For example, the monitor service may ask the batch report service to run a report, the job service to run a job, or the agent service to run an agent. • Creates history objects within the content manager and manages failover and recovery for executing entries
Planning administration console service	Manages communication with the Contributor Administration Console.
Planning data service	Manages communications for real-time reporting from Contributor plan data.
Planning job service	Manages communications with the Planning Job Server subsystem.
Planning web service	Manages communications with Contributor Web and Contributor Add-in for *Excel* users.
PowerPlay service	Manages requests to run PowerPlay reports.

Table 17. IBM Cognos services (continued)

Service	Purpose
Presentation service	• Transforms generic XML responses from another service into output format, such as HTML or PDF • Provides display, navigation, and administration capabilities
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.
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.
System service	Defines the Bus API-compliant service used to obtain application-wide configuration parameters. It also provides methods that normalize and validate locale strings and map locale strings to locales supported by your application.
Visualization Gallery service	Used to load and retrieve RAVE1 visualizations into the Visualization Gallery in Reporting. It is required by the Report Service.

Stopping and starting dispatchers and services

You can stop and start dispatchers and services manually. If a service stops responding, you must stop and restart it.

Each dispatcher and service can be

- started
- stopped immediately and delete all the requests that are running or queued, without completing those requests
- stopped after running and queued requests are processed

You can stop or start all dispatchers and services in the IBM Cognos environment at once.

When you start IBM Cognos software using the configuration tool, all dispatchers and services start unless they are disabled in the configuration tool. For more information, see the *IBM Cognos Analytics Installation and Configuration Guide*.

By default, all services start when you restart the computer on which they are installed.

Before you begin

Stopping a service also stops all its processes. When you stop a dispatcher, all its services are stopped. If the suspended dispatcher has an active Content Manager, all users except administrators are locked out.

After a service is stopped, it has a suspended status Chapter 4, “System Performance Metrics,” on page 21.

You must have the required permissions to access **IBM Cognos Administration** functionality. See Chapter 13, “Capabilities,” on page 185.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click the dispatchers or services that you want.

   Click **All servers**, **All server groups**, or **All dispatchers**. To select a service, pause your pointer over **Services** and click the required service.
3. Click the Actions menu arrow for the dispatcher or service, and choose the action that you want to perform.

   Depending on the dispatcher or service, you can perform the following actions:

Table 18. Stopping and starting dispatchers and services: goals, views, and actions

Goal	Scorecard pane view	Action
Start all dispatchers in system	**All servers**	From the Group actions menu, click **Start dispatchers**. **Tip:** To apply an action to only some entries, select check boxes for one or more entries and then click the action that you want.
Start all dispatchers for a server group	**All server groups**	From the server group Actions menu, click **Start dispatchers**.
Start all dispatchers for a server	**All servers**	From the server Actions menu, click **Start dispatchers**.
Start a specific dispatcher	**All dispatchers**	From the dispatcher Actions menu, click **Start**.
Start a specific service	**All services**	From the service Actions menu, click **Start**.
Stop all dispatchers in system	**All servers**	From the Group actions menu, click **Stop dispatchers immediately** or **Stop dispatchers after running and queue processed**.
Stop all dispatchers for a server group	**All server groups**	From the server group Actions menu, click **Stop dispatchers immediately** or **Stop dispatchers after running and queue processed**.

Table 18. Stopping and starting dispatchers and services: goals, views, and actions (continued)

Goal	Scorecard pane view	Action
Stop all dispatchers for a server	**All servers**	From the server Actions menu, click **Stop dispatchers immediately** or **Stop dispatchers after running and queue processed**.
Stop a specific dispatcher	**All dispatchers**	From the dispatcher Actions menu, click **Stop immediately** or **Stop after running and queue processed**.
Stop a specific service	**All services**	From the service Actions menu, click **Stop immediately** or **Stop after running and queue processed**.

A dialog box appears and confirms the action.

4. Click **Close**.

Active Content Manager Service

You can manually activate a Content Manager service that is in standby mode.

One Content Manager service is designated to become active at startup. All other Content Manager services start up in standby mode. Only one Content Manager service can be active at any time.When you activate a service, any currently active service switches to standby mode.

You can also specify a Content Manager service which is currently standby as the default active service at startup.

You must have the required permissions to access **IBM Cognos Administration**. See Chapter 13, “Capabilities,” on page 185.

Specifying a default Content Manager service

You can specify a default content manager service.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **Services** > **Content Manager**.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. From the **ContentManagerService Actions** menu, click **Set as active by default**.

   Tip: Only Content Manager services that are not already the default have **Set as active by default** displayed in the Actions menu.

Activate a Content Manager service

You can activate a specific content manager service.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **Services** > **Content Manager**.

Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.

3. From the **ContentManagerService Actions** menu, click **Start**.

Removing dispatchers from the environment

You can remove a dispatcher if you no longer need it in the IBM Cognos environment.

You can stop the IBM Cognos service using IBM Cognos Configuration. This will stop the dispatcher as well. If you delete a dispatcher without stopping the IBM Cognos service first, the dispatcher will automatically be reinstated in 30 seconds.

Before you begin

To remove a dispatcher, you must first stop the dispatcher from the computer where it is installed. After stopping the dispatcher, you must then remove the dispatcher from the content store by unregistering it in IBM Cognos Administration.

You must have the required permissions to access **IBM Cognos Administration** functionality. See Chapter 13, "Capabilities," on page 185.

Procedure

1. Stop the IBM Cognos service using IBM Cognos Configuration.

   This also stops the dispatcher. For information about stopping the IBM Cognos service, see the *IBM Cognos Analytics Installation and Configuration Guide*.
2. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
3. Determine the dispatchers that you want to unregister. You can unregister all dispatchers in the system, unregister all dispatchers for a server, or unregister all dispatchers for a server group.
4. In the **Scorecard** pane, from the change view menu of the current view, click **All servers**, **All server groups**, or **All dispatchers**. The view you choose depends on which dispatchers you want to unregister.

Table 19. Actions required to achieve unregister goals for dispatchers

Goal	Action
Unregister all dispatchers in system	In the **Scorecard**, **All dispatchers** view, click the arrow to view the **Group actions** menu, and then click **Unregister dispatchers**. **Tip:** To apply an action to only some entries, select check boxes for one or more entries and then click the action that you want.
Unregister all dispatchers for a server	In the **Scorecard**, **All servers** view, from a server **Actions** menu, click **Unregister dispatchers**.
Unregister all dispatchers for a server group	In the **Scorecard**, **All server groups** view, from a dispatcher **Actions** menu, click **Unregister dispatchers**.
Unregister a specific dispatcher	In the **Scorecard**, **All dispatchers** view, from a dispatcher **Actions** menu, click **Unregister**.

   A dialog box appears to confirms the action.
5. Click **OK**.

   The dispatcher information is removed from the content store.

Grouping dispatchers in configuration folders

Configuration folders are useful to organize dispatchers if your installation includes many dispatchers. You can group dispatchers so that you can apply the same configuration settings once to all the dispatchers and services in the folder.

Before you begin

You must have the required permissions to access **IBM Cognos Administration** functionality. See Chapter 13, “Capabilities,” on page 185.

About this task

When you add a dispatcher to a configuration folder, it automatically inherits the configuration settings of the folder. However, if you previously changed the default values of that dispatcher or service, the changed values are kept.

When you change the configuration settings of a dispatcher or configuration folder, the services for the dispatcher and any child entries for the folder automatically acquire the new values. However, if you change the values of the services, the changed values are kept.

You can create a new configuration folder at the root of the Configuration area or in an existing configuration folder.

Tip:

- To view and edit the configuration properties of the parent of an entry shown in the path on the toolbar, click the **Set properties - Configuration** button. You can change and apply configuration settings for all the dispatchers and services in the Configuration area when you are in the root of the Configuration area.
- Use the path on the toolbar to explore the different levels of your configuration. The path starts with Configuration and, when the path becomes too long, it wraps.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Dispatchers and Services**.
2. Click the new folder button.
3. Type a name and, if you want, a description, and specify where to save the configuration folder.
4. Click **Finish**.

   You can now add dispatchers to the configuration folder by cutting them from their original location and then pasting them inside the folder. You can also change settings at the configuration folder level.

   Tip: To move a dispatcher to another folder, click **More** next to the dispatcher and then click **Move**.

Dispatcher routing

Depending on how your system is set up, you may want to control how reports are distributed among servers.

For example, you have different departments that maintain their own servers, or you have specific servers set up for specific data access, such as Microsoft Windows servers for Microsoft SQL Server databases and Linux servers set up for IBM Db2 access. You can set up IBM Cognos software so that report requests are processed by specific servers by applying routing rules.

Affinity settings take precedence over advanced routing settings. For more information, see “Maximum Number of Processes and Connections” on page 60.

When you define the routing rules, you must select a server group. Server group names are a property of a dispatcher or the configuration folders into which the dispatchers are organized. For more information to set server group names, see “Creating server groups for advanced dispatcher routing” on page 57.

To determine which server groups process certain reports, you must associate the server groups with routing tags for data objects, such as packages, data modules, or uploaded files, and for user groups or roles. Then, you need to specify how the routing tags are distributed among the dispatchers in your environment. The distribution is controlled by routing rules that you create for the routing tags. The report request will be processed by a specific server depending on the routing tags associated with the data object from which the report was created and/or the user or group running the report.

Tip: A routing tag can by any word or phrase, but as a best practice, specify a tag that is meaningful for your environment. You could have tags such as `Sales reports`, `Db2 data`, `Europe`.

When you create the routing rules, you create conditions that determine the server groups by which the reports are to be processed. For example, you can set up routing rules so that reports from a Finance package that were created by a user in the Finance group are processed by Finance servers. Alternatively, you can set up routing rules so that reports that were created by any Sales users, regardless of which data object was used to create the report, are processed by the Sales servers. In the first example, you would specify routing tags for both the group or role and the package, but in the second example you would only specify a routing tag for the group or role and leave the package routing tag blank. You do not have to specify a routing tag for both the data object and the group or role in your routing rules.

You must have the required permissions to access **IBM Cognos Administration** functionality. For more information, see Chapter 13, “Capabilities,” on page 185.

Setting routing tags for groups or roles

You can set routing tags for groups or roles. The routing tags are used to specify routing rules for dispatchers.

Procedure

1. From **Manage** > **Administration console**, open **IBM Cognos Administration**.
2. On the **Security** tab, click **Users, Groups, and Roles**.
3. Click the **Cognos** namespace to display the groups and roles.
4. Click the set properties button ▤ for a group or role.
5. Under **Advanced routing** > **Routing sets**, click **Set**.

   The **Assign routing sets** page appears.
6. Select a routing tag for the users role or group in **Available routing sets**, or type it in **Type Routing Sets**, and click the add button to add the tag to the **Assigned routing sets** box. When typing multiple tags, separate each tag with a semi-colon. For example, `Sales groups;Marketing;Development`.
7. Repeat step 5 to add other routing keywords that you want to apply to the group or role.

   The order in which the routing tags are added does not matter.
8. Click **OK**.

   The routing tags are displayed under **Advanced routing** in the group or role properties page.
9. On the **Set properties page**, click **OK**.

Results

The routing tags are used when “Setting routing rules for dispatchers” on page 45.

Setting routing rules for dispatchers

You can set routing rules for dispatchers or configuration folders.

Server groups are a property of dispatchers or configuration folders, and must be set up before you can set routing rules for server groups. For more information, see “Creating server groups for advanced dispatcher routing” on page 57.

Procedure

1. From **Manage** > **Administration console**, open **IBM Cognos Administration**.
2. On the **Configuration** tab, click **Dispatchers and Services**.

   The dispatchers and any configuration folders that have been created are shown.

   Tip: Server groups must already be set up. For more information, see "Creating server groups for advanced dispatcher routing" on page 57.
3. In the toolbar, select the specify routing rules button .

   The **Specify the routing rules** page appears.
4. Click **Add a rule**.
5. Specify the routing rules by matching the routing tags with server groups. A routing rule can be a combination of the following tags and server groups:
   - **Data routing tag** and **Server group**
   - **Group routing tag** or **Role routing tag** and **Server group**
   - **Data routing tag** and **Group routing tag** or **Role routing tag** and **Server group**
6. In the **Actions** column, click the View the members button to see an overview of the members.
7. To change the order of routing rules, select **Modify the sequence**. Select the rule that you want to move, and click **Up**, **Down**, **To top**, or **To bottom**.

   Important: Unlike routing tags, the order in which routing rules are listed affects how they are applied.

   A rule is matched when properties associated with the data object or group or role involved in the request satisfy the criteria of the rule. The rules are evaluated in order until the first one is matched, and the request is routed to the server group named by the first rule that was matched.
8. Click **OK**.

Specifying gateway mappings for IBM Cognos Series 7 PowerPlay data

You can specify the location of a Series 7 PowerPlay server.

IBM Cognos for Microsoft Office users may send requests to Report data service (RDS) for data that resides on a Series 7 PowerPlay server. Report data service (running on the IBM Cognos application server) communicates with Series 7 PowerPlay through the Series 7 PowerPlay Enterprise Server gateway.

If the network configuration prohibits application server access to the Web tier server that hosts the Series 7 PowerPlay Enterprise Server gateway, then a second internal Series 7 PowerPlay Enterprise Server gateway must be installed in the application server tier. In this type of configuration, you can specify the location of the Series 7 PowerPlay server.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **Services** > **Report data**.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. From the **reportDataService Actions** menu, click **Set properties**.
4. Click the **Settings** tab.
5. In the **Value** column, click **Edit** for Gateway mappings.
6. Click the check box **Override the settings acquired from the parent entry**.
7. Click **Add a mapping**.
8. For **Application gateway (external)**, type the address of the Web server.
9. For **Application gateway (internal)**, type the address of the Series 7 PowerPlay server.

10. Click **OK**.

Renaming dispatchers

As a security measure, you can rename dispatchers if you do not want to reveal the host computer name, port number, servlet, or path of the dispatcher.

For more information, see “Securing Dispatchers” on page 49

Typically, server administrators can view and change the name of dispatchers.

We recommend that when renaming a dispatcher, you do not use any information that reveals the host computer name or port, or other system or path information. However, it is important to remember where the dispatcher is installed, for monitoring purposes.

Tip: If you rename a dispatcher and need to access the host, port, and path information, you can use the Software Development Kit methods to find this information in the dispatcherPath property of the Dispatcher Object.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **All dispatchers**.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. From a dispatcher **Actions** menu, click **Set properties**.
4. In the **Name** box, type the new name for the dispatcher.

   Use a meaningful name to help you distinguish dispatchers. Do not reveal system information in the name.
5. If you want, add a screen tip and description information.
6. Click **OK**.

Testing dispatchers

To evaluate how IBM Cognos software is performing, you can test the status of dispatchers.

You can also ensure that the dispatchers are responding and view the uptime, which is the time in seconds during which the dispatchers are working without failure.

You can view the status of dispatchers and service and review log messages.

Before you begin

When you test a dispatcher, you also test the services that belong to that dispatcher.

You must have the required permissions to access **IBM Cognos Administration** Chapter 13, “Capabilities,” on page 185.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. Determine the dispatchers that you want to test then follow the instructions in this table. In the **Scorecard** pane, from the change view menu of the current view, click the items you want to display.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.

Table 20. Goals, views, and actions for testing dispatchers

Goal	Scorecard pane view	Action
Test all dispatchers in system	**All servers**	From the Group Actions menu, click **Test**. **Tip:** To apply an action to only some entries, select check boxes for one or more entries and then click the action that you want.
Test all dispatchers for a server group	**All servers**	From the Group Actions menu, click, **Test dispatchers**.
Test all dispatchers for a server	**All servers**	Find the server you want to test. From the server Actions menu, click **Test**.
Test a specific dispatcher	**All dispatchers**	Find the dispatcher that you want to test. From the dispatcher Actions menu, click **Test**.

A dialog box appears and confirms the action.

3. Click **OK**.

   If dispatchers are not performing as they should, you can tune server performance by changing their configuration settings. For more information, see "Tuning server performance" on page 56.

Failover for Multiple Dispatchers

In a distributed IBM Cognos software installation, you can configure each of your gateway components to communicate with more than one dispatcher for failover purposes.

The gateway components scan their associated dispatchers to ensure that requests are routed to dispatchers that are in service and responding correctly. You can set the frequency with which these scans are executed.

For information about configuring multiple dispatcher, see the "Configuring Gateway Computers" topic in the *IBM Cognos Analytics Installation and Configuration Guide*.

Set the Frequency of Dispatcher Status Scans

You can specify how often dispatchers are scanned to determine their current status for failover purposes.

Use the following parameters:

- ConnectionCheckingSleepTime

  Specifies, in seconds, the interval between scans for the state of dispatchers.

  Valid settings are 1 to 2147483647. Settings less than 5 may consume too many resources (CPU time and network bandwidth). The default setting is 30.

- ConnectionCheckingQuickSleepTime

  Specifies, in seconds, the interval between scans when no operational dispatchers are found. This value of this parameter must be less than ConnectionCheckingSleepTime.

  Valid settings are 1 to 2147483647. Settings less than 5 may consume too many resources (CPU time and network bandwidth). The default setting is 5.

Procedure

1. Copy the *install_location*/cgi-bin/cognoscgi.conf.sample file to *install_location*/bin and rename it cognoscgi.conf.
2. Open the cognoscgi.conf file in an editor that can save files in UTF-8 format.
3. Add the following lines to the file:

   ```
   ConnectionCheckingSleepTime=time in seconds
   ```

   ```
   ConnectionCheckingQuickSleepTime=time in seconds
   ```

4. Save the cognoscgi.conf file in UTF-8 format.

Securing Dispatchers

You can change the default dispatcher name to avoid security risks.

Users of IBM Cognos software can enter XPath search paths in the address field of a Web browser or in hyperlinks. The users can input any search path syntax against search path parameters in the user interface. IBM Cognos software relies on the Content Manager Access Control List (ACL) to check the objects that are returned to the user.

In some cases, malicious users could see the dispatcher name. This can pose a security risk, even though the users cannot click the dispatcher name or perform any actions on it.

To avoid this type of security risk, change the default dispatcher name. The default dispatcher name is *computer_name*:9300 and it can be changed to, for example, *server1* to mask the port number and host name. For more information, see “Renaming dispatchers” on page 47

Specifying the dispatchers to host the JMX proxy server

Administrators can create a list of one or more dispatchers as candidates to host the Java Management Extensions (JMX) proxy server. This helps reduce the number of threads required to collect JMX metrics and increases the number of threads that are available for content manager.

The JMX Proxy server communicates with dispatchers and collects their JMX metrics. This communication requires approximately four threads per dispatcher. A distributed install with a large number of dispatchers requires a large volume of threads, which impacts the performance of content manager. To resolve this issue and enhance the performance of content manager, administrators can choose one or more dispatchers as candidates to host the Java Management Extensions (JMX) proxy server.

Choosing dispatchers

Since IBM Cognos Administration uses the presentation service and has a connection to the proxy server, choose dispatchers that are running the presentation service. This provides local calls to the proxy server.

Use IBM Cognos Administration to create a list of one or more dispatchers to host the Java Management Extensions (JMX) proxy server. The dispatcher that is at the top of the list and is currently running is the dispatcher that is chosen to host the JMX proxy service.

If none of the dispatchers in the preferred list are running then any random available dispatcher is chosen to host the JMX proxy server. Note that this is the default behaviour if you do not create a list of dispatchers.

Editing JMX Host Dispatchers

Use IBM Cognos Administration to add one or more dispatchers to the list of dispatcher candidates that can be the host for the Java Management Extensions (JMX) proxy server.

Procedure

1. Launch IBM Cognos Administration.
2. On the **Status** tab, click **System**.
3. In the **Scorecard** pane, for the **System** entry, click the Actions menu arrow, and click **Set properties**.
4. On the **Set Properties - Configuration** page, click the **Settings** tab.
5. Click **Edit** to set the **JMX Proxy host dispatchers**.

   The **Set JMX Proxy host dispatchers configuration** page appears.
6. Click **Add** to add a dispatcher.
7. Select the dispatchers that you want to add.
8. Click the right-arrow button and when the entries you want appear in the **Selected entries** box, click **OK**.
9. Click **OK**.
10. Click **Up**, **Down**, **To top**, or **To bottom** to order the dispatchers.
11. Click **OK**.

Results

The dispatcher that is at the top of the list and is currently running is the dispatcher that is chosen to run the JMX proxy service. You can change the order of the dispatchers at any time. If none of the dispatchers in this list are running, then any random available dispatcher is chosen to host the JMX proxy server.

Content Manager Locations

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

Ensure that the clocks on each computer where Content Manager is installed are synchronized. If they are not, you may experience odd behavior if a failover occurs. For example, there may be a delay before the status of a newly disabled server is updated in IBM Cognos Administration. For more information about Content Manager, see the *IBM Cognos Analytics Installation and Configuration Guide*.

For more information on setting Content Manager parameters, see "Setting advanced Content Manager parameters" on page 50.

You must have the required permissions to access **IBM Cognos Administration** functionality Chapter 13, "Capabilities," on page 185.

Setting advanced Content Manager parameters

You can set advanced Content Manager parameters.

Advanced Content Manager parameters include settings for the database connection pool, sorted entries for non-English locales, synchronization, and browsing of external namespaces.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **Services** > **Content Manager**.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. From the **ContentManagerService Actions** menu, click **Set properties**.

4. Click the **Settings** tab.
5. Click **Edit** next to **Advanced Settings**.
6. Select **Override the settings acquired from the parent entry**.
7. In the **Parameter** column, type the parameter name.

   For example, type `CM.DbConnectPoolCleanUpPeriod`.
8. In the **Value** column, type the associated value for the setting.
9. Continue typing setting names and values as required.
10. Click **OK**.
11. On the **Set properties** page, click **OK**.

Managing Database Connection Pool Settings for Content Manager

Content Manager uses database connections to access the content store. You can change connection pool settings for Content Manager to increase performance.

With pooled connections, Content Manager does not have to create and open connections for new requests. This provides faster response times. However, pooled connections reserve database resources, so idle connections should be closed if they are not needed.

You can manage the number of connections to the content store by limiting the maximum number of connections and by specifying how long connections stay in the pool before they are automatically closed.

The following parameters are available:

- **CM.DbConnectPoolMax**

  Specifies the maximum number of concurrent database connections that the content store allows.

  This parameter applies only to the Content Manager connection pool settings. If you have other services that access the same content store, there may be more concurrent database connections than specified in this parameter.

  The valid settings are -1, or 5 to 2147483647, or the database setting, whichever is less. The default is -1 (unlimited).
- **CM.DbConnectPoolTimeout**

  Specifies in milliseconds the maximum length of time that a thread waits for a connection to be available from the pool.

  The valid settings are -1 to 2147483627. A setting of 0 specifies that threads never wait for a connection if one is not available immediately. The default is -1 (unlimited).
- **CM.DbConnectPoolIdleTime**

  Specifies in milliseconds the minimum length of time that a connection stays idle in the pool. This parameter is used only if the value of the DbConnectPoolCleanUpPeriod setting is positive.

  The valid settings are -1 to 2147483647. A setting of 0 or -1 specifies that idle connections are closed when Content Manager restarts. The default is 300000 (5 min).
- **CM.DbConnectPoolCleanUp Period**

  Specifies in milliseconds the length of time between invocations of a cleanup thread that closes idle connections in the pool that exceed the setting of DbConnectPoolIdleTime.

  The valid settings are -1 to 2147483647. The default is 300000 (5 min).

Sorting Entries for Non-English Locales

You can correct sorting problems in locales other than English for an Oracle or Microsoft SQL content store.

To correct a sorting problem, use the CM.SortCollation parameter. For example, to sort entries in an Oracle database using a Chinese phonetic collation, set CM.SortCollation parameter to SCHINESE_PINYIN_M.

For information about supported collations, see the Oracle and SQL Server documentation. Setting the CM.SortCollation value has no effect on Content Manager running against IBM Db2 or Sybase databases.

Managing Content Manager Synchronization

If your installation includes standby Content Manager computers, you can set parameters that specify Content Manager standby activities.

You can specify how often checks occur to ensure that the active dispatcher has not failed, how long it takes to determine which Content Manager is active when failover occurs and at startup, how often an active Content Manager sends a response when it is busy, and how long a short network interruption can be without causing a failover.

The following parameters are available:

- **CM.CMSync_NegotiationTime**

  Specifies in milliseconds the length of time that it takes to determine the active Content Manager when a failover occurs.

  The valid settings are 1 to 9223372036854775807. The default is 2000.

- **CM.CMSync_NegotiationTimeForStartUp**

  Specifies in milliseconds the length of time that it takes to determine the active Content Manager at startup.

  The valid settings are 1 to 9223372036854775807. The default is 60000.

- **CM.CMSync_CheckActive Time**

  Specifies in milliseconds the length of time that it takes for an active Content Manager to become standby when another Content Manager becomes active.

  The default is 10000.

- **CM.CMSync_PingTimeout**

  Specifies in milliseconds the length of time that it takes for a busy Content Manager to send a response if it is running.

  The valid settings are 1 to 9223372036854775807. The default is 120000.

- **CM.CMSync_ShortNetworkInterruptionTime**

  Specifies in milliseconds the length of time that a short network interruption can occur without causing a failover.

  The valid settings are 1 to 9223372036854775807. The default is 3000.

Control Browsing of External Namespaces

You can control whether users can browse external namespaces.

When the CM.SecurityQueryRequiresRead setting is set to true, the Content Manager prevents browsing of external namespaces when the external namespace policy is updated to deny read permissions to users or groups. This setting controls whether the Content Manager forces a read permission filter for external namespace query results. The default is false.

Setting the cache size limit for the Content Manager cache

You can specify the upper limit of the cache size, as a percentage of the JVM heap size.

The default is 10%. Valid values are 0 to 100. Increasing the cache size can reduce the load on the Content Manager, allowing it to serve more distributed nodes. However, setting this value too high may cause out-of-memory errors in the dispatcher.

Setting the value to 0 (zero) disables the cache system-wide, sending all query requests directly to the Content Manager, which may degrade system performance. However, this is useful for comparing performance with and without the cache.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **Services** > **Content Manager Cache**.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. From the **ContentManagerCacheService Actions** menu, click **Set properties**.
4. Click the **Settings** tab.
5. In the **Value** column, change the number for **Heap limit for the content manager cache service**.
6. Type the setting that you want, and click **OK**.

Reducing the Content Manager load by storing user session files locally

You can change the location where user session files are stored.

When a user runs an interactive report, the report server sends a request to the Content Manager, asking it to store the report output in the session cache for the user. Such report output may be in one of the following formats: PDF, HTML with images, Microsoft Excel speadsheet software, CSV, or XML.

To reduce the processing load on the Content Manager, user session files are stored on the report server local file system. By default, this location is on the report server. You can change the location to a remote computer, such as a shared directory on Microsoft Windows operating system or a common mounted directory on UNIX operating system. For more information, see the topic about changing the location of temporary report output in the *IBM Cognos Analytics Installation and Configuration Guide*.

If you're upgrading, user session files are stored in Content Manager. You will need to change the report server local file system if you want to reduce the Content Manager load.

Storing temporary files might result in increased disk usage. Make sure to allocate sufficient space for the files.

This will not interfere with older versions of applications, such as Software Development Kit, which still send requests to the Content Manager.

The following parameters are available:

- **Temporary objects location**

  Specifies the location of temporary cache files. To store the temporary cache files on the report server, select **ServerFileSystem**. To store the temporary cache files on the Content Manager, select **ContentStore**.

  The default is **ServerFileSystem**.
- **Temporary objects lifetime**

  Specifies in hours the length of time that temporary cache files are kept. If you set this to zero, files are kept until they are manually deleted.

This setting is used only by the dispatcher. The report server deletes temporary cache files when the browser is closed or when the user clicks the back button in the browser. If the report server does not delete the files, the dispatcher uses this setting to delete the files.

The default is 4 hours.

There is also a setting in Cognos Configuration for encrypting temporary files, which is not affected by the **Temporary objects lifetime** or the **Temporary objects location** settings. For more information, see the *IBM Cognos Analytics Installation and Configuration Guide*.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Dispatchers and Services**.
2. Click the **Set Properties - Configuration** button then click **Settings**.
3. From the **Category** menu, click **Tuning**.
4. Change the settings for **Temporary objects location** and **Temporary objects lifetime**, as required.
5. Click **OK**.

Overriding the default locale processing in the prompt cache

You can override the locale processing in the prompt cache for all reports.

This can be done using the RSVP.PROMPTCACHE.LOCALE advanced setting. When this setting is configured, the specified locale is used instead of the locale specified in the report whenever prompt cache data is created, updated, or used. This means that a single prompt cache is used for each report regardless of the report user's locale.

Procedure

1. Follow the steps in the section "Configuring advanced settings for specific services" on page 464.
2. For the **ReportService**, in the **Parameter** column, type **`RSVP.PROMPTCACHE.LOCALE`**.
3. In the **Value** column, type the associated value for the parameter, and click **OK**.

Content store maintenance tasks

You can create content maintenance tasks and run them on demand, at a scheduled time or based on a trigger.

For example, a database refresh or an email. You can schedule content maintenance tasks as part of a job, or as part of an agent. You can also view the run history of content maintenance tasks.

You can find and fix inconsistencies within the content store or between the content store and external namespaces.

Content maintenance tasks can check for inconsistencies within the content store due to missing data or obsolete data or between the content store and external namespaces.

If necessary, you can also start and stop background tasks that are running in the content store.

For information about using content store maintenance tasks in a multitenant environment, see "Creating and running a content store consistency check " on page 319.

Before You Start Internal Content Store Maintenance

To ensure that you do not lose any data that you wanted to keep, you should choose the find mode first and check the results before fixing the content store.

Missing data within the content store may cause updates to fail. Obsolete data may prevent you from creating new objects. When a content store maintenance task fixes the content store, it adds default values for the missing data, which you can update later. It also permanently deletes any obsolete data.

When you find and fix the data, the content store is not fixed while the content maintenance task is running. Instead, Content Manager fixes the inconsistencies in the content store the next time it starts up.

Important: After you run a content maintenance task to find and fix the content store, back up your content store before you restart Content Manager.

We recommend that you perform internal maintenance checks regularly, but it is particularly important to do so before you upgrade, to ensure the consistency of the content stores.

Content Store Maintenance on External Namespaces

You can use IBM Cognos Administration for content store maintenance on external namespaces.

When you delete users in your authentication provider, the user account information remains in the content store. You can use the IBM Cognos Administration to find user information that still exists in the content store and fix the content store by deleting any users that do not exist in your external namespaces. You can also delete individual user profiles from the content stores.

If you want to run a content maintenance task on more than one namespace, do one of the following:

- If you want to run the content maintenance task now, simply log on to the namespaces and create the content maintenance task.
- If you want to schedule a content maintenance task to run in the future or on a recurring basis, keep in mind that a scheduled content maintenance task runs against the namespaces that you select when you create the content maintenance task. Before you schedule a content maintenance task, ensure that your credentials contain logon information for each namespace by renewing the credentials after you log on to every namespace that you select to run the content maintenance task against.

  Tip: Click **My Area Options**, **My Preferences**, click the **Personal** tab, and then click **Renew the credentials**.

You must have access permissions for each selected external namespace and read permissions for all user accounts in each external namespace. If you do not have read permissions for a user account, it is assumed that the user was deleted from the namespace. When you run a content maintenance job, the user information in the content store is either listed as inconsistent (for **Find only** or automatically deleted (for **Find and fix**).

You must have the required permissions to access **IBM Cognos Administration**. For more inforamtion, see Chapter 13, “Capabilities,” on page 185.

Creating a content store maintenance task

You can create a content store maintenance task.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Content Administration**.
2. Click the arrow on the new content maintenance button on the toolbar, and then click **New Consistency Check**.
3. Type a name and, if you want, a description and screen tip, and click **Next**.
4. Choose the consistency check that you want:
   - To check the content store for inconsistencies, click **Internal references**.
   - To run content maintenance on namespaces, click **References to external namespaces** and select the namespaces that you want.
5. Click **Next**.
6. Choose the action that you want:
   - To run the task now or later, click **Save and run once** and click **Finish**. Specify a time and date for the run. Click **Find only** or **Find and fix**, and then click **Run**. Review the run time and click **OK**.

- To schedule the task at a recurring time, click **Save and schedule** and click **Finish**. Then, select frequency and start and end dates. Click **Find only** or **Find and fix** and click **OK**.

  Tip: To temporarily disable the schedule, select the **Disable the schedule** check box. To view the schedule status, see "Managing scheduled activities" on page 259.

- To save the task without scheduling or running, click **Save only** and click **Finish**.

Run a Content Store Maintenance Task

You can run a content store maintenance task.

Procedure

1. On the **Configuration** tab, click **Content Administration**.
2. Click **Run with options** next to the content maintenance task.
3. Select the **Now** check box to run the content maintenance task immediately or the **Later** check box to set a day and time.
4. Click **Find** or **Find and fix**.
5. Click **Run**.

Starting and stopping background activities

You can start and stop background activities that are running on Content Manager.

About this task

Stopping background activities decreases the processing load on Content Manager, allowing performance to increase. You can start background activities after Content Manager completes the job that required a higher volume of resources.

Procedure

1. Launch IBM Cognos Administration.
2. On the **Status** tab, click **System**.
3. In the **Scorecard** pane, from the change view menu of the current view, click **Services** > **Content Manager**.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
4. Click the arrow to view the Actions menu next to the Content Manager service, and then click **Start background activities** or **Stop background activities**.

Tuning server performance

You should include performance tuning as a regular part of administering servers.

By tuning the configuration settings of dispatchers and services, you can optimize the speed and efficiency of IBM Cognos software. For users, optimal performance means that their reports run fast and without errors. For you, it means that IBM Cognos software is stable and that the users are happy.

Ideally, you want to tune the servers to meet the user demand at the peak usage times.

You may need to add dispatchers to your installation to meet the demands of users. Or, you may need to distribute your installation or upgrade the computer on which IBM Cognos software is installed. For more information, see the *IBM Cognos Analytics Installation and Configuration Guide*.

The level of logging "Setting logging levels" on page 16 can affect performance. When IBM Cognos software logs more detail, more resources are allocated to logging and fewer resources are then available to run reports.

Before you change any settings, ensure that you tested the dispatchers, and reviewed the pertinent log messages "Log messages" on page 13. For more information on testing dispatchers, see "Testing dispatchers" on page 47. You should also understand your performance requirements.

Models

Ensure that your models are optimized for reporting. For more information, see the *IBM Cognos Framework Manager User Guide*.

Operating systems

How IBM Cognos software performs is tightly related to the performance of the operating system of the computer where IBM Cognos software is installed. Therefore, ensure that your operating system is tuned.

Creating server groups for advanced dispatcher routing

If you intend to define routing rules for reports, you must create server groups for the dispatchers or configuration folders to which you want reports to be routed.

For information about defining routing rules, see "Dispatcher routing" on page 44.

Tip: If you are setting up advanced dispatcher routing and are using PowerPlay, you must ensure that the server group includes at least one PowerPlay server to handle PowerPlay requests.

About this task

You can

Procedure

1. From **Manage** > **Administration console**, open **IBM Cognos Administration**.
2. On the **Status** tab, click **System**.
3. In the **Scorecard** pane, from the change view menu of the current view, click **All dispatchers**.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
4. From the **Actions** menu of the dispatcher, click **Set properties**.
5. Click the **Settings** tab.
6. Select **Tuning** from the **Category** list.
7. Type a name in the **Value** column for the **Server Group** property.

   Important: The name can contain a maximum of 40 characters.
8. Click **OK**.

   You use this server group when you define routing rules, as documented in the topic *Setting routing rules for dispatchers*in the topic ../com.ibm.swg.ba.cognos.ag_manage.doc/t_set_routing_rules.html.

Balancing requests among dispatchers

If your installation includes more than one dispatcher, you can specify the proportion of requests that each dispatcher handles by changing their processing capacity.

This is commonly referred to as load balancing. You typically set the capacity for a dispatcher based on the CPU speed of the computer where it is installed.

For example, a first dispatcher is installed on a 2 GHz computer and a second dispatcher on a 1 GHz computer. You set the processing capacity of the first dispatcher to 2.0 and the second to 1.0. The first dispatcher handles two-thirds of the requests while the second handles one-third of the requests. If you set the capacity of both dispatchers to 1.0, requests are sent to each dispatcher alternately.

The default processing capacity for each dispatcher is 1.0.

Affinity settings take precedence over balance request settings. For more information, see “Maximum Number of Processes and Connections” on page 60.

You can also control dispatcher load balancing by setting the in-progress request factor. See “Balance Dispatcher Load with In-Progress Request Factor” on page 58. You can also turn off the weighted round robin format of load balancing for the dispatcher. See “Setting the dispatcher load balancing property to cluster compatible mode ” on page 59.

Before you begin

You must have the required permissions to access **IBM Cognos Administration** functionality. See Chapter 13, “Capabilities,” on page 185.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. Click the arrow for the Actions menu next to **System** and click **Set properties**.
3. Click the **Settings** tab.
4. Select **Tuning** from the **Category** list.
5. In the **Value** column, type a new value for the **Processing capacity**, and then click **OK**.

   The new value takes effect immediately.

Balance Dispatcher Load with In-Progress Request Factor

You can set the in-progress request factor to provide feedback to the round robin algorithm, telling it how well each dispatcher is doing.

The weighted round robin format of load balancing treats all requests as equal, and all dispatchers as equally capable of handling the number of requests that they receive. However, different requests require more or less processing power. Dispatchers also run on different servers, with different processing capabilities. For example, if a dispatcher falls behind because it is running on a slower server or because it is getting a lot of requests that require a lot of processing power, the round robin format still treats all dispatchers the same. Dispatchers that start to fall behind have a higher number of in-progress requests in their queue. The round robin algorithm can use this information to avoid sending new requests to those dispatchers until they're no longer overloaded.

The inProgressRequestFactor advanced setting controls how much feedback is sent to the round robin algorithm. The larger the value, the less likely it is that a node with more in-progress requests will be used. Our research shows that the ideal amount of feedback is the default value of 2.0. To use a simple round robin format, set it to 0.0 at a system level.

You can set the value at the system level or at the service level. The system level setting is used as the default for all services. The service settings take precedence over the system level setting.

You can also control dispatcher load balancing by setting capacity processing. See “Balancing requests among dispatchers” on page 57. You can also turn off the weighted round robin format of load balancing for the dispatcher. See “Setting the dispatcher load balancing property to cluster compatible mode ” on page 59. You must have the required permissions to access **IBM Cognos Administration** functionality. See Chapter 13, “Capabilities,” on page 185.

Setting the In-Progress Request Factor property system-wide

You can specify the in-progress request factor property for all services.

Procedure

1. Follow the steps in the section “Configuring advanced settings globally” on page 463.
2. In the **Parameter** column, type **`DISP.default.inProgressRequestFactor`**.

3. In the **Value** column, type the value that will be used as a default for all services. For information about the values that can be specified, see “Balance Dispatcher Load with In-Progress Request Factor” on page 58.
4. Click **OK**.

   The new value is applied immediately.

Set the In-Progress Request Factor property for a specific service

You can specify the in-progress request factor property for a specific service.

Procedure

1. Follow the steps in the section “Configuring advanced settings for specific services” on page 464.
2. For the service that you want to configure, in the **Parameter** column, type **`DISP.service_name.inProgressRequestFactor`**, where *service_name* is the name of the service.

   For example, for the report service, type **`DISP.reportService.inProgressRequestFactor`**.
3. In the **Value** column, type the associated value that will be used as a default for the service. For information about the values that can be specified, see “Balance Dispatcher Load with In-Progress Request Factor” on page 58.
4. Click **OK**.

   The new value is applied immediately.

Setting the dispatcher load balancing property to cluster compatible mode

If your IBM Cognos servers operate within a load balancing infrastructure, you can turn off the weighted round robin format of load balancing for the dispatcher.

If you don't set this parameter, load balancing may be duplicated by the cluster and by IBM Cognos software, which can degrade performance.

You can set the dispatcher property named loadBalancingMode either to weightedRoundRobin or clusterCompatible.

In weightedRoundRobin mode, the dispatcher sprays requests in a weighted round fashion, according to the configuration settings for the dispatcher. For more information, see “Balancing requests among dispatchers” on page 57. This is the default mode.

In clusterCompatible mode, non-affinity requests are processed locally if possible. If there is no service on the local dispatcher, the request fails. This ensures that IBM Cognos software respects any load balancing performed by your own load balancing infrastructure.

You can set the loadBalancingMode property for single dispatchers or for a group of dispatchers in a configuration folder. For more information, see “Grouping dispatchers in configuration folders” on page 44. Because it is an inherited property, you can move dispatchers to a configuration folder and set the loadBalancingMode property for the folder to quickly set the property for a group of dispatchers.

You can also control dispatcher load balancing by setting the in-progress request factor, see “Balance Dispatcher Load with In-Progress Request Factor” on page 58, or by setting capacity processing, see “Balancing requests among dispatchers” on page 57 .

Before you begin

You must have the required permissions to access **IBM Cognos Administration** functionality. See Chapter 13, “Capabilities,” on page 185.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.

2. Click the arrow for the Actions menu next to **System** and click **Set properties**.

   Tip: You can also change the load balancing setting at the dispatcher level.
3. Click the **Settings** tab.
4. Select **Tuning** from the **Category** list.
5. In the **Value** column, select the value for the **Load Balancing Mode**, either Weighted Round Robin or Cluster Compatible, and then click **OK**.

   The new value takes effect immediately.

Setting usage peak periods

You can specify the start and end hours of the peak demand period for your organization.

Most organizations have a period of peak demand. This period is usually during business hours when employees are at work and run interactive reports.

During the peak period, you may want to set the number of connections and processes low enough so that jobs can run faster and system resources can process interactive requests from users. For more information, see “Maximum Number of Processes and Connections” on page 60. During the non-peak period, you can set the number of connections and processes higher because demands on the system are lower.

The default peak period is from 07:00 to 18:00. The default number of connections for each service during the peak period and during the non-peak period is four.

Before you begin

You must have the required permissions to access **IBM Cognos Administration** functionality. See Chapter 13, “Capabilities,” on page 185.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **All dispatchers**.

   Tip: In the **Scorecard** pane, the current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. From the **Actions** menu of the dispatcher, click **Set properties**.
4. Click the **Settings** tab.
5. Select **Tuning** from the **Category** list.
6. In the **Value** column, type new values for the following settings:

   - **Peak period start hour**
   - **Non Peak period start hour**

   Tip: If you want to reset a configuration setting to its default value, select its check box and click **Reset to default value**.
7. Click **OK**.

Maximum Number of Processes and Connections

You can set the maximum number of processes and connections.

For the report service and the batch report service, you can set the maximum number of processes and the maximum number of high affinity and low affinity connections that the dispatcher can open to handle requests. For the agent, Content Manager, delivery, job, and report data services, you can set the maximum number of connections.

There are separate settings for peak and non-peak hours. For more information, see “Setting usage peak periods” on page 60.

Maximum Number of Connections

There is a maximum of one of each of these services per dispatcher: agent, Content Manager, delivery, job, report data. Connections handle one request from one service at a time.

You can specify the maximum number of connections for each service during peak periods and non-peak periods using the following settings:

- **Maximum connections for** *<service_name>* **service during non-peak period**
- **Maximum connections for** *<service_name>* **service during peak period**

The default number of connections is four.

Maximum Number of Processes

There can be multiple report service and batch report service processes on each dispatcher. You can specify the maximum number of processes during peak periods using the following settings:

- **Maximum number of processes for the** *<service_name>* **during peak period**
- **Maximum number of processes for the** *<service_name>* **during non-peak period**

The default number of processes for each service is two.

Affinity Connections

Report servers accept low and high affinity connections to process requests from the batch report and report services.

Low affinity requests can be handled by any report server. Typically, low affinity requests are used when a report run is initially requested.

High affinity requests are ideally handled by a specific report server. Typically, high affinity requests are for reports that were already requested and may include actions, such as going to the next page in a report. If the specific report server is not available or busy, then the report is rerun (low affinity request) on any report server and the next page (high affinity request) is directed to that server.

Affinity settings take precedence over balance request settings and advanced routing settings. For more information, see “Balancing requests among dispatchers” on page 57 and “Dispatcher routing” on page 44.

If affinity settings are changed for a service while entries are running, the number of server processes could double. The number of processes may temporarily exceed the maximum setting while the change takes effect. This may cause problems if your system does not have enough memory for the interim period.

You can specify the number of low and high affinity connections for the report service and the batch report service using the following setting:

Number of <low | high> affinity connections for the *<service_name>* **during non-peak period**

Note: Although the wording of this setting implies that it applies to non-peak periods only, it applies to both non-peak periods and peak periods.

For batch report service, the default number of low affinity connections is two. For the report service, the default number of low affinity connections is four. The default number of high affinity connections for all services is one.

Setting the maximum number of processes and connections

You can set the maximum number of processes and connections.

Before you begin

You must have the required permissions to access **IBM Cognos Administration** functionality. See Chapter 13, "Capabilities," on page 185.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **Services** and then click the service you want.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. From the **Actions** menu of the service, click **Set properties**.

   Tip: For report service and batch report service, you can also set some settings at the system or dispatcher level.
4. Click the **Settings** tab.
5. Select **Tuning** from the **Category** list.
6. In the **Value** column, type new values for the processes and connections that you want to change.

   Tip: If you want to reset a configuration setting to its default value, select its check box and click **Reset to parent value**.
7. Click **OK**.

Specify Queue Time Limits

You can specify the maximum number of seconds that interactive requests made by users wait in the queue for an available report service connection.

If a request cannot be processed within the time limit, the request fails and users receive an error message. If your operating system has adequate resources and IBM Cognos software is properly configured, requests should not take longer than the time limit.

When you specify a time limit, consider the maximum number of seconds that you want users to wait for a response. The default queue time limit is 240 seconds.

Requests for the batch report service stay in the queue indefinitely.

If you have a high user load (over 165 users) and interactive reports are running continuously in a distributed installation, increase the queue time limit to 360 to avoid getting error messages. You may also want to increase the asynchronous timeout setting to avoid getting error messages. For more information, see the *IBM Cognos Analytics Installation and Configuration Guide*.

Before you begin

You must have the required permissions to access **IBM Cognos Administration** functionality. See Chapter 13, "Capabilities," on page 185.

Procedure

1. On the **Status** tab, click **System**.
2. Click the arrow for the Actions menu next to **System** and click **Set properties**.

   Tip: You can also change the queue time limit settings at the dispatcher or service level.
3. Click the **Settings** tab.
4. Select **Tuning** from the **Category** list.
5. In the **Value** column, type a new value for the **Queue time limit of report service (seconds)**setting.

   Tip: If you want to reset a configuration setting to its default value, select its check box, and click **Reset to default value**.

6. Click **OK**.

PDF File Settings

There are four settings for PDF files that together determine the speed at which PDF files are created and the size of PDF files.

The ideal settings are different for different environments. For example, if you create PDF files as part of batch jobs overnight, you may not care about speed. You may choose settings that create small files that can be easily distributed but take longer to generate. If you create ad hoc PDF files or complex PDF files with many charts and graphics, you may care more about speed than file size.

You can use different PDF file settings for report service and for batch report service.

PDF Character Encoding

PDF character encoding determines the character set that is used to create PDF files. You can choose to use Windows1252 encoding, the standard Microsoft Windows operating system single-byte encoding for Latin text in Western writing systems, or unicode (UTF-16) encoding. By default, PDF character encoding is determined automatically, based on the characters found in the file.

The settings names are:

- **PDF Character Encoding for report service**
- **PDF Character Encoding for batch report service**.

Value	Purpose
Windows1252	If you know your files contain only Windows1252 characters, use this setting for faster PDF file creation. Any unicode (UTF-16) character without a Windows1252 equivalent is converted to an indeterminate Windows1252 character.
Font	If you know your files contain non-Windows1252 characters (for example, Chinese characters), use this setting for faster PDF generation than with the Auto setting. PDF built-in fonts are all Windows1252 character encoded. Almost all other fonts use the UTF-16 character set. This setting typically creates larger PDF files than the Windows1252 setting. It is possible for UTF-16 encoded files to gain better compression (see "Content Compression Type" on page 65.
Auto	Use this setting to automatically determine if Windows1252 or UTF-16 should be used to encode the text in the document. If large bodies of text must be analyzed, this is the slowest of the three settings. If speed is a concern you may choose to try the other values with various reports to determine the best setting for your environment. This is the default.

Font Embedding

To ensure that the fonts that are used in a report are available to all readers, fonts can be embedded in PDF files. In IBM Cognos Configuration, there are two font embedding lists, one for the report service and one for the batch report service.

Fonts can be specified as always embedded or never embedded. For example, fonts that you do not have a legal right to redistribute may be specified as never embedded. Fonts that are not available at your remote sales offices but are required to read PDF reports may be specified as always embedded.

For more information about the font embedding lists, see the *IBM Cognos Analytics Installation and Configuration Guide*.

In **IBM Cognos Administration**, you can allow or disallow font embedding in report service and batch report service PDF files. You can also choose automatic font embedding. Keep in mind that files with embedded fonts are larger and take more time to generate. Embedding fonts can cause a strain on network resources. Fewer embedded fonts can reduce network resource consumption.

The license for some fonts prohibits embedding. Ensure that you have permission from the vendor to embed licensed fonts.

The settings names are:

- **Option to allow the report service to embed fonts in generated PDF documents**
- **Option to allow the batch report service to embed fonts in generated PDF documents**.

There are specialized fonts, such as bar-code fonts, that are always embedded when used. These settings do not control embedding of specialized fonts. PDF built-in fonts are never embedded.

Value	Purpose
Allow	If you know that your audience does not have all the fonts they need to view PDF reports, use this setting. Files are larger and PDF output is generated more slowly. Fonts that are in the never embed list in IBM Cognos Configuration are prevented from being embedded. This is the default.
Disallow	If you know that your audience has all the fonts they need to view PDF reports, use this setting. Files are smaller and are generated faster. Fonts are not embedded unless they're in the always embed list in IBM Cognos Configuration.
Auto	Automatically determines which fonts to embed. This setting takes the longest time to generate PDF reports. If the data contains only Windows1252 characters, both the always embed and the never embed list in IBM Cognos Configuration are used. If there is a conflict, the never embed list is used. Except for specialized fonts, unlisted fonts are usually embedded only if UTF-16 characters from that font are used in the file.

Content Compression Type

You can set the compression type to use when PDF reports are created. It takes longer to create PDF output for files with a higher compression type but the resulting files are smaller.

The content compression type specifies which data is compressed. The "Specifying PDF file settings" on page 65 specifies how much the data is compressed. The combination of the two settings determines the final file size.

The settings names are:

- **The PDF compression type for PDF documents created by the report service**
- **The PDF compression type for PDF documents created by the batch report service**.

The choices for this setting, from lowest to highest compression type, are: **Classic**, **Basic**, **Improved**, **Advanced**, and **Full**. **Classic** is the default.

Compression type refers to the amount of data that is compressed within a PDF report. Typically, less compression means faster compression and a larger document. Versions of the Adobe PDF Acrobat Reader earlier than version 6.0 do not support compression types higher than Classic.

There are rare cases where compression causes small files to become slightly larger.

Compression Algorithm Level

The content compression type specifies which data is compressed. The "Content Compression Type" on page 65 specifies how much the data is compressed. The combination of the two settings determines the final file size.

The settings names are:

- **Content Compression level for PDF documents created by the report service**
- **Content Compression level for PDF documents created by the batch report service**

Valid choices for compression algorithm level are 0 (no compression) to 9 (maximum compression). The default is 9.

Specifying PDF file settings

You can specify PDF file settings.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **Services** and click the service that you want.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. From the **Actions** menu of the service, click **Set properties**.
4. Click the **Settings** tab.
5. Select **Tuning** from the **Category** list.
6. In the **Value** column, type the value that you want for each of the PDF file settings.

   Tip: If you want to reset a configuration setting to its default value, select its check box and click **Reset to default value**.
7. Click **OK**.

Setting the maximum execution time

You can set the maximum execution time for the report service and the batch report service.

For example, you may want to limit execution time if you know that there is something wrong because tasks are taking longer. You may also want to ensure that no one task monopolizes server time to the detriment of others.

If the time limit is exceeded, the execution is canceled. The default is zero, which specifies no limit on execution time.

This setting has priority over the governor limit setting. For more information, see “Set the Report Size Limit for the Report Data Service” on page 67.

Before you begin

You must have the required permissions to access **IBM Cognos Administration** functionality. See Chapter 13, “Capabilities,” on page 185.

About this task

This setting can be changed at the system, dispatcher, or service level.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **Services** and then click service you want.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. From the **Actions** menu for the service, click **Set properties**.
4. Click the **Settings** tab.
5. Select **Tuning** from the **Category** list.
6. In the **Value** column, type a new value for the **Maximum execution time for the** *service_name* **(seconds)** setting.
7. Click **OK**.

Specify How Long to Keep Watch List Report Output

You can keep watch list report output for a specific number of runs or for a specific number of days or months.

For example, you can keep up to 10 versions or you can keep the report output versions for 2 days or 6 months.

There are two settings:

- If you want to specify the maximum length of time to keep watch list report output, use the **Periodical document version retention age** setting. The default is 1 day. In the **Settings** pane, this appears as 1 Day(s).
- If you want to specify the maximum number of copies to keep, use the **Periodical document version retention count** setting. There is no default.

If you specify both settings, whichever is reached first determines how many versions are kept.

The settings that you choose depend on how often watch list report output is generated and your system resources. For example, if a report runs nightly to provide output during the day on demand via the portal and watch lists are updated on a weekly basis, you may only want to keep four version each month, but no more than 5 versions during that time. If a job is used to run reports and watch lists are updated only when the job is run, you may only want to keep 1 version each day.

Before you begin

You must have the required permissions to access **IBM Cognos Administration** functionality. See Chapter 13, “Capabilities,” on page 185.

Procedure

1. On the **Status** tab, click **System**.
2. Click the arrow for the Actions menu next to **System** and click **Set properties**.
3. Click the **Settings** tab.
4. Select **Tuning** from the **Category** list.
5. In the **Value** column, type a new value for the **Periodical document version retention age** setting and select **Day(s)** or **Month(s)** from the drop-down menu.
6. In the **Value** column, type a new value for the **Periodical document version retention count** setting.
7. Click **OK**.

Limit Hotspots That are Generated in an Analysis Studio or Reporting Chart

To improve performance, you can limit the number of hotspots that are generated for Analysis Studio and Reporting charts.

A hotspot in a chart appears when you pause a pointer over it. For example, a hotspot on a drill-down symbol or a tooltip gives details about the column, line, or pie slice. The browser response time increases with the number of hotspots. When charts with many members are generated, the hotspots can become an additional burden for the system resources, which can freeze the browser.

When you limit the number of hotspots, priority is given to items such as axis labels and legend labels before individual graphical elements such as bars, pie slices, and so on. Depending on the number of items in a chart and the setting for maximum number of hotspots, some axis items may have hotspots while other axis items and all graphical elements do not, or all axis items and some graphical elements may have hotspots while other graphical elements do not.

The maximum hotspot setting in Reporting overrides this setting. For more information, see the *IBM Cognos Analytics - Reporting User Guide*.

The default is an unlimited number of hotspots.

Procedure

1. On the **Status** tab, click **System**.
2. Click the arrow for the Actions menu next to **System** and click **Set properties**.

   Tip: You can also change the hotspot setting at the dispatcher or service level.
3. Click the **Settings** tab.
4. Select **Tuning** from the **Category** list.
5. Locate the **Number of hotspots generated in a chart by the Batch report service** or the **Number of hotspots generated in a chart by the Report service** setting. In the **Value** column, click the arrow next to **Unlimited** and then click **<Number>**. Type a new value for the maximum number of hotspots
6. Click **OK**.

Set the Report Size Limit for the Report Data Service

You can increase the size limit for report data.

To limit the resources, such as memory, that are used by Report data service, IBM Cognos software restricts the size of the report data that can be sent out. If you receive errors in IBM Cognos for Microsoft Office that a report result is too large, you can increase the size limit for report data by changing the Governor limit setting.

The maximum execution time setting has priority over this setting. For more information, see "Setting the maximum execution time" on page 66.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **Services** > **Report Data**.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. From the **ReportDataService Actions** menu, click **Set properties**.
4. Click the **Settings** tab.
5. In the **Value** column, change the number for **Governor limit (MB)**.
6. Click **OK**.

Excluding the context ID for an agent from IBM WebSphere web service tasks

By default, when the agent service interacts with a web service, the context ID of the agent is included.

If you are running an agent that includes a web service task in IBM WebSphere®, you should exclude this context ID to avoid a conflict with WebSphere's own context IDs.

Procedure

1. Follow the steps in the section "Configuring advanced settings for specific services" on page 464.
2. For the **AgentService**, in the **Parameter** column, type **asv.webservice.useRunContext**.

   You must specify this setting on every **AgentService** instance that you are running.
3. Type **true** as a value for this parameter, and click **OK**.
4. Restart IBM Cognos services.

Tune cache for the repository service

You can tune the cache for the repository service. There are various sizing properties that can be set for local memory and disk resources. Settings can be unique on each dispatcher.

The following table provides a description of the types of cache that can be tuned for the repository service.

Table 21. Types of cache available on the repository service

Parameter	Description
Maximum number of seconds reports and report elements can exist in the cache	The maximum number of seconds that a report can exist in the cache, regardless of how often it is used. After a report expires, it is retrieved from the repository instead of the cache. The default value is 1200 seconds (20 minutes). A value of 0 means that the report is not saved in the cache.
Maximum number of reports and report elements that can overflow to disk	The maximum number of cache entries in to be kept in local memory. The default value is 1000 entries. A value of 0 means that there is no limit to the number of items held in local memory.

Table 21. Types of cache available on the repository service (continued)

Parameter	Description
Maximum number of reports and report elements that can be stored in memory	The maximum number of cache entries that can be written on the local disk. When the memory cache reaches the limit the items overflow to the local disk. The default value is 100 reports and report elements. A setting of 0 means that there is no limit to the number of items written to disk. The entries are written to the data files location defined in IBM Cognos Configuration.

The repository service uses the advanced setting **`repository.maxCacheDocSize`** to specify, in megabytes, the maximum size of each report output that can be stored in the cache. Outputs that are larger than the specified size are not cached and must always be retrieved from the repository or Content Manager. The default value is 10. You can specify this advanced setting individually for a specific repository service or a dispatcher, or globally for the whole IBM Cognos environment. For more information, see Appendix G, "Advanced settings configuration," on page 463.

Bulk cleanup of NC tables

Use the bulk cleanup process to remove finished tasks from NC tables in the content store.

Batch processing is supported for various tasks and objects. A common example can be a scheduled job that contains report executions. The monitor service stores the job and report execution commands in a task queue in NC tables. Under ideal circumstances, the finished tasks are removed one-by-one by a background thread. However, on busy servers or when the scheduled execution rate exceeds the system capacity there might not be enough time to remove the finished tasks this way. The tasks queue keeps growing and might cause server performance issues. The problem manifests itself as a long list of pending report executions when you view current activities in the administration component.

The following NC tables are affected:

- NC_TASK_ANCESTOR_STOREIDS
- NC_TASK_HISTORY_DETAIL
- NC_TASK_QUEUE
- NC_TSE_STATE_MAP
- NC_TASK_PROPERTY

The bulk cleanup process uses a database-specific `BulkFinishedTaskCleanerThread` script. This script is initiated by the monitor service during IBM Cognos service startup. When enabled, the script first checks if there is a certain (configurable) number of completed tasks in the NC tables. If such tasks are found, they are moved to a temporary table, and the NC tables are cleared all in one transaction. No table needs to be dropped or re-created from NC schema. You do not need to stop the IBM Cognos services either.

The cleanup process is enabled and configured by using the following monitor service advanced settings:

- `event.finished.check.active`
- `event.finished.check.interval`
- `event.finished.check.threshold`

For more information about these settings, see the topic "Monitor service advanced settings" on page 484.

For information about configuring advanced settings, see Appendix G, "Advanced settings configuration," on page 463.

Important: Ensure that you always have a valid and current backup of the content store.

Concurrent Query Execution

Depending on your environment, you may be able to improve report run performance by enabling concurrent query execution.

By default, IBM Cognos software executes queries in a report sequentially. You can do this by setting advanced server properties for the report service, the batch report service, or both. When concurrent query execution is enabled, the report server determines which queries in the report can be run concurrently.

The report author must specify the queries in a report that are candidates for concurrent execution. For more information, see the *IBM Cognos Analytics - Reporting User Guide*.

RSVP.CONCURRENTQUERY.NUMHELPERSPERPROCESS

Use this parameter to enable concurrent query execution and set the maximum number of query execution helpers for each report service or batch report service process.

The default value is 0, meaning that the concurrent query execution disabled.

Each query execution helper results in an additional data source connection. For example, a report service has four processes with two high affinity connections and two low affinity connections:

- If the maximum number of query execution helpers is set to 0 (disabled), the maximum number of data source connections created by the report service is 16 (two low affinity connections plus two high affinity connections plus zero query execution helpers times four processes).
- If the maximum number of query execution helpers is set to 2, the maximum number of data source connections created by the report service is 24 (two low affinity connections plus two high affinity connections plus two query execution helpers times four processes).

RSVP.CONCURRENTQUERY.MAXNUMHELPERSPERREPORT

Use this parameter to specify the maximum number of query execution helpers for each report. This parameter is used to prevent a single report from consuming all available query execution helpers.

For example, a report has eight queries that can run concurrently:

- If RSVP.CONCURRENTQUERY.NUMHELPERSPERPROCESS and RSVP.CONCURRENTQUERY.MAXNUMHELPERSPERREPORT are both set to four, the report consumes all query helpers when executed. No other report is able to run queries concurrently until the report has finished executing.
- If RSVP.CONCURRENTQUERY.MAXNUMHELPERSPERREPORT is set to two instead, the report consumes two query helpers, leaving two for other reports to use.

The default value for this parameter is 1.

This setting has no effect unless RSVP.CONCURRENTQUERY.NUMHELPERSPERPROCESS is set to greater than 0.

RSVP.CONCURRENTQUERY.ENABLEDFORINTERACTIVEOUTPUT

Use this parameter to enable concurrent query execution when the report service is producing interactive output.

For interactive reports, if concurrent query execution is enabled, some queries may be unnecessarily executed because the results are not used. For example, all the queries for a multi-page report may execute with at least one query on each page, but the user may view only the first page. If you do not want to use resources for results that are not used in interactive reports, disable this parameter.

Authored prompt pages are not interactive output and are not affected by this setting.

The default value for this parameter is false, meaning disabled.

RSVP.PROMPT.EFFECTIVEPROMPTINFO.IGNORE

Use this parameter to disable the issuing of effectivePromptInfo attribute in metadata requests and effectively disable moving the prompt information from under the caption attribute of a level to the level itself.

The default value for this parameter is false, meaning disabled.

Guidelines for concurrent query execution

We recommend that you follow these guidelines to improve the efficiency of your concurrent query execution.

Report Servers can execute multiple reports at the same time. Each report runs on one thread within the Report Server. Having more CPUs allows more reports to run at the same time. As a report is executed, requests for data will be made via the query engine. In some scenarios, leveraging the concurrent query feature can allow several queries to be started prior to the data being required for rendering. This in turn reduces the total elapsed time for a report to complete.

Concurrent query execution allows an individual report to consume more resources, which in turn may reduce elapsed times. Increasing the number of concurrent activities may impact the throughput of the Cognos Application or database tiers in an environment.

Trying to use more threads than there are actual CPUs on a computer does not reduce the time it takes to run a report. It may also cause reports to run more slowly due to more contention on the memory heap in the Report Server process.

One scenario in which concurrent queries may improve elapsed times would be when a report renders very few pages, perhaps one page. That page may include several layouts whose queries execute quickly within the database, when run at the same time.

As a starting point, define max helpers per process set to the number of CPUs on the machine. Cognos Application tier servers normally run several services. Therefore the actual number per server would be a smaller value.

If a Report Server is frequently running multiple reports at the same time, set the number of helpers per report to a smaller number so that each report gets a few threads. This will produce more consistent execution times. If you set the max per report equal to max per process, you run the risk that one report gets all the extra threads while others don't get any extra threads.

By increasing the threads used to "n", each Report Server (BiBusTKServerMain) process has "n" threads. The potential load on the computer will be the sum of `(Report Server processes * n)`.

When Compatible Query Mode (CQM) is used, each Report Server has its own in-process query engine. When Dynamic Query Mode (DQM) is used, Report Servers send their data request to a DQM service. As a result, the Dynamic Query server resource usage and load may increase.

Concurrent queries in batch reports versus interactive reports

In general, to render reports more quickly, you should run them in a non-interactive mode instead of in interactive mode.

The concurrent query manager processes queries starting from the last query of the report and works its way to the first. When reports are rendered in a non-interactive mode, the Report Server main thread will run the first queries. It will also start to use available helper threads to start queries associated with layouts it will move to. By starting those queries, data can be available to render instead of waiting for the query to be executed at that time.

The same strategy is also used for interactive reports. However, a report design may include several page layouts which a user never navigates to. In effect, the system may have run several queries that will never be rendered as the layout is not required. Interactive mode should be enabled only if interactive reports tend to be completely consumed, such as single-page layouts. It should not be enabled if interactive reports tend to be used to view just a few pages of many.

Reports with a subset of queries enabled as concurrent

To optimize the run times of your report, set only a subset of its queries to be processed concurrently.

The Report server constructs a list of queries that are submitted to the concurrent query manager. Queries must satisfy the following requirements:

- The query's **Execute method** property must be set to **Concurrent**.
- It is referenced in a report page from a data container (List, Crosstab, Char, and so on.)
- It is not a detail layout.
- It is referenced by a prompt control that is not a cascade child.

If the list does not include two or more queries, no concurrent query processing is required.

For example, a report has 3 lists using queries Q1, Q2, and Q3. If Q2 and Q3 are marked concurrent, then only Q2 and Q3 will run concurrently; Q1 will not. In addition, if Q2 is a union of Q2.1 and Q2.2, you must mark Q2 as concurrent. Marking Q2.1 or Q2.2 as concurrent will have no effect, since Q2.1 and Q2.2 are not referenced from the layout. That is, the Report server executes Q2, not Q2.1 or Q2.2, unless some other data container references Q2.1 or Q2.2.

In complex reports, with many page layouts and queries, do not set all the queries to concurrent. This may result in excessive resource usage (memory and CPU) and not reduce elapsed times. Applications using Dynamic Query should review if the usage of Master-Detail optimization and explicit control of query re-use can reduce elapsed times.

Prerequisites for concurrent queries

To enable concurrent queries, advanced server settings and the execution method must both be set

Before report queries can be run concurrently, you and the report author must perform these tasks:

- The administrator must configure the advanced server settings for concurrent queries.
- The report author must set the **Execution method** property for the query to **Concurrent** in Cognos Analytics Reporting.

Setting parameters for concurrent query execution

Use the following procedure to set up parameters for concurrent query execution.

Note:

A concurrent query setting is ignored when

- a query is referenced by a prompt page
- a query is used as a detail in a master-detail layout

Procedure

1. Follow the steps in the section "Configuring advanced settings for specific services" on page 464.
2. For the **ReportService** or the **BatchReportService**, configure the parameters described in the section "Concurrent Query Execution" on page 70.

   Type the following parameters and values:

Parameter	Value
RSVP.CONCURRENTQUERY.NUMHELPERSPERPROCESS	n
RSVP.CONCURRENTQUERY.MAXNUMHELPERSPERREPORT	n
RSVP.CONCURRENTQUERY.ENABLEDFORINTERACTIVEOUTPUT	TRUE

3. Click **OK**.

Setting query prioritization

You can set parameters that specify how query prioritization works.

When you run a report with prompt controls defined, all parameter information is retrieved, including parameter information defined in the report, the model, and the data source. This is required for data typing and to align capabilities for prompt controls with those of its associated parameter. This operation can impact performance, especially when there are many or complex queries. From the user perspective, it can take too long to present the first prompt page or report page.

To increase speed, report authors can set a query hint in Reporting to give a query priority in determining parameter information. Queries are prioritized based on where they are used and whether they contain filters. A priority group is the set of queries sharing similar attributes, such as a filter. Instead of retrieving the parameters for all the queries at the same time, parameters for queries with author-defined priority are retrieved first, regardless of how automated query prioritization is set. For more information about parameters, filters, and prompt controls, see the *IBM Cognos Analytics - Reporting User Guide*.

Queries are grouped by priority as shown in the following table. When a query group has sub-groups, the first sub-group has priority over the second.

Query group	Priority
Queries with the **Use for Parameter Info** property set to Yes in Reporting	1
Queries with defined filters that are not used to populate prompt controls • First reference to such queries • Subsequent references to such queries	2
Queries with defined filters that are used to populate prompt controls • First reference to such queries • Subsequent references to such queries	3
Queries with no defined filters that are not used to populate prompt controls • First reference to such queries • Subsequent references to such queries	4
Queries with no defined filters that are used to populate prompt controls • First reference to such queries • Subsequent references to such queries	5

To specify a system-wide configuration that defines how queries and query groups are processed, you can assign either a setting value or name to the report server advanced setting, RSVP.PROMPT.RECONCILIATION. This allows you to specify the degree of reconciliation between prompt control capabilities and data type to that of the associated parameter. The setting you choose determines whether reconciliation accuracy or speed is more important. For example, if the report author ensures that parameters are defined with the same datatype and capabilities (i.e., optionality, cardinality, and discreteness), across all queries, specifying CHUNKED or 3 would likely achieve the best performance in the widest variety of situations.

RSVP.PROMPT.RECONCILIATION.CHUNKSIZE lets you specify chunk size. This setting is applicable when you use CHUNKED GROUPED and CHUNKED. The default chunk size is 5.

The report server advanced properties and Reporting query hints work cooperatively to provide the best performance.

You can use the settings shown in the following table to configure RSVP.PROMPT.RECONCILIATION.

Setting	Name	Purpose
0	COMPLETE	All queries are sent at once. This is the slowest, most accurate form of reconciliation. This is the default setting.
1	GROUPED	Queries are sent by priority group. This setting works best for reports that have many unfiltered queries and few filtered queries. It provides medium speed and high reconciliation accuracy.
2	CHUNKED GROUPED	Queries are sent by priority group with a maximum number per request. The queries do not span groups. This setting works best on reports that have many queries with similar filter expressions. It provides maximum speed and low reconciliation accuracy.
3	CHUNKED	Queries are sent by priority group with a maximum number per request. The queries can span groups.

Before you begin

You must have the required permissions to access **IBM Cognos Administration** Chapter 13, "Capabilities," on page 185.

Procedure

1. Follow the steps in the section "Configuring advanced settings for specific services" on page 464.
2. For the **Report** service, in the **Parameter** column, type one of the parameter names described in this section.
3. In the **Value** column, type a value associated with the setting.
4. Optional: If required, continue typing other settings and values.
5. Click **OK**.
6. Repeat the same steps for the **BatchReportService**.

Conversion of numeric search keys to strings in queries

An error may occur if your data source does not convert numeric data items to strings.

A search prompt is associated with a query that does not get executed when the search prompt is rendered the first time. Typing a search string filters the query and the results are displayed in a list box. The report server does not check the data type of the filtered query item because most data sources convert the data item to a string (varchar) and the filter becomes valid. However, some data sources, such as Teradata, do not make the conversion, which causes an error.

The following error message is displayed when a Reporting or Query Studio report runs:

RQP-DEF-0177 An error occurred while performing operation 'sqlPrepareWithOptions' status='-69' UDA-SQL-0043 The underlying database detected an error during processing the SQL request.[NCR][ODBC Teradata Driver][Teradata Database] Partial string matching requires character operands.

To avoid this error, ensure that the advanced setting **RSVP.PROMPT.CASTNUMERICSEARCHKEYTOSTRING** is set to `true` (default value) for **ReportService** and **BatchReportService**. This advanced setting is used to convert numeric data items into a string (varchar) format. For more information about configuring advanced settings, see "Configuring advanced settings for specific services" on page 464.

Example of unconverted data item

```
[data item] starts with '20'
```

```
[data item] contains '123'
```

Or a Boolean combination:

```
[data item] starts with '2' AND [data item] contains '009' OR [data item]
contains '119'
```

Example of unconverted data item with lower function

If the search is case insensitive then these expressions will contain the lower function, which makes more sense when searching on string data items than on numeric:

```
lower([data item]) starts with lower('20')
```

```
lower([data item]) contains ('123')lower
```

```
([data item]) starts with lower('2') AND lower([data item]) contains
lower('009') OR lower([data item]) contains lower('119')
```

Example of data item converted to a string

```
cast([data item], varchar(128)) starts with '20'
```

```
cast([data item], varchar(128)) contains '123'
```

```
cast([data item], varchar(128)) starts with '2' AND cast([data item],
varchar(128)) contains '009' OR cast([data item], varchar(128)) contains '119'
```

Session Caching

In Reporting, Query Studio, and IBM Cognos Viewer the results for previous requests to the database are cached for the duration of a session when session caching is enabled.

To increase performance, for subsequent queries, IBM Cognos software uses cached results for some actions rather than accessing the database. This applies when the same results can be used or when the new results are a subset of the cached results. You can disable session caching at the server level or at the package or report level.

Because performance may be affected, you may want to disable session caching at the server level in the following situations:

- users expect up-to-date results directly from the database for every query, for example new records that were added to the database in the interim
- you want to limit the number of times the cache is accessed during a session

You may also want to disable session caching for individual reports because of high resource consumption, for example, reports that use bursting.

You can also enable and disable session caching for specific queries in reports in Reporting (see the *IBM Cognos Analytics - Reporting User Guide*) and for models in Framework Manager (see the *IBM Cognos Framework Manager User Guide*).

Session caching for new models and reports is enabled by default. Existing packages and reports retain existing session caching settings.

Disabling session caching at server level

You can disable session caching at the server level.

Procedure

1. In the *`install_location`*`/configuration` directory, make a copy of the `CQEConfig.xml.sample` file and rename it to `CQEConfig.xml`.
2. Open the *`install_location`*`/configuration/CQEConfig.xml` file in an editor.

   Ensure that your editor supports saving files in UTF-8 format.
3. Find the `queryReuse` parameter in the `CQEConfig.xml` file and change the value to 0.
4. Save the `CQEConfig.xml` file.
5. Using IBM Cognos Configuration, stop and then restart IBM Cognos service. For more information, see the *IBM Cognos Analytics Installation and Configuration Guide*.

Disable Session Caching at the Package or Report Level

You can disable session caching at the package or report level.

Procedure

1. Copy the *install_location*/configuration/CQEConfig.xml.sample file to install_location/bin and rename it CQEConfig.xml.
2. Open the *install_location*/bin/CQEConfig.xml in an editor.
3. Ensure that your editor supports saving files in UTF-8 format.
4. Find the `queryReuse` parameter and remove it.
5. Save the CQEConfig.xml file.
6. Using IBM Cognos Configuration, stop and then restart IBM Cognos software. For information, see the *IBM Cognos Analytics Installation and Configuration Guide*.

Enabling the HTTPOnly parameter to secure the CAM passport cookie

CAM passport identifies the user's web browser session with the server. Administrators can set the HTTPOnly attribute to block scripts from reading or manipulating the CAM passport cookie during a user's session with the web browser.

About this task

Enabling the HTTPOnly attribute prevents malicious scripts from stealing the user's session identity. When an administrator sets this attribute, the web browser can use the session cookie only to send HTTP requests to the server.

If you want to enable the HTTPOnly attribute, ensure that the users have a web browser that supports this attribute.

Procedure

1. Go to IBM Cognos Administration.
2. On the **Status** tab, click **System**.
3. In the **Scorecard** pane, from the **System** drop-down menu click **Set properties**.
4. Click the **Settings** tab.
5. From the **Category** list, select **Environment**.
6. For the **HTTPOnly Cookie Support** parameter, select the corresponding check box in the **Value** column.
7. Click **OK**.

Reduce Decimal Precision

You can set decimal precision in crosstab reports.

In a crosstab report, values support a maximum of 18 digits, plus the decimal point. Decimal precision determines the number of the digits that are reserved to express the decimal component of a number. The remaining digits are reserved to express the integer component of the number. By default, the decimal precision is set to 7 digits, which restricts the length of integers to 11 digits.

If you want to reserve more than 11 integers to express the integer component of a number, you must reduce the decimal precision. For example, you may set the decimal precision to 2, which allows you to reserve up to 16 digits for the integer component of a number.

Procedure

1. In the *install_location*\configuration directory, locate the qfs_config.xml file.
2. Copy the qfs_config.xml file, and rename the copied file to qfs_config.xml.backup.
3. Open the original qfs_config.xml file, and find the following line of code:

```
<provider name="CubeBuildProvider"libraryName="qfsCubeBuildProvider"
serviceProvider="true">
    <providerDetails>
```

4. For the `providerDetails` element, add the following line:

```
<scaleOfFloatDouble value="n"/>
```

   where "n" represents the decimal precision value that you want to specify.

   The default value is 7.
5. Save the qfs_config.xml file.
6. Restart the IBM Cognos service.

External object store to store the report output locally

You can configure Content Manager to store report outputs to a local drive or network share by defining an external object store.

Using an external object store for report output reduces the size of the content store and provides performance improvements for Content Manager.

For more information about setting up an external object store, see the *IBM Cognos Analytics Installation and Configuration Guide*.

Saved report output

You can specify where to save copies of report output files.

The following report output formats can be saved: PDF, CSV, XML, Microsoft Excel 2002, 2007, and 2007 Data, and HTML that does not have embedded graphics.

You can share the saved report output files with external applications or with users who do not have access to IBM Cognos software.

You have the following options for saving report output files:

- A location outside of IBM Cognos software

  With this option, the users can control which report output files are saved to the file system. For more information, see "Saving report output files outside of IBM Cognos software" on page 78.
- A location in IBM Cognos software

With this option, all report output files are saved to the same file system location defined in Content Manager. This makes this option useful for deployment purposes. A descriptor file with an `_desc` extension, which is created with this option, contains useful information for IBM or third-party archival software.

This option also allows for running a predefined script for each output file, which helps with third-party integration.

For more information, see “Saving report output files in IBM Cognos software” on page 79

Both options for saving report output files are independent from each other, but they can be used at the same time.

Saving report output files outside of IBM Cognos software

Report output files can be saved to a file system outside of IBM Cognos software. Users can choose which output files to save.

About this task

This option is useful when users want to share reports with an external application, such as a website. The reports are saved to this location every time they are updated so that current content is always available. You can also save reports on a local network for users who do not have access to IBM Cognos software.

Multiple locations can be specified for the dispatchers and services.

Procedure

1. Create a directory in which to save your report outputs.
2. Enable saving report output to the file system.
   a) Start Cognos Configuration.
   b) Click **Actions** > **Edit Global Configuration**.
   c) On the **General** tab, enter the path to the directory you created in **Archive Location File System Root**.

      The path must be in the format of `file://(file-system-path)`. For example, `file://C:/reports`.
   d) Click **OK**.
   e) In the **Explorer** window, expand **Data Access**, and click **Content Manager**.
   f) Set **Save report outputs to a file system** to **True**.
   g) In the **Explorer** window, click **Environment**, and ensure that the server name or IP address is used in the URI settings. Using `localhost` in the URI settings can cause errors if you are saving the report output to a shared directory.
   h) Click **File** > **Save**.
   i) Restart the IBM Cognos services.
3. Enable saving reports in IBM Cognos Administration.
   a) In **IBM Cognos Administration**, on the **Configuration** tab, click **Dispatchers and Services**.
   b) On the toolbar, click the **Define File System Locations** icon.
   c) Click **New**, and then type a name, description, and screen tip.
   d) In **File systems location** box, type the path to the directory you created in step 1.
   e) Click **Finish**.
4. Select the output location for a report.

a) In the **Team content** or **My content** folder, select a report, click the ellipsis button, then select **Properties**.

b) Click the **Schedule** tab.

c) In the **Options** section, select **Override the default values**.

d) In the **Delivery** section, enable **Save to the file system**, and click **Edit the options**.

e) On the options page, in **Location**, select the output location.

f) Click **OK**.

What to do next

When users select **Save report as an external file** as the report delivery method when they run or schedule a report, the report output files are saved to this location.

Saving report output files in IBM Cognos software

Users can save copies of report output files in IBM Cognos software. All report output files are saved to a location specified in Content Manager.

Before you begin

Before using this functionality, set the **Save report outputs to a file system** property in IBM Cognos Configuration to true. For more information, see the *IBM Cognos Analytics Installation and Configuration Guide*.

About this task

You must specify a location in Content Manager where copies of the report output files will be saved. The location applies to saved output originating from the selected Content Manager service. This location is represented by the **`CM.OutPutLocation`** parameter.

When you save a report output this way, an XML descriptor file is also created for the output file. The descriptor file contains information about the report output, such as the name, locale, creation time, burst key, search path for the associated report, and report version contact. The descriptor file takes the name of the output file with the added suffix `_desc`. For example, a saved PDF report named 158_1075940415360.pdf will have a descriptor file named 158_1075940415360_desc.xml.

You can also specify a script so that post-processing commands can be run each time a report output is copied to the file system.

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. Follow the steps in the section “Configuring advanced settings for specific services” on page 464.
2. For the **ContentManagerService**, define the following parameters:
   - **`CM.OutPutLocation`**

     Specifies a location in IBM Cognos software where copies of report output files are saved. Old report versions are not deleted from this location when new versions are saved. This location must be properly managed so that only selected report versions are kept.

     This parameter is mandatory if you want to save report output files in IBM Cognos software.
   - **`CM.OutputScript`**

Specifies the location and name of a shell script, such as a .bat or .sh file, that runs after the report output is saved to the target directory. Full names of the report output file and the associated descriptor file are passed to the script. This parameter is optional.

- **`CM.OutputByBurstKey`**

  This parameter is applicable when report output is distributed by bursting. It specifies whether to store report output files in a subdirectory with the same name as the burst key. The default is false, which means that the output is not stored by the burst keys.

Configuring the report and batch report services to use large worksheets

Administrators can enable support for large Microsoft Excel 2007 worksheets. When this is done, worksheets with up to 1 048 576 rows are supported.

To enable support for large worksheets, specify the advanced setting **`RSVP.EXCEL.EXCEL_2007_LARGE_WORKSHEET`** for the **ReportService** and the **BatchReportService**. When the **`RSVP.EXCEL.EXCEL_2007_LARGE_WORKSHEET`** setting is specified, the following settings can also be specified:

- **`RSVP.EXCEL.EXCEL_2007_WORKSHEET_MAXIMUM_ROWS`**

  Specifies the number of rows to output before moving to a new worksheet.

- **`RSVP.EXCEL.EXCEL_2007_OUTPUT_FRAGMENT_SIZE`**

  Adjusts the internal memory fragment size, in rows, that the IBM Cognos Analytics server generates before flushing to a disk. If this value is not specified, the default is approximately 45 000 rows. This property can be useful when there are issues, such as running out of memory, when generating reports with the default value. The values might need to be lowered to allow the report to run successfully.

Procedure

1. Follow the steps in the section "Configuring advanced settings for specific services" on page 464.
2. For the **ReportService**, in the **Parameter** column, type **`RSVP.EXCEL.EXCEL_2007_LARGE_WORKSHEET`**.
3. In the **Value** column, type true.
4. Specify the **`RSVP.EXCEL.EXCEL_2007_WORKSHEET_MAXIMUM_ROWS`** and **`RSVP.EXCEL.EXCEL_2007_OUTPUT_FRAGMENT_SIZE`** settings in a similar way, and type the required values for them.
5. Click **OK**.
6. Repeat the same steps for the **BatchReportService**.

Dynamically naming worksheet tabs in Excel 2007 reports

In IBM Cognos Analytics, when the advanced property RSVP.EXCEL.PAGEGROUP_WSNAME_ITEMVALUE is set to true, the tabs in Excel 2007 output are dynamically named according to the page breaks that are specified.

Note: This property does not apply to Analysis Studio.

About this task

If page breaks are specified by product line, then the worksheet tabs have corresponding names. For example, pages that are broken with the product lines Camping Equipment, Mountaineering Equipment, Personal Accessories, Outdoor Protection, and Golf Equipment have tabs with the same names.

For more information on tab names when reports contain two page sets that use product line as the grouping item, or contain nested page sets, see the *IBM Cognos Reporting User Guide*.

Procedure

1. Follow the steps in the topic “Configuring advanced settings for specific services” on page 464.
2. On the **Set advanced settings - ReportService** page, in the **Parameter** column, type `RSVP.EXCEL.PAGEGROUP_WSNAME_ITEMVALUE`.
3. In the **Value** column, type `true`.

Configuring the lineage solution

Lineage provides details about data in a report, such as the data source and calculation expressions. You can configure the default IBM Cognos software lineage solution, the IBM InfoSphere® Information Governance Catalog lineage tool, or a custom lineage solution.

You can access lineage information in IBM Cognos Viewer, Reporting, Query Studio, and Analysis Studio. To use the default solution or IBM InfoSphere Information Governance Catalog, ensure that the value for the **Metadata Information Service URI** parameter of the **Environment** category is configured as specified in the steps in this section.

To implement a custom lineage solution, you must

- create a Web interface that translates the IBM Cognos software lineage request parameters and invokes the custom lineage solution.

  For more information, see the section about integrating a custom lineage solution in the *IBM Cognos Software Development Kit Developer Guide*.
- change the value for the **Metadata Information Service URI** parameter of the **Environment** category to the URL of your lineage server.

Before you begin

The **lineage** capability must be enabled. For more information, see Chapter 13, “Capabilities,” on page 185, and Chapter 14, “Object Capabilities,” on page 197.

Note: To see a list of the supported versions of InfoSphere Information Server, see the Cognos Analytics Software Product Compatibility Reports.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. From the **System** Actions menu, click **Set Properties**.
3. Click the **Settings** tab.
4. For the **Environment** category, **Metadata Information Service URI**, type one of the following values.
   - If you want to configure the default IBM Cognos software lineage solution, type **/lineageUIService**.

     If this value is already specified, click **Cancel**. You do not need to change anything.
   - If you want to configure IBM InfoSphere Information Governance Catalog as your lineage solution, type the url as follows

     /lineageUIService?iis=https://*igc_server_name*:9080/ibm/iis/igc#cognosLineage/*cognos_server_name*

     where https://*igc_server_name*:9080/ibm/iis/igc#cognosLineage/*cognos_server_name* is the URL where IBM InfoSphere Information Governance Catalog can be accessed on the network.

     igc_server_name represents the server name where IBM InfoSphere Information Governance Catalog is installed.

     – To leverage a combination of Cognos lineage and InfoSphere Information Governance Catalog lineage, there is an additional parameter to be configured. A "launchPoint" parameter set with a value of "indirect" will indicate that Cognos lineage should be used for Cognos level lineage (that is, report and model level information) and Information Governance Catalog can be used to explore lineage for the data source. Clicking on the data source object in the Cognos lineage viewer will invoke IBM InfoSphere Information Governance Catalog to explore in-depth data source level lineage information.

/lineageUIService?launchPoint=indirect&iis=*Information_Governance_Catalog_URL*

For example, /lineageUIService?launchPoint=indirect&iis=https://*igc_server_name*:9080/ibm/iis/igc#cognosLineage/*cognos_server_name*

igc_server_name represents the server name where IBM InfoSphere Information Governance Catalog is installed.

- If you want to configure a custom lineage solution, replace the existing value with the URI that represents your lineage Web interface.

  For example, type https://mycompany.com/ourLineageService.cgi

5. Click **OK**.

Configure the InfoSphere Business Glossary URI

To access the IBM InfoSphere Business Glossary from the viewer in IBM Cognos Analytics, and from the metadata tree in Reporting, Query Studio, and Analysis Studio, you must specify the URI of the Glossary web page.

By default, the Glossary search results in Cognos software return only terms that contain the keyword specified in the search. Other types of assets are not returned.

For more information, see "Access the InfoSphere Business Glossary" on page 324.

Before you begin

To access the InfoSphere Business Glossary, users must have permissions for the **Glossary** capability. For more information, see Chapter 13, "Capabilities," on page 185, and Chapter 14, "Object Capabilities," on page 197.

Procedure

1. From **Manage** > **Administration console**, open **IBM Cognos Administration**.
2. On the **Status** tab, click **System**.
3. For **System**, click the **Actions** menu, and then click **Set Properties**.
4. Click the **Settings** tab.
5. For the **Environment** category, **IBM Business Glossary URI**, type the following URI: `https://`*`igc_server_name`*`:`*`port_number`*`/ibm/iis/igc/popup/popupSearch.do?exactMatch=1`

   For example, type `https://`*`igc_server_name`*`:9080/ibm/iis/igc/popup/popupSearch.do?exactMatch=1`
6. Click **OK**.

Configuring the Collaboration Discovery URI

You can configure IBM Cognos Analytics and IBM Cognos Workspace 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 IBM Connections activities from within IBM Cognos Workspace and to the IBM Connections homepage from within IBM Cognos Analytics and IBM Cognos Workspace.

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
- a link to the IBM Connections homepage is added to the Actions menu in IBM Cognos Workspace
- the **Collaborate** menu button is added on the workspace application bar in IBM Cognos Workspace. This allows the user to create or view a workspace activity in IBM Connections.

To access the IBM Connections homepage and activities page, the administrator must enable the **Collaborate** capability. For more information, see Chapter 13, "Capabilities," on page 185.

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**.

Enabling job, SMTP, and task queue metrics

By default, only the queue length metric for job, task, and SMTP queue metrics is enabled. Other metrics are also available for each but are set to zero and do not appear in the user interface unless you enable them.

- **Time in queue high water mark**
- **Time in queue low water mark**
- **Time in queue**
- **Number of queue requests**
- **Queue length high water mark**
- **Queue length low water mark**

For more information about these metrics, see Chapter 4, "System Performance Metrics," on page 21. Note that enabling these settings may affect performance.

Before you begin

You must have the required permissions to access **IBM Cognos Administration** functionality. See Chapter 13, "Capabilities," on page 185.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. From the **System** Actions menu, click **Set Properties**.
3. Click the **Settings** tab.
4. For the **Environment** category, next to **Advanced settings**, click the **Edit** link.
5. If it appears, select the **Override the settings acquired from the parent entry** check box. Otherwise, proceed to the next step.

6. In the **Parameter** column, type the following settings: **enable.tide.metrics.smtpqueue**, **enable.tide.metrics.jobqueue**, and **enable.tide.metrics.taskqueue**.
7. Beside each parameter, in the **Value** column, type **True** to enable the metric.
8. Click **OK**.
9. Open the *install_location*/webapps/p2pd/WEB-INF/classes/iManage-metadata.xml file in an editor.

   Ensure that your editor supports saving files in UTF-8 format.

   For a distributed install, you must edit the iManage-metadata.xml file on every computer, otherwise, the global metrics may display initially but not persist after navigating away from the page.
10. Uncomment the sections that begin with `<!-- These metrics have been explicitly disabled. Please consult documentation on how to enable them. -->`
11. Save the file.
12. Using IBM Cognos Configuration, stop and then restart IBM Cognos software.

    For information about stopping IBM Cognos software, see the *IBM Cognos Analytics Installation and Configuration Guide*.

Setting lifetime of completed human tasks and annotations (comments)

You can set the lifetime of completed annotations and human tasks.

The lifetime is the length of time after the associated entry is deleted. For example, if the lifetime for an annotation is set to 60 days, the annotation is deleted 60 days after the associated report is deleted. If the lifetime for a human task is set to 120, the human task might be deleted 120 days if all linked reports or dashboards are deleted.

The default lifetime is 90 days for completed human tasks and 180 days for completed annotations.

For more information about human tasks, see Chapter 25, “Managing Human Tasks,” on page 331. For more information about annotations (comments), see the *IBM Cognos Workspace User Guide*.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **Services** > **Human Task Service** or **Services** > **Annotation Service**.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. From the **Actions** menu of the service, click **Set properties**.
4. Click the **Settings** tab.
5. For annotations, find the setting **Completed annotation lifetime**. For **HumanTaskService**, find the setting **Completed human task lifetime**. Set the lifetime in days or months and click **OK**.

Results

Completed annotations or human tasks are deleted after the number of days that you specify.

Changing Drill-Through Filter Behavior

You can change the dynamic drill-through filter behavior if you want drill-through to generate a filter using the Member Business Key instead of the default Member Caption.

Set the RSVP.DRILL.DynamicFilterUsesBusinessKey parameter to 0 to use Member Caption. Set it to 1 to use the Business Key.

Before you begin

You must have the required permissions to access **IBM Cognos Administration** functionality. See Chapter 13, “Capabilities,” on page 185.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **Services** > **Report**, or **Services** > **Batch Report**.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. From the **ReportService** or **BatchReport Service**, **Actions** menu and click **Set properties**.
4. Click the **Settings** tab.
5. Click **Edit** next to **Advanced Settings**.
6. Select **Override the settings acquired from the parent entry**.
7. In the **Parameter** column, type `RSVP.DRILL.DynamicFilterUsesBusinessKey`.
8. In the **Value** column, type the associated value for the setting.
9. Click **OK**.
10. On the **Set properties** page, click **OK**.

Controlling whether URL parameters are sent to Content Manager

For performance considerations, URL parameters are not included with queries to Content Manager.

However, URL parameters may be required, for example, to avoid single signon failure with authentication providers. If URL parameters are required, you can include them by setting the **`forwardURLParamsToCM`** to true.

The default setting for this parameter is false.

Procedure

1. In IBM Cognos Administration, click **Configuration** > **Dispatchers and Services**.
2. To specify the **`forwardURLParamsToCM`** setting for a single dispatcher, do the following:
   a) In the **Name** column, click a dispatcher, and click **Set properties**.
   b) Go to the **PresentationService**, and click **Set properties**.
   c) Click the **Settings** tab, and for **Environment**, **Advanced settings**, click **Edit**.
   d) Click **Override the settings acquired from the parent entry**. Now, go to step 4.
3. To specify the **`forwardURLParamsToCM`** parameter globally, for multiple dispatchers, do the following:
   a) On the **Configuration** toolbar, click **Set properties - Configuration**.
   b) Click the **Settings** tab, and for **Environment**, **Advanced settings**, click **Edit**.
4. In the **Parameter** field, type **`forwardURLParamsToCM`**, and in the **Value** field, type **`true`**.
5. Click **OK**.

Printing from UNIX operating systems

The RSVP.PRINT.POSTSCRIPT property controls which interface to use to print PDF documents from a UNIX operating system. If you want to continue using the Adobe Acrobat PDF interface, set the value of this property to false.

The RSVP.PRINT.POSTSCRIPT property applies only to UNIX operating systems and its default value is true. Keeping the default value provides users with the ability to print PDFs using the internal postscript interface from a UNIX operating system.

Before you change the RSVP.PRINT.POSTSCRIPT property value to false, ensure that you have installed the latest version of Adobe Acrobat Reader for your operating system.

Procedure

1. Follow the steps in the section “Configuring advanced settings for specific services” on page 464.
2. For the **BatchReportService**, in the **Parameter** column, type **`RSVP.PRINT.POSTSCRIPT`**.
3. In the **Value** column, type false.
4. Click **OK**.

Adding Cognos Workspace domains to the valid domain list

You must use valid domains for URLs in toolbox widgets in IBM Cognos Workspace. Add the domains that Cognos Workspace users will use to the Valid Domain List.

Procedure

1. In IBM Cognos Administration, click **Configuration** > **Dispatchers and Services**.
2. Click the **Set properties** icon.
3. Open the **Settings** tab.
4. Select the **Advanced settings** and click **Edit**.
5. Add the parameter **`BUXClientValidDomainList`**.
6. In the **Value** column, add the domains in a comma-separated list.

Preventing content store locking when you add or update numerous schedules

In IBM Cognos Analytics, when numerous schedules are added or updated, the content store database can lock if the schedules contain invalid data. If you experience this problem, you can set an advanced property that validates schedule properties and disables invalid schedules.

About this task

Schedules that contain invalid data can lock the content store database. For example, a schedule can contain invalid user account credentials. If you add or update schedules, and the credential property references invalid user account credentials, Content Manager repeatedly attempts to update invalid schedules without success.

If the emf.schedule.validation.enabled property is set to true, schedule properties such as start date, end date, data types, and user account credentials are validated. Invalid schedules that are encountered are disabled, and details of the disabled schedules are logged in the log files.

The default for this property is false. To enable schedule validation, set the property to true.

Procedure

1. Follow the steps in the topic, "Configuring advanced settings for specific services" on page 464.
2. In the list of dispatcher services, select **EventManagementService**.
3. For the **Environment** configuration setting, in the **Value** column, click **Edit**.
4. To add the parameter name, type `emf.schedule.validation.enabled`.
5. To add the value, type `true`.

Chapter 6. Data sources and connections

A data source defines the physical connection to a database. IBM Cognos Analytics supports multiple relational, OLAP, and DMR data sources.

The data source connection specifies the parameters needed to connect to the database, such as the location of the database and the timeout duration. A data source connection can include credentials information and a signon. One data source can have multiple connections.

You can make one or more data sources available by combining them, along with other elements, in packages created and published using Framework Manager. For instructions on creating packages, see the *IBM Cognos Framework Manager User Guide*. You can also create and edit packages in IBM Cognos software for some data sources. For more information, see Chapter 20, “Packages,” on page 291.

You can secure data sources using IBM Cognos security. IBM Cognos software also respects any security that is defined within the data source. For more information, see “Securing data sources” on page 138

You move data sources from one environment to another environment by deploying the entire content store. For more information, see Chapter 19, “Deployment,” on page 267.

Compatible query mode

This type of query processing is used in IBM Cognos Analytics version 10.2.2 and earlier. 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.

If the data source is 64-bit, ensure that you use the 32-bit client libraries to connect to the data source to use the compatibility query mode.

Dynamic query mode

Dynamic query mode provides communication to data sources using Java or 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 relational databases, the JDBC drivers must be copied to the IBM Cognos Analytics `*install_location*\drivers` directory. For more information, see the topic about setting database connectivity for reporting databases in the *IBM Cognos Analytics Installation and Configuration Guide*.

For supported OLAP data sources, 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.

For more information, see “Using JDBC connections for data sources” on page 115.

Data source types

IBM Cognos Analytics supports many different types of data sources, including relational, OLAP, and XML data sources.

The list of supported data source types might change from release to release. For information about the currently supported data sources, see the Supported Software Environments (www.ibm.com/support/docview.wss?uid=swg27047186) website. For additional information, see the list of Critical issues (www.ibm.com/support/docview.wss?uid=swg27047185) that might also include information about data sources.

The data source connection information for each type of data source might be different. For information about the parameters that you need to specify to connect to your data source, see the vendor documentation.

IBM Db2 Data Sources

IBM Cognos Analytics supports Db2 data sources.

JDBC connections can be used to connect to Db2 for Linux, UNIX, and Microsoft Windows operating systems, and Db2 for z/OS®.

Trusted IBM Db2 Database Connections

You can establish a connection between the IBM Db2 database and IBM Cognos software where multiple users connect to the database using the database trusted context feature.

A data source that is used for trusted application connections must define open session blocks for any user-specific database state that must be defined before the proxy users queries being issued. The associated Open Connection block is only executed once when the trusted connection is attempted, while Open Session blocks can execute many times for different users.

The information that a connection is going to proxy a request on behalf of a user, who is allowed to use proxy logons, is provided to the database using the following session command block attached to the trusted database connection. The value that you use for the session variable, OCI_ATTR_USERNAME, must match the Db2 user name.

```
<commandBlock>
    <commands>
        <sessionStartCommand>
            <arguments>
                <argument>
                    <name>OCI_ATTR_USERNAME</name>
                    <value>#$account.defaultName#</value>
                </argument>
            </arguments>
        </sessionStartCommand>
    </commands>
</commandBlock>
```

For information about adding a command block for a data source connection, see "Adding command blocks while creating a data source" on page 133.

Prerequisites for using trusted connections

There are some prerequisites to consider if you plan to use trusted connections.

- Use Db2 client version 9.5 or higher on all platforms.
- Use a Db2 Call Level Interface (Db2 CLI) to create a trusted connection.
- You must create a signon for the data source connection to specify the Db2 credentials of the trusted Db2 user.
- The Trusted Context that you defined in your Db2 database must not request credentials for the user that is being proxied.

IBM Db2 Connection Parameters

You specify connection parameters when you create a data source or modify a data source connection.

For more information, see "Data source connections" on page 115.

Table 22. Db2 connection parameters

Parameter	Description
Db2 database name	Enter the name (alias) of the Db2 database that was used when the Db2 client was configured.

Table 22. Db2 connection parameters (continued)

Parameter	Description
Db2 connect string	Optional. Enter name/name value pairs that the Db2 CLI or ODBC vendors can accept.
Collation sequence	Enter the collation sequence to be included in the database connection string. Collation sequences are required only in rare cases where there may be sorting discrepancies between IBM Cognos Analytics and a database. The Cognos query engine can detect certain types of collation sequences in a Db2 database, including 1252-IDENTITY and 1252-UNIQUE. Sorting between local processing and database processing is consistent if the Db2 database is set to one of these collation sequences.
Open asynchronously	Not used.
Trusted context	Select this check box to allow IBM Cognos Analytics to attempt a trusted connection to an appropriately configured Db2 server. For more information, refer to the Db2 administration documentation. If you select this check box with a client or server that does not support the feature, you may get a connection error or a report execution error.
Timeouts	Specify the time in seconds within which you want the database to connect or wait for your reply before timing out. Valid entries are zero to 32,767. To have the database wait indefinitely, enter zero, which is the default.
Signon	For more information on signon, see "Securing data sources" on page 138. If no authentication is required, click **No authentication**. If authentication is required, click **Signons**. If a user ID and password is required in the connection string, select the **User ID** check box. If a password is required, select the **Password** check box and enter the password in the **Password** and **Confirm password** boxes. To create a user ID and password that automatically connects to the data source, click **Create a signon that the Everyone group can use**. Enter the **User ID** and then enter the password in the **Password** and **Confirm password** boxes.

IBM Db2 JDBC Connection Parameters

If you have selected the **Configure JDBC connection** check box, you can specify JDBC connection parameters when you create a data source.

For more information, see "Data source connections" on page 115.

IBM Cognos Cubes

The IBM Cognos cubes that can be used as data sources in IBM Cognos Analytics include IBM Cognos Planning Contributor and IBM Cognos PowerCubes.

If you have problems creating data source connections to Cognos cubes, see the *IBM Cognos Analytics Troubleshooting Guide*.

For information about connecting to the IBM Cognos Planning - Contributor unpublished (real-time) data, see the IBM Cognos Planning *Installation Guide*.

IBM Cognos Planning Contributor

IBM Cognos Analytics supports IBM Cognos Planning Contributor as a data source.

You can use IBM Cognos Analytics to report on and analyze real-time Contributor data.

You can create an IBM Cognos Contributor package in one of the following ways:

- Using the Contributor Administration Console, you can create a package that contains all the cubes in the application. When a user opens the package in a studio, they are presented with metadata for all the cubes in the application and can choose from multiple cubes to create reports. However, users may be at risk of inadvertently building queries that attempt to use values from more than one cube, resulting in reports with no data. For more information, refer to the *IBM Cognos Planning Contributor Administration Guide*.
- Using Framework Manager, you can determine how many cubes to expose in a package. By default, you get one cube in each package. However, this may result in a large number of packages, which could be difficult to manage. For more information, refer to the *IBM Cognos Framework Manager User Guide*.

You specify connection parameters when you create a data source or modify a data source connection. For more information, see "Data source connections" on page 115.

Table 23. Planning Contributor data source connection parameters

Parameter	Description
External namespace	Select the external namespace.

IBM Cognos PowerCubes

IBM Cognos Analytics supports PowerCubes generated by Transformer 7.3 and later versions.

You make a PowerCube available to end users by creating a package and publishing it from Transformer or Framework Manager. You can also create PowerCube packages in IBM Cognos Analytics (see Chapter 20, "Packages," on page 291. You create a data source connection to a PowerCube in Transformer or in Framework Manager while publishing the cube, or in IBM Cognos Administration after the cube is published.

PowerCubes can be created in Linux operating system and HPUX Itanium environments using Transformer. You can use IBM Cognos security with these types of cubes, but not Series 7 security. However, you can deploy secured Series 7 PowerCubes to Linux and HPUX Itanium computers running as report servers in the IBM Cognos environment if the Cognos content store is running on a Series 7 - compliant server.

You cannot build cubes on Linux or HPUX Itanium if you are using Impromptu Query Definition (.iqd) files as data sources because the Series 7 IQD Bridge is not supported on those platforms.

After a connection to a PowerCube is created, you can:

- create a package for a PowerCube, see "Create a Package for a PowerCube" on page 291
- deploy updated PowerCubes, see "Deploying updated PowerCubes" on page 138

For more information about PowerCubes, see the *IBM Cognos Transformer User Guide*.

You specify connection parameters when you create a data source or modify a data source connection. For more information, see "Data source connections" on page 115.

Table 24. PowerCubes data source connection parameters

Parameter	Description
Read cache size	**Note:** The default value for this parameter is 80 MB. You can set this parameter to a value between 1 MB and 1 GB, as required for optimal query performance. The optimal read cache size may be higher or lower than the default value of 80 MB. This is to be expected, as PowerCubes in production vary widely in type and query characteristics. Note that the read cache size has no effect on the initial time required to open a cube. The typical profile for query performance, or processing time, follows a pattern whereby performance increases with the read cache size and then levels off beyond the optimal setting. To determine the optimal setting, we recommend that you lower the default by 10 MB (or 5 MB, or 1 MB, depending on the level of fine tuning desired) and use the resulting query performance results as a guide for establishing whether further reductions, or increases, are required. The optimal read cache size will change as the cube grows and changes in the production environment. As a result, you should review the optimal read cache size when changes to the user's query performance pattern, or changes in the PowerCube characteristics, occur.
Location	If all your report servers are installed on Microsoft Windows operating system computers, specify the **Windows location**. If all report servers are installed on UNIX operating system computers, specify the **Unix or Linux location**. Type the full path and file name for the cube. For example, for a local cube type C:\cubes\sales_and_marketing.mdc. For a network cube type \\servername\cubes \sales_and_marketing.mdc **Note:** For cubes that reside on UNIX computers, specify the correct UNIX location and type any characters in the Windows location because the Windows location cannot be empty. **Note:** If the report servers are installed on Windows and UNIX computers, and you want the report server running a request to access the PowerCube in both environments, specify the Windows and UNIX locations. To ensure that the same data is returned regardless of the environment in which the report server accesses the cube, the same cube file must be saved in both locations.

Table 24. PowerCubes data source connection parameters (continued)

Parameter	Description
Signon	If you are using IBM Cognos security, click **Restrict PowerCube authentication to a single namespace**, and select a namespace from the list. If you are connecting to a password-protected PowerCube, click **Cube password**, and type the password in the **Password** and **Confirm password** boxes. **Note:** Select **All applicable namespaces (including unsecured PowerCubes)** only if you are migrating Series 7 PowerCubes to IBM Cognos Analytics in your development or test environment. This setting can also be used for unsecured PowerCubes in a production environment. If a cube password is required, click **Cube password**, then enter the password in the **Password** and **Confirm password** boxes. To create a user ID and password that automatically connects to the data source, click **Create a signon that the Everyone group can use**. For more information, see "Securing data sources" on page 138.

Recommendation - Using PowerCubes in IBM Cognos Software

There are recommendations if you use PowerCubes in IBM Cognos Software.

Specifically:

- When testing the migration of Series 7 PowerCubes, you can select the signon option to authenticate with **All applicable namespaces**.

  This option is only used for the migration of namespaces in Transformer models. It does not change the fact that multiple namespaces are not supported in a production environment.
- When you use Series 7 PowerCubes as data sources, we recommend that you optimize them for IBM Cognos Analytics.

  Optimized PowerCubes provide faster data retrieval at runtime. You optimize PowerCubes using a command line utility named pcoptimizer, which is supplied with IBM Cognos software.

  For more information about optimizing PowerCubes, see the *IBM Cognos Analytics Troubleshooting Guide*.
- When you publish a PowerCube and the cube contains custom views, you must be authenticated in IBM Cognos software using a valid user ID and a password.

  Anonymous access is not supported in this situation.

Securing PowerCubes

PowerCubes supported by IBM Cognos software can be secured using IBM Cognos security namespaces. Security can be applied to an entire cube or to its custom views. Before accessing a cube secured against an IBM Cognos namespace, you must log on to the applicable namespace.

In production environments, IBM Cognos software supports only PowerCubes secured against a single namespace. Therefore, when you deploy PowerCubes for use in a production environment, you must select the signon option **Restrict PowerCube authentication to a single namespace**.

Note: Instead of using IBM Cognos security, you can add password protection to a PowerCube or decide not to use security.

Oracle Essbase Data Source

Before connecting to an Oracle Essbase data source, some configuration is required if the data source uses scenario dimensions, hierarchies, or measures.

When a Oracle Essbase System 9 Data Source is configured with an LDAP namespace, single signon is supported. The user ID and password used to log on to the LDAP namespace automatically connects to the data source. For more information about configuring an LDAP namespace, see the *IBM Cognos Analytics Installation and Configuration Guide*.

You specify connection parameters when you create a data source or modify a data source connection. For more information, see "Data source connections" on page 115.

Table 25. Oracle Essbase data source parameters

Parameter	Description
Server name	Enter the name of the server where the database is located. For UNIX operating system, this can be the TCP/IP address of the server.
Signon	For more information on signon, see "Securing data sources" on page 138. If no authentication is required, click **No authentication**. For Essbase Server System 9 and IBM Cognos 8.4, single signon is supported if your Essbase server is configured for an LDAP namespace. • Select **An external namespace** and select **LDAP** from the list. • The user ID and password used to log on to the LDAP namespace automatically connects to the data source. If a user ID and password is required in the connection string, click **Signons**. • If a password is required, select the **Password** check box and enter the password in the **Password** and **Confirm password** boxes. • To create a user ID and password that automatically connects to the data source, click **Create a signon that the Everyone group can use**. Enter the **User ID** and then enter the password in the **Password** and **Confirm password** boxes.

Configure Scenario Dimensions

If you connect to an Oracle Essbase data source and it contains a scenario dimension, you must manually configure the scenario dimension so that IBM Cognos Analytics recognizes it. Otherwise, IBM Cognos Analytics treats the scenario dimension as a regular dimension.

Procedure

In the Oracle Essbase, assign a User Defined Attribute (UDA) named COGNOS_SCENARIO_DIMENSION to the scenario dimension.

Specify Balanced Hierarchies

Oracle Essbase Provider does not determine if a hierarchy is balanced or unbalanced. It considers all hierarchies as being unbalanced by default.

In a balanced hierarchy, each path descends to the same depth while the branches in an unbalanced hierarchy descend to different levels.

Procedure

1. In the Hyperion Solutions Essbase Administration Services tool, create a special User Defined Attribute (UDA) named COGNOS_HIERARCHY_BALANCED in the outline of the Essbase database. The UDA is created for the root member of the corresponding dimension containing a balanced hierarchy.
2. Set the attribute to 1.

Specify Measure Formats

To improve the readability of the values reported, you can specify an alternative format string for any measure.

Define a UDA for the appropriate members in the Account dimension:

```
COGNOS_FORMAT=format_string
```

The *format_string* value can be any one of the predefined number formats listed in the table below. You can use a preset numeric format to show values as millions (M) or thousands (K). For example, 1,801,791 can be shown as 1.8M or 1,801.8K.

The predefined format strings are as follows:

Table 26. Oracle Essbase data source predefined strings

Format Option	Sample Value	Example
General	1000000	1000000
0	1000000	1000000
#,##0	1000000	1,000,000
$0	1000000	$1000000
$#,##0	1000000	$1,000,000
0%	1000000	100000000%
%0	1000000	%100000000
0E+000	1000000	1E+006
0K	1000000	1000K
#,##0K	1000000	1,000K

Table 26. Oracle Essbase data source predefined strings (continued)

Format Option	Sample Value	Example
K0	1000000	K1000
K#,##0	1000000	K1,000
$0K	1000000	$1000K
$#,##0K	1000000	$1,000K
0M	1000000000	1000M
#,##0M	1000000000	1,000M
M0	1000000000	M1000
M#,##0	1000000000	M1,000
$0M	1000000000	$1000M
$#,##0M	1000000000	$1,000M

With the exception of the General format string, you can also preset the number of decimal places to show, using the format_string ~n, where n is the number of decimal places. For example, 1,801,791 can be shown as $1,801,791.00 using the format string $#,##0~2. If you do not want any decimal places, end the format string with ~0.

If your client application uses a different locale, you must replace the Currency ($), Thousands (,) and Decimal (.) symbols in the format_string value for the COGNOS_FORMAT UDA with the corresponding locale symbols in effect for the client application.

If you do not specify the number of decimal places to show, or if the format string does not match one of the predefined values (including locale symbols), the General format string is used by default.

You can apply a different format for each measure. The following illustrates some examples of how you can apply different formatting to different measures:

Table 27. Oracle Essbase data source formats for measures

Measure	Applied Format
Measures (Account dimension)	COGNOS_FORMAT=#,##0
Units	COGNOS_FORMAT=#,##K
Costs	COGNOS_FORMAT=$#,###
Profits	COGNOS_FORMAT=0%

IBM InfoSphere Warehouse Cubing Services

IBM Cognos software provides support for accessing the cubing services technology of IBM InfoSphere Warehouse for version 9.5.2 and greater. No IBM Cognos components need to be installed on the cubing services server.

You specify connection parameters when you create a data source or modify a data source connection. For more information, see "Data source connections" on page 115.

Table 28. InfoSphere warehouse cubing services data source connection parameters

Parameter	Description
Server URL	Enter the URL of the server in the format http://<hostname>:<cube server xmla port>/IBMXmlAnalysis/ or https://<hostname>:<cube server xmla port>/IBMXmlAnalysis/. An example of the <hostname>:<cube server xmla port> is wottcub1:80.
Open SSL Connection	To use secure sockets, select this check box. To use unsecure sockets, do not select it. The setting must be the same as the setting on the server.
Signon	If a user ID and password is required in the connection string, select the **User ID** check box. If a password is required, select the **Password** check box and enter the password in the **Password and Confirm** password boxes.

Informix Data Sources

IBM Cognos software provides support for Informix® data sources.

You specify connection parameters when you create a data source or modify a data source connection. For more information, see "Data source connections" on page 115.

Table 29. Informix data source connection parameters

Parameter	Description
Informix database name	Enter the database name.
Host name	Enter the host name.
Server name	Enter the server name.
Collation sequence	Enter the collation sequence to be included in the database connection string. Collation sequences are required only in rare cases where there may be sorting discrepancies between IBM Cognos software and a database.
Service	Select or enter the service name that the remote database server uses for incoming requests.

Table 29. Informix data source connection parameters (continued)

Parameter	Description
Signon	For more information on signon, see "Securing data sources" on page 138. If a user ID or password are required in the connection string, select the **User ID** check box. If a password is required, select the **Password** check box and enter the password in the **Password** and **Confirm password** boxes. To create a user ID and password that automatically connects to the data source, select **Create a signon that the Everyone group can use**. Enter the **User ID** and then enter the password in the **Password** and **Confirm password** boxes.

Microsoft Analysis Services Data Sources

IBM Cognos software supports connectivity to Microsoft Analysis Services from a Microsoft Windows operating system platform.

When you install Microsoft SQL Server, you can choose to add Analysis Services. Connectivity requires the Microsoft Pivot Table client Libraries, which are installed with Microsoft SQL Server client components

You must install a matching version of SQL Server client software on each computer running Application Tier Components for the IBM Cognos Analytics Server or IBM Cognos Framework Manager.

You must enable the TCP protocol for Microsoft SQL Server and Microsoft SQL Server client components.

The IBM Cognos Analytics Server supports three different types of authentication for Analysis Services data sources:

- "Authentication using Signons" on page 100
- "Authentication using Service Credentials" on page 101
- "Authentication using an External Namespace" on page 101

There are special considerations if you are using Framework Manager, see "Framework Manager Considerations" on page 102 and for multidimensional expression (MDX) queries, see "Multidimensional Expression (MDX) Queries" on page 102.

You specify connection parameters when you create a data source or modify a data source connection. You can select from the following data source types:

- Microsoft Analysis Services 2012 (ODBO)
- Microsoft Analysis Services 2014 (ODBO)
- Microsoft Analysis Services 2016 (ODBO)
- Microsoft Analysis Services (HTTP XMLA)

For more information, see "Data source connections" on page 115.

Table 30. Microsoft analysis services data source connection parameters

Parameter	Description
Server Name	**Note:** Enter the server name where the databases are located.

Table 30. Microsoft analysis services data source connection parameters (continued)

Parameter	Description
Named instance	Enter the named instance if one was specified during installation. **Note:** This parameter applies to Microsoft Analysis Services 2005 and 2008 only.
Language	Select the language. For Microsoft Analysis Services 2005 and 2008, this is used as a design locale by the report author for retrieving metadata from the cube to display in reports. Once the reports are created, they can be run in any locale.
Signon	For more information on signon, see "Securing data sources" on page 138. To authenticate using the credentials of the Windows domain account that is running the IBM Cognos service, select **IBM Cognos software service credentials**. For more information, see "Authentication using Service Credentials" on page 101 To use an external namespace, select **An external namespace** and select a namespace. For more information, see "Authentication using an External Namespace" on page 101. When modifying an existing data source that previously used signons, after you switch to an external namespace, delete the signons. Otherwise, the signons take precedence. To create a static signon that everyone can use, select **Signons** and **Create a signon that the Everyone group can use**. Select the **Password** checkbox and enter a valid Windows domain **User ID**, and then enter the password in the **Password** and **Confirm password** boxes. For more information, see "Authentication using Signons" on page 100.

Authentication using Signons

When you want to store and maintain credentials to authenticate to Microsoft Analysis Services data sources in IBM Cognos software, use a signon when you create the data source. You can define a signon which is used by everyone (default) or you can grant access to specific users. You can also create multiple signons and use permissions to grant access for specified users, groups or roles.

The signon stores valid Windows domain credentials, which are used to authenticate to Analysis Services. They must be specified in the following syntax:

<DOMAIN>\<USERNAME>

For Microsoft Analysis Services 2005 and 2008, users with credentials should be a part of the local OLAP users group that exists on the computer where Analysis Services is running. This group, which is created when Analysis Services is installed, is called SQLServerMSASUser$<SERVERNAME>$MSSQLSERVER.

On every installation of an IBM Cognos Application Tier component, ensure that IBM Cognos software is run as a LocalSystem built-in account or that IBM Cognos software is run as a valid domain account which has been granted the **Act as part of the operating System** privilege in the local security policy.

IBM Cognos users must be granted read and execute permission for that signon.

Authentication using Service Credentials

When you want to use the credentials of the account that is executing the IBM Cognos service to authenticate to Microsoft Analysis Services, use service credentials. Every connection to Microsoft Analysis Services data sources uses the service credentials regardless of which user executes the request.

To use service credentials, IBM Cognos software must be started as a Windows service. The service must be run as a valid Windows domain user. The built-in accounts of LocalSystem or NetworkService are not applicable. For information on how to start the IBM Cognos service under an account, see information about configuring a user account or network service account in the *IBM Cognos Analytics Installation and Configuration Guide*.

The account running the IBM Cognos service must fulfill the following requirements:

- The account must either be a member of the same Active Directory Forest as Analysis Services or Forest trust must be established for cross-forest setups.
- The account must be granted the **Log on as a service** privilege in the local security policy of all Windows computers running IBM Cognos Application Tier components
- For multi-node setups, the same account must be used on all computers running IBM Cognos Application Tier components.
- For Microsoft Analysis Services 2005 and 2008, the service account must be granted sufficient privileges in SSAS security to attach to the desired cubes and retrieve data.
- For Microsoft Analysis Services 2005 and 2008, the account should be a part of the local OLAP Users group, existing on the computer where Analysis Services is running. This group, which is created when Analysis Services is installed, is called SQLServerMSASUser$<SERVERNAME>$MSSQLSERVER.

Authentication using an External Namespace

If you want IBM Cognos users to access Microsoft Analysis Services data sources with their own credentials (user pass-through authentication, signon), use an external namespace. The credentials that are used to authenticate to Analysis Services are taken from the specified namespace to which the user authenticated previously.

The credentials provided by a user who is logged on to the namespace are passed to Analysis Services. Due to the authentication methods supported by Analysis Services, you can only choose a namespace of type Microsoft Active Directory.

Depending on how the user is authenticated to the Active Directory namespace specified for external namespace authentication, you can have the following sign-on setups that provide a seamless user experience:

- If a user authenticated explicitly by providing a domain user name and a password, pass-through authentication is possible. The domain credentials that are provided are passed to Analysis Services.
- If a user authenticated to the Active Directory namespace by a signon which is not based on Kerberos, user pass-through authentication is not possible. This applies to setups where the Active Directory Namespace is configured for identity mapping mode.

To configure user pass-through authentication to Analysis Services, ensure that the following conditions are met:

- All computers running IBM Cognos Application Tier components must run IBM Cognos Analytics as a Windows service under a valid domain account or LocalSystem.
- All computers running IBM Cognos software must have a Microsoft Windows server operating system. (Pass-through authentication is not supported for Windows XP.)
- The computers running Analysis Services and IBM Cognos software must be part of the same Active Directory Forest.
- The domain account (user account) or the computer account (LocalSystem) must be trusted for delegation.
- All user Windows accounts that require access to Analysis Services through IBM Cognos software must not have the **Account is sensitive and cannot be delegated** property set.

Analysis Services are configured for Kerberos authentication. For details, contact your Analysis Services Administrator.

For SSAS 2005 and SSAS 2008, Windows accounts for all users must be a part of the local OLAP users group on the computer where Analysis Services is running. This group, which is created when Analysis Services is installed, is called SQLServerMSASUser$<SERVERNAME>$MSSQLSERVER.

Note that there is a Microsoft issue that hinders user pass-through authentication when Analysis Services and the clients accessing it are both run on AES-aware operating systems (Windows 2008, Microsoft Vista, Windows 7). Refer to Microsoft documentation for details.

Note that you cannot test a data source which is configured for external namespace authentication. To verify that it is working, access the data source in a query.

Framework Manager Considerations

IBM Cognos Framework Manager accesses Analysis Services data sources directly without using the Report or Metadata services. This has important implications, especially for configurations with user pass-through authentication for Analysis Services.

If Kerberos-based signon is enabled for the Active Directory namespace that is configured, as an external namespace authentication source for the Analysis Services data source, ensure that the users running Framework Manager meet the following criterion:

- has the **Act as part of the operating System** privilege set in the local security policy on the computer running Framework Manager or is a member of the Local Administrators group on the Framework Manager computer with the **log on locally** privilege
- is trusted for delegation

Multidimensional Expression (MDX) Queries

You must install the following Microsoft Office components for Microsoft Excel Visual Basic for Applications (VBA) functions, such as ROUNDDOWN for MDX queries:

- Office Excel
- Microsoft Visual Basic for Applications (a shared feature in Office)

Install these components on the IBM Cognos Server for MSAS and on the Analysis Services server computer for SSAS 2005 or SSAS 2008, then restart the server machine.

Microsoft SQL Server Data Sources

IBM Cognos software supports the following types of Microsoft SQL Server data sources: ODBC, SQL 2012 Native Client, and SQL 2014 Native Client.

Depending on the types of Microsoft SQL Server data sources you are using, there are considerations you should keep in mind when defining some types of authentication.

Authentication Using IBM Cognos Service Credentials

You should not use a Microsoft Windows local system account for the IBM Cognos server logon with a Microsoft SQL Server OLE DB data source.

Authentication Using an External Namespace

You can configure IBM Cognos software to use a Microsoft Active Directory namespace, where users are prompted for credentials as part of the IBM Cognos logon process. You can configure IBM Cognos software to use these same credentials automatically when accessing the Microsoft SQL Server data source. The data source connection for Microsoft SQL Server must be configured for **An external namespace** and that namespace must be the Active Directory namespace.

You can configure IBM Cognos software to use a Microsoft Active Directory namespace and to authenticate users for IBM Cognos software using Kerberos authentication and delegation. You can configure IBM Cognos software to automatically authenticate the user when accessing the Microsoft SQL Server data source. The following configuration is required:

- The IBM Cognos gateway must be installed on an IIS Web server that is configured for Windows Integrated Authentication.
- Content Manager, the report server (Application Tier Components), IIS Web server, and the data source server (Microsoft SQL Server) must belong to the same Active Directory domain.
- The data source connection for Microsoft SQL Server must be configured for **An external namespace** and that namespace must be the Active Directory namespace.
- The report servers are trusted for delegation.

Restriction: If you use Kerberos authentication for single signon, each data source can have only one connection. For multiple connections to SQL Server with single signon enabled, you must create multiple data sources, or one connection for each data source.

For more information about installation options for the gateway and Content Manager, as well as configuring the namespace and delegating trust, see the *Installation and Configuration Guide*.

Microsoft SQL Server Connection Parameters

The following parameters are used by Microsoft SQL Server data sources.

Table 31. Microsoft SQL Server connection parameters

Parameter	Description
Server name	Enter the server name. If there are multiple instances of Microsoft SQL Server, specify `server_name\instance_name`.
Database Name	Enter the database name.
Application Name	Enter the application name.
Collation Sequence	Enter the collation sequence to be included in the database connection string. Collation sequences are required only in rare cases where there may be sorting discrepancies between IBM Cognos software and a database.

Table 31. Microsoft SQL Server connection parameters (continued)

Parameter	Description
MARS Connection	Select the Multiple Active Results Set (MARS) connection. This parameter is used only by Microsoft SQL Server (SQL 2005 Native Client or higher). Click **Yes** to allow applications to have more than one pending request per connection and more than one active default result set per connection.
Optional Connection Parameters	Enter an optional, a key-value type of a parameter, using the following syntax: `param1=value1`. Multiple parameters must be delimited by a semicolon, as shown in the following example: `param1=value1;param2=value2` Anything that you type for this parameter is appended to the database portion of the connection string. **Tip:** The first occurrence of the @ character separates the database portion of the connection string from the IBM Cognos portion of the connection string, except if the @ character is a part of the user ID or password. This does not apply to the dynamic query mode.
Signon	For more information on signon, see "Securing data sources" on page 138. If no authentication is required, select **No authentication**. For more information on **IBM Cognos Analytics**, see "Authentication Using IBM Cognos Service Credentials" on page 103. If you use a Microsoft Active Directory namespace and you want to support single signon, select **An external namespace**, and select the Active Directory namespace. For more information, see "Authentication Using an External Namespace" on page 103. If authentication is required, select **Signons**. If a user ID and password is required in the connection string, select the **User ID** check box. If a password is required, select the **Password** check box and enter the password in the **Password** and **Confirm password** boxes.

You can include database commands in the connection information for this type of data source. For more information, see "Passing IBM Cognos context to a database" on page 128.

For information about Microsoft SQL Server (ODBC) connection parameters, see "ODBC Data Source Connections" on page 104.

ODBC Data Source Connections

IBM Cognos software supports ODBC data sources.

IBM Cognos software divides ODBC connections into two categories: vendor-specific ODBC data sources connections, which use driver-specific capabilities for query creation, and generic ODBC data source connections, which use general capabilities.

IBM Cognos software supports the ODBC data sources listed in the following table. The database code appears in the connection string, but cannot be edited.

Table 32. ODBC data sources and database code

ODBC Data Source	Database code
ODBC	OD
Microsoft SQL Server (ODBC)	SS
Netezza® (ODBC)	NZ
Sybase IQ (ODBC)	IQ
Teradata (ODBC)	TD

Any ODBC data source connection not listed should be created using the generic ODBC data source, database code OD.

ODBC Connection Parameters

You specify connection parameters when you create a data source or modify a data source connection.

For more information, see "Data source connections" on page 115.

Table 33. ODBC connection parameters

Parameter	Description
ODBC data source	Enter the data source name (DSN) as defined in the ODBC.ini file. For more information about the ODBC.ini file, see the IBM Cognos Analytics *Installation and Configuration Guide*.
ODBC connect string	Enter any text that must be appended to the connection string. This parameter is typically left blank.
Collation sequence	Enter the collation sequence to be included in the database connection string. Collation sequences are required only in rare cases where there may be sorting discrepancies between IBM Cognos software and a database.
Open asynchronously	Select if you want the connection to process requests independent of each other. Do not select if you want the connection to complete the current request before starting another one.

Table 33. ODBC connection parameters (continued)

Parameter	Description
Unicode ODBC	When the UNICODE option is checked the ODBC API for Unicode will be called otherwise the non-Unicode ODBC API will be called. When the non-UNICODE API is called, SQL statements and parameters will be encoded in the character set of the machine where the query engine is running. For more details on the ODBC API and UNICODE support refer to the Microsoft ODBC API reference.
Timeouts	Specify the time in seconds within which you want the database to connect or wait for your reply before timing out. Valid entries are zero to 32,767. To have the database have wait indefinitely, enter zero, which is the default.
Signon	For more information on signon, see "Securing data sources" on page 138. For Teradata, Microsoft SQL, and generic ODBC: • If no authentication is required, select **No authentication**. • If the credentials to the database match the credentials used to logon to the IBM Cognos environment, for single signon, select **An external namespace** and select the appropriate namespace. • If authentication is required, select **Signons**. If a password is required, select the **Password** check box and enter the password in the **Password** and **Confirm password** boxes. To create a user ID and password that automatically connects to the data source, select **Create a signon that the Everyone group can use**. Enter the **User ID** and then enter the password in the **Password** and **Confirm password** boxes.

Oracle Data Sources

IBM Cognos software supports Oracle data sources.

Oracle Connection Parameters

You specify connection parameters when you create a data source or modify a data source connection.

For more information, see "Data source connections" on page 115.

Table 34. Oracle connection parameters

Parameter	Description
SQL*Net connect string	Type the instance name of the Oracle database as it is entered in the tnsnames.ora file.
Collation sequence	Enter the collation sequence to be included in the database connection string. Collation sequences are required only in rare cases where there may be sorting discrepancies between IBM Cognos software and a database.
Signon	For more information on signon, see "Securing data sources" on page 138. If a user ID is required in the connection string, type the user ID in the **User ID** box. If a password is required, select the **Password** check box, and enter the password in the **Password** and **Confirm password** boxes. To create a user ID and password that automatically connects to the data source, select **Create a signon that the Everyone group can use**. Enter the **User ID** and then enter the password in the **Password** and **Confirm password** boxes.

External Repository data source connections

IBM Cognos software supports data source connections to external report repositories. You use the Report Repository connection to connect to a file system or an IBM FileNet® Content Manager repository.

You need to install, configure, and set up your IBM FileNet Content Manager repository before you create an External Repository data source connection.

You specify connection parameters when you create a data source or modify a data source connection. For more information, see "Data source connections" on page 115.

IBM FileNet Content Manager connections

Use the information in the following table to specify the parameters required to create a connection to your IBM FileNet Content Manager repository.

For more information about creating data sources, see "Creating a data source connection " on page 116.

Table 35. Connection parameters used to connect to a FileNet repository

Parameter	Description
Repository Type	Select **IBM FileNet Content Manager** to connect to your external FileNet repository.
Repository CMIS URL	Enter the URL for the Filenet location using the format: http://<server_name>:portnumber/<FileNet CMIS_name>/resources/<FileNet_object store_name>/ For example: http://server1:9080/fncmis/resources/archive/

Table 35. Connection parameters used to connect to a FileNet repository (continued)

Parameter	Description
Root path	Enter the location of the folder to store the archived content in FileNet. This location must already exist in FileNet. For example, you could have a folder in Filenet called report_repository.
Repository Connection Parameters	Optionally, enter parameters to append to the URL for the Driver class name.
Signon	Select the **User ID** check box. Select the **Password** checkbox. To create a user ID and password that automatically connects to the data source, click Create a signon that the Everyone group can use. Enter the User ID and then enter the password in the Password and Confirm password boxes.

File system connections

You can create a data source connection to a file system after you configure the alias root in IBM Cognos Configuration. The alias root points to a file location on a local drive or network share.

Use the information in the following table to enter the parameters required when you create a data source connection to your file system repository.

Table 36. Connection parameters used to connect to a file system repository

Parameter	Description
Repository File System Root	Select the alias root.
Root path	This is an optional parameter, which is a subfolder of the alias root. To specify the root path, enter the subfolder location to store the archived content in your file system location. This location must already exist. For example, /sales.
Repository Connection Parameters	Optionally, enter parameters to append to the URL for the Driver class name.

SAP Business Information Warehouse (SAP BW) Data Sources

IBM Cognos software supports access to SAP BW data sources.

You specify connection parameters when you create a data source or modify a data source connection. For more information, see "Data source connections" on page 115. The parameter types that you specify are different depending on the type of SAP BW logon you choose:

- Application server logon type
- Destination logon type
- Message server logon type

Application Server Logon Type Connection Parameters

If you select **Application server** as the **SAP logon type**, specify the parameters in the following table.

Table 37. Application Server logon type connection parameters

Parameter	Description
Application server	Enter the SAP application server name. For more information, contact your SAP system administrator.
System number	Enter the system number. For more information, contact your SAP system administrator.
Client number	Enter the client number. For more information, contact your SAP system administrator.
SAP server code page	Select the SAP server code page. IBM Cognos software follows the SAP internationalization rules, providing a compatible application that supports multiple scripts and languages without modifying SAP BW in IBM Cognos software. For more information, contact your SAP system administrator.
SAP router string	Enter the SAP router string. The router string describes the stations of a connection required between two hosts. For more information, contact your SAP system administrator.
Signon	For more information on signon, see "Securing data sources" on page 138. If a trusted signon namespace is configured using IBM Cognos Configuration, you can select **An external namespace** and select the namespace you want to use. To create a user ID and password that automatically connects to the data source, select **Create a signon that the Everyone group can use**. Enter the **User ID** and then enter the password in the **Password** and **Confirm password** boxes.

Destination Logon Type Connection Parameters

If you select **Destination** as the **SAP BW logon type**, specify the parameters in the following table.

Table 38. Destination logon type connection parameters

Parameter	Description
Client number	Enter the client number. For more information, contact your SAP system administrator.
SAP server code page	Select the SAP server code page. IBM Cognos software follows the SAP internationalization rules, providing a compatible application that supports multiple scripts and languages without modifying SAP BW in IBM Cognos software. For more information, contact your SAP system administrator.
Signon	For more information on signon, see "Securing data sources" on page 138. If a trusted signon namespace is configured using IBM Cognos Configuration, you can select **An external namespace** and select the namespace you want to use. To create a user ID and password that automatically connects to the data source, select **Create a signon that the Everyone group can use**. Enter the **User ID** and then enter the password in the **Password** and **Confirm password** boxes.

Message Server Logon Type Connection Parameters

If you select **Message server** as the **SAP BW logon type**, specify the parameters in the following table.

Table 39. Message Server logon type connection parameters

Parameter	Description
System ID	Enter the system ID of the SAP system that you want to connect to. For more information, contact your SAP system administrator.
Logon Group	Enter the SAP group. For more information, contact your SAP system administrator.
Client number	Enter the client number. For more information, contact your SAP system administrator.

Table 39. Message Server logon type connection parameters (continued)

Parameter	Description
Signon	For more information on signon, see "Securing data sources" on page 138. If a trusted signon namespace is configured using IBM Cognos Configuration, you can select **An external namespace** and select the namespace you want to use. To create a user ID and password that automatically connects to the data source, select **Create a signon that the Everyone group can use**. Enter the **User ID** and then enter the password in the **Password** and **Confirm password** boxes.

Sybase Adaptive Server Enterprise Data Sources

IBM Cognos software supports Sybase Adaptive Server Enterprise CT-15.

You specify connection parameters when you create a data source or modify a data source connection.

Table 40. Sybase Adaptive Server Enterprise data source parameters

Parameter	Description
Server name	Enter the name of the server.
Database name	Enter the database name. Select **Master** if you want the Sybase server to determine the default database. To override the default, enter a valid database name.
Application name	Enter the application name. If you leave this blank, the default is the name of the Cognos executable, for example, BiBustkservermain or DataBuild.
Collation sequence	Enter the collation sequence to be included in the database connection string. Collation sequences are required only in rare cases where there may be sorting discrepancies between IBM Cognos software and a database.
Packet size	Enter the packet size. The default is 2048. Increase the packet size to reduce the number of packets that must be sent. Decrease the packet size if larger packet size is an issue. The size that you can request can not be larger than the Sybase server allows. Contact your database administrator for more information.
Asynchronous levels	Select the asynchronous level.
Polling time slice	Enter the polling time slice. The default is 100.

Table 40. Sybase Adaptive Server Enterprise data source parameters (continued)

Parameter	Description
Timeouts	Specify the time in seconds within which you want the database to connect or wait for your reply before timing out. Valid entries are zero to 32,767. To have the database wait indefinitely, enter zero, which is the default.
Signon	For more information on signon, see "Data source signons" on page 124 . If a user ID or password are required in the connection string, select the **User ID** check box. If a password is required, select the **Password** check box and enter the password in the **Password** and **Confirm password** boxes. To create a user ID and password that automatically connects to the data source, select **Create a signon that the Everyone group can use**. Enter the **User ID** and then enter the password in the **Password** and **Confirm password** boxes.

TM1 Data Sources

IBM Cognos software provides support for accessing TM1® servers and cubes.

You must install the TM1 client on the same computer as the IBM Cognos Business Intelligence installation. When you create a TM1 data source connection, consider how you would like to set up authentication.

You specify connection parameters when you create a data source or modify a data source connection. For more information, see "Data source connections" on page 115.

Table 41. TM1 data source parameters

Parameter	Description
Administration Host	Enter the name of a machine that can be identified by the network.
Server Name	Enter the server name as configured in the TM1S.cfg file. For more information, see your TM1 documentation.

Table 41. TM1 data source parameters (continued)

Parameter	Description
Signon	For more information on signon, see "Securing data sources" on page 138. If no authentication is required, select **No authentication**. If an external namespace is used, select **An external namespace** and then select the namespace. If authentication is required, select **Signons**. If a user ID is required in the connection string, select the **User ID** check box. If a password is required, select the **Password** check box and enter the password in the **Password** and **Confirm password** boxes. To create a user ID and password that automatically connects to the data source, select **Create a signon that the Everyone group can use**. Enter the **User ID** and then enter the password in the **Password** and **Confirm password** boxes.

Authentication

Your choice must meet the TM1 server authentication requirement. For example, if you do not create a user ID and password, but the TM1 server requires a log on, the user is prompted to log on.

You can use an external namespace (third-party directory service provider) as an authentication method. The TM1 server must be configured to authenticate with IBM Cognos BI. For more information, see your TM1 documentation on Cognos Access Manager Authentication.

Unexpected Results When Using Aggregation with TM1 Data Sources

TM1 data sources can include rule-derived cells. IBM Cognos BI cannot identify these rule-derived cells ahead of time, so performing an aggregation on these cells may yield unexpected results. For example, aggregating a set containing a rule-derived value may produce unexpected results in Report Studio and Analysis Studio.

Note: Explicit aggregation operations like sum, average, count, minimum, and maximum are not affected.

If you are using TM1 data cubes with rule-derived cells in IBM Cognos BI, we recommend that you install TM1 build number 9.4.00001.576, which identifies aggregation errors by marking the error cells with dashes (--).

Administration Host Must be Fully Qualified to Support TM1 Data Sources

Your installation includes IBM Cognos 8 Business Intelligence Server and TM1 data sources. After upgrading or when creating or changing a TM1 data source connection, you may receive the following error message:

COGCQ00223094 - TM1-ERR-0060 the TM1 server is configured with an unsupported security mode.

To resolve the issue, change the Administration Host name to a fully qualified domain name in the Data Source Connections wizard.

XML Data Sources

When you create an XML data source, you must use XML as the type of connection and specify the location of the XML document in the connection string.

You can specify the connection string for an XML data source as:

- an HTTP URL that identifies the content store required to connect to the XML document.

  An example is HTTP://xmltestserver.cognos.com/XML/countryregion.xml.

  Ensure that you create a Web alias for the directory that contains the XML file and that you enable directory browsing.
- a file path

  A Microsoft Windows operating system file path example is \\servername\XML\countryregion.xml.

  A UNIX operating system file path example is /*mount name*/XML/countryregion.xml.
- a local file

  An example is C:\XML\countryregion.xml;VALIDATE=ON.

To access a local file, use a file path that uses platform-specific syntax.

To test an XML connection string, you must type the following code at the end of the string:

```
;VALIDATE=ON
```

The text of this code is not case sensitive.

You specify connection parameters when you create a data source or modify a data source connection. For more information, see "Data source connections" on page 115.

Table 42. XML data source parameters

Parameter	Description
Connection string	Enter the connection string.

Parameterized XML Connection Strings

In an HTTP URL connection string for an XML data source, you can use parameters to send additional information. You can embed a prompt definition string in the parameter component.

If the prompt definition is specified in the report, that value is used. Otherwise, the user is prompted to supply a value. Prompting is not supported for other types of connection strings.

An example of a URL component is addressing_scheme://*network_location*/path;parameters?query#fragment_identifier

Encode the parameter component with the definition string in between two sets of question marks. A prompt cannot cross a component boundary.

An example of a parameterized XML string is http://*My_Network_Location*/*My_Path*/myxml.asp?countryregionsid=??CanadaPrompt??

Parameterized XML connection strings have these restrictions:

- When a URL component is a prompt, it cannot contain other data.
- Prompts embedded in XML connection strings do not work in Framework Manager. You cannot import data from a parameterized XML connection string.
- When you set up a parameterized XML connection string, the Test button does not work.
- Validation of the query specification in Reporting does not work if you are connected to a parameterized XML connection string.

Data source connections

A data source connection specifies the parameters needed to connect to a database, such as the location of the database and the timeout duration. These parameters form a connection string for the data source.

If you are an administrator, you can set up all required data sources before models are created in Framework Manager so that all connections are available in the Framework Manager Metadata wizard.

Data sources are stored in the **Cognos** namespace and must have unique names. For example, you cannot use the same name for a data source and a group.

Using JDBC connections for data sources

For some data source connections, you can provide additional Java database connectivity (JDBC) data source connection information. JDBC data source connection information is optional. JDBC data source connections are required if your packages are published from Framework Manager with the **Use Dynamic Query Mode** option enabled.

The JDBC connection strings for relational data sources have the following format:

```
^User ID:^?Password:;LOCAL;JD;URL=<urlspec>;
DRIVER_NAME=<driver class name spec>[;CognosProperty=value[;...]]
```

For example, the JDBC connection string for a Microsoft SQL Server data source might look like this:

```
^UserID:^?Password:;LOCAL;JD-SS;URL=jdbc:sqlserver://sotaimpqc05:1433;
databaseName=dmsqc1;DRIVER_NAME=com.microsoft.sqlserver.jdbc.SQLServerDriver;
LOCALSORT=us_us_ASCII;LEVEL=PRIMARY
```

For relational databases, the JDBC drivers must be copied to the Cognos Analytics `*install_location*\drivers` directory. For more information, see the topic about setting database connectivity for reporting databases in the *IBM Cognos Analytics Installation and Configuration Guide*.

For information on query service settings, see the Chapter 7, “Query Service Administration,” on page 141.

Note that isolation levels are not implemented for JDBC connections. You may see different behaviour if the isolation level that you choose for the native client connection is different from the default one used by the JDBC driver. Consult your JDBC driver documentation for details on the driver default.

For more information on isolation levels, see “Isolation levels” on page 126 .

Using network paths for file-based data sources

If you have a distributed installation with several servers, we recommend that you use network paths for all file-based data sources rather than local paths. This ensures that the data sources can be accessed by the services that require them, regardless of which server requires the data.

When you create a connection to a file-based data source, such as a PowerCube, you enter a path and file name. To point to the file, use a local path, such as C:\cubes\Great Outdoors Company.mdc, or a network path, such as \\servername\cubes\Great Outdoors Company.mdc.

In a distributed installation, where report servers are running on different computers, using a local path requires that the file and path be valid on each computer where a report server is running. Alternatively, if you use a network path to point to a file, each report server points to the same file on the network without having the file available locally. Also, to ensure that the file is always available, we recommend that you store it in a shared directory that can be accessed on your network.

If you installed IBM Cognos Analytics components on UNIX operating system servers, we recommend that you also locate the file-based data source on a UNIX server. You should then use a UNIX path, such as `/servername/cubes/Great Outdoors Company.mdc` to access the file.

If you have installed all components on a single computer, you can use local paths, but you must ensure that the services requesting the data have the appropriate access to the data files on the computer.

For Microsoft Windows operating system distributed installations, we recommend that you use UNC paths to shared directories for any file based data source, such as PowerCubes or XML files.

Creating a data source connection

A data source connection specifies the parameters needed to connect to a database, such as the location of the database and the timeout duration. These parameters form a connection string for the data source.

You can include authentication information for the database in the data source connection by creating a signon. Users need not enter database authentication information each time the connection is used because the authentication information is encrypted and stored on the server. The signon produced when you create a data source is available to the Everyone group. Later, you can modify who can use the signon or create more signons.

Before you begin

You must have write permissions for the folder where you want to save the data source, and for the **Cognos** namespace. You must also have execute permissions for the **Data Source Connections** secured feature. For more information, see Chapter 13, “Capabilities,” on page 185.

About this task

Existing data source connections cannot be edited in Framework Manager.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, select **Data Source Connections**.

   Tip: To remove a data source, select the check box for the data source and select the delete button.
2. Select the new data source button.
3. In the name and description page, type a unique name for the data source and, optionally, a description and screen tip, and then select **Next**.
4. In the connection page, from the **Type** drop-down list, select the type of data source that you want to create.

   If your data source is not listed, click **Other type**.

   Tip: If you are configuring a connection to The Weather Company service, select **JDBC**.

   If you selected a relational data source, the **Configure JDBC Connection** check box is selected. If you do not want to create a JDBC connection, clear the check box. For more information about JDBC connections, see “Using JDBC connections for data sources” on page 115.
5. Specify the isolation level:

   - If **Isolation level** does not appear, select **Next**.
   - If **Isolation level** also appears, select the default object gateway or specify a value, and then select **Next**.
6. Specify the connection parameters for the data source.

   For information about connection parameters for the type of data source that you are using, click the associated item in the following list:

   - “ IBM Cognos Planning Contributor” on page 92
   - “ IBM Cognos PowerCubes” on page 92
   - “ODBC Data Source Connections” on page 104
   - “IBM Db2 Data Sources” on page 90
   - “ IBM InfoSphere Warehouse Cubing Services” on page 97
   - “ Informix Data Sources” on page 98

- “ Microsoft SQL Server Data Sources ” on page 102
- “ Microsoft Analysis Services Data Sources” on page 99
- “Oracle Data Sources” on page 106
- “SAP Business Information Warehouse (SAP BW) Data Sources” on page 108
- “Sybase Adaptive Server Enterprise Data Sources” on page 111
- “ TM1 Data Sources” on page 112
- “XML Data Sources” on page 114
- “External Repository data source connections” on page 107
- “IBM Weather Company connections” on page 120

7. Select **Test the connection**, and then **Test** to test whether parameters are correct.

   In the **Status** column, you can see if the connection was successful. If it was unsuccessful, select **Close**, return to the previous steps, and verify your connection parameters. If it was successful, go to the next step.
8. Click **Finish**.

   If you selected a data source other than IBM Cognos PowerCube or SAP BW, the new data source appears in **Data Source Connections** on the **Configuration** tab, and can be selected when using the Metadata Wizard in Framework Manager.

   If you selected IBM Cognos PowerCube or SAP BW, go to the next step.
9. Click **OK** to return to **Data Source Connections**, or for some data sources, you can click **Create a Package** and **OK**.

   Note: You can create a package with your new data source now or later. The **Create a Package** check box is available only if you have the required capabilities.
10. To make the data source connection available in the new administration interface in **Manage** > **Data server connections**, click the set properties button ▤ for the connection, and on the **Connection** tab, check the **Allow web-based modeling** check box.

What to do next

If you created a signon, you can now modify it or add more signons. For more information, see “Data source signons” on page 124.

Cognos-specific connection parameters

You can specify some optional, Cognos-specific parameters for JDBC connections.

You can specify these parameters when creating or updating JDBC connections for data sources in IBM Cognos Administration or IBM Cognos Framework Manager, or when creating or updating data server connections in the **Manage** > **Data server connections** administration interface.

In different connection editors, these parameters can be specified as **Connection properties** or **JDBC Connection Parameters**.

ibmcognos.fetchBufferSize

This parameter is used to set the JDBC driver fetch size for data source connections in IBM Cognos Analytics.

When the query service in IBM Cognos Analytics executes queries by using JDBC, the fetch size value that is passed to a JDBC driver is calculated dynamically. Support for fetch sizes depends on database vendors. The vendors also decide what the fetch size means, and what the fetch size is when it is used internally in the driver and server. For more details, refer to your vendor’s JDBC documentation.

The query service computes a value for a query by using the following formula:

```
maximum( (bufferSize / ‘row-size’), 10)
```

The default value for buffer size is 100 kilobytes (KB). The row size is computed from the size of the columns that are projected by the result set in a query. Queries that project columns with large precision or project many columns use a smaller fetch size than those projecting fewer columns or columns with smaller precision.

If the retrieval of a result set can be significantly improved by using a larger buffer size, a Cognos administrator can specify the connection property **`ibmcognos.fetchBufferSize`**. The query service automatically adjusts the value if it is lower than 10 kilobytes or greater than 10 megabytes.

If ibmcognos.fetchBufferSize > 1024 * 10240 then bufferSize = 1024 * 10240

If ibmcognos.fetchBufferSize < 10240 then bufferSize = 10240

Larger fetch sizes are not always recommended because they can potentially increase the memory consumption by the JDBC driver and not lead to improved performance. Always review the database vendor documentation and recommended practices before using large values for the **`ibmcognos.fetchBufferSize`** property.

ibmcognos.decfloat

When this parameter is specified, the query service is directed to use a decimal float type, DECFLOAT 128, which accurately represents values with precision of up to 34 digits. When a column with large precision is detected, it is internally changed to DECFLOAT and the data type in the model or report is described as DECIMAL(0,0).

To enable this feature, specify the connection parameter **`ibmcognos.decfloat=true`** for the database connection that is used by the query service. In existing models, the columns must be remapped to DECIMAL(0,0) instead of double.

For the query service to read the rows that are returned by a query, the JDBC driver must return the column values using a specific Java data type. In previous releases, it was possible for a database such as ORACLE to return a numeric column where the precision caused the query service to use the double data type. When the values that were returned by a query had precision greater than 16 digits, the conversion could result in an inaccurate value.

For example, if an ORACLE column was defined as NUMBER (without stating precision), or an aggregate such as SUM was computed that ORACLE returned as a NUMBER, the returned value of 1234567890123456789 might be converted to the value of 1.23456789012345677E18. The two values are not the same.

If the database does not return large values, do not use this parameter and ensure that the models do not include columns with the DECIMAL(0,0) data type. This allows the query service to use a data type that requires less memory than the DECFLOAT type.

ibmcognos.qualifier_list

This parameter is used to disambiguate metadata when dynamic queries are executed. It assigns a list of one or more qualifiers to data sources that are defined in IBM Cognos Analytics.

The following examples show the syntax to use when specifying the **`ibmcognos.qualifier_list`** parameter, and the values that can be assigned for it:

- ibmcognos.qualifier_list=CATALOG1.SCHEMA1, CATALOG2.SCHEMA2
- ibmcognos.qualifier_list=SCHEMA1, SCHEMA2
- ibmcognos.qualifier_list=CATALOG1.SCHEMA1, SCHEMA2
- ibmcognos.qualifier_list=CATALOG1, CATALOG2

A period in the qualifier is used to separate the catalog and schema components. If no period is present and the database supports schemas, the value is treated as a schema. Otherwise, the value is treated as a catalog, if the database supports catalogs.

The query service searches the list in the order specified, and uses the column metadata that it finds for the first qualifier that matches. If no match is found, an ambiguous metadata error is thrown.

The administrator should confirm that the list of qualifiers that are provided for this parameter is identical in order and content to any search list that the user's database session might have defined. The qualifier list is applied only when the session attempts to disambiguate metadata that is returned by a JDBC driver. Qualified names in dynamic SQL statements reflect the values assigned to catalog or schema properties that the package data source used during query planning.

ibmcognos.authentication

This parameter is used to configure data source connections when using Kerberos authentication.

For the different data source connection types, specify **`ibmcognos.authentication=java_krb5`**, and then add the properties that are required by the JDBC driver for Kerberos authentication, if they are required. The following examples show how to specify this parameter for some data source connections:

- For Teradata connections, specify **`ibmcognos.authentication=java_krb5;LOGMECH=KRB5;`**
- For SAP-HANA connections, specify **`ibmcognos.authentication=java_krb5;`**
- For Microsoft SQL Server connections, specify **`ibmcognos.authentication=java_krb5;authenticationScheme=JavaKerberos;`**

ibmcognos.maxvarcharsize

The query service can use a larger default VARCHAR precision value than the default value that is supported by the database. This parameter is used to override the database default VARCHAR precision value for the query service.

To specify this parameter, use the following syntax, where `N` is an integer value greater than zero that is supported by the database vendor:

```
ibmcognos.maxvarcharsize=N
```

The SQL standard uses the CLOB data type and the national character large object type (NCLOB) to hold large character values. Different databases support the CLOB data type or their own versions of this type with similar characteristics. The CLOB data type imposes several restrictions on the types of SQL constructs that can be used in queries. Also, database vendors might impose additional restrictions on how CLOB columns must be handled in the client interfaces, such as JDBC. To avoid CLOB-related restrictions, the query service automatically converts CLOB columns into VARCHAR columns by using the CAST function. As a result, the first `N` characters of the CLOB type are returned as VARCHAR to the query service.

Tip: The automatic CAST function is not performed when a JDBC driver describes the column data type as a VARCHAR (Variable Character field) and not as a CLOB (Character Large Object) data type, and when the column reference has a user-specified CAST function surrounding it.

If the length of a `CLOB` in a row is larger than the CAST precision data, truncation occurs.

In some cases, a database vendor might support a larger precision if specific database configuration settings, such as page and row size, or server settings, are satisfied. If such preconditions are satisfied, a larger value can be specified on a data server connection. If the preconditions are not satisfied, when you use a value greater than the one that is supported by the database, the SQL statements fail to execute. Before using larger VARCHAR precision values, refer to the database vendor documentation, and verify the value with the database administrator.

The query service uses the following default VARCHAR precision values for the different databases:

Table 43. Default precision VARCHAR values in the query service

Database	Default VARCHAR precision
Db2 iSeries	32739
Db2 ZSeries	4096
Db2 LUW	8168
Exasol	2000000

Table 43. Default precision VARCHAR values in the query service (continued)

Database	Default VARCHAR precision
Informix Dynamic Server	255
MariaDB	21845
MemSQL	21845
MySQL	65535
Oracle	4000
Pivotal Greenplum	2000000
PostgreSQL	2000000
SAP Hana	5000
SQL Server	varchar(max)
Teradata	32000
Other vendors	1024

If the `ibmcognos.maxvarcharsize` value is higher than the Java Integer max (2147483647), or not an integer at all, the value is ignored.

If the `ibmcognos.maxvarcharsize` value is lower than both the default 1024 and the vendor VARCHAR size, the lowest of these 2 values is used instead of the `ibmcognos.maxvarcharsize` value.

ibmcognos.typeinsqldisabled

When this property is specified, queries that are based on typed-in SQL are not allowed by the connection. This property is needed for data modules with security filters to prevent security vulnerabilities that typed-in SQL can introduce.

If you try to create an SQL-based table after this property was specified, the table will not be created. If you specify this property after an SQL-based table was created, the query execution is stopped.

These restrictions apply to all data modules that are based on connections that have this property specified. To bypass these restrictions, create a separate data server connection for data modules with security filters, and specify this property only for this connection. Other connections to the same data server that do not have this property specified can process queries based on typed-in SQL.

IBM Weather Company connections

You can specify some optional parameters in the connection URL or in the connection properties for IBM Weather Company.

Specify the JDBC URL in the following format:

```
jdbc:twc://[database][?properties]
```

where *database* is optional and specifies the name of the database and *properties* is zero or more of the parameters described in the following table. Separate each parameter by a comma.

Note: You must also configure at least one signon in the data source connection. The password must be your Weather Company API key. For more information, see *Importing The Weather Company sample* in the *Samples Guide*.

Parameter	Description
UNITS	Unit of measure. The following list shows the valid values: **e or E** Imperial or English **m or M** metric **s or S** International System of Units An exception is raised if an unsupported value is specified.
LANGUAGE	String in the format `xx-XX`. Currently, the only supported value is `en-US`. An exception is raised if the value is not in the format `xx-XX`.
MAX_STATEMENTS	Integer Maximum number of concurrent requests that are made to The Weather Company through the connection. The value must be greater than or equal to 1. The default value is 15. An exception is raised if an unsupported value is specified.
CACHE_SIZE	Integer Number of results cached by the connection. To ensure current information is returned, caching is not performed for a request to the forecast on demand service. The value must be a greater than or equal to 0. 0 means no caching. Default value is 100 (MB of space). An exception is raised if an unsupported value is specified.
CACHE_TTL	Time to live in seconds for a result set in the cache. A result is removed when it's older than this value. The value must be greater than or equal to 1. The default value is 86400 (24 hours). An exception is raised if an unsupported value is specified.
CACHE_DIR	The folder into which results are cached. The default is the folder used by the Java runtime environment (`java.io.tmpdir`). The Cognos processes running on the computer must have read/write access to the folder. The folder is created if it doesn't exist. If the location is not accessible connections will fail.
QUERY_TIMEOUT	The number of seconds after which a query times out. The default value is 60 seconds. An exception is raised if an unsupported value is specified.
PROXY_HOST, PROXY_PORT	Host name and port of an HTTP caching service. Queries to The Weather Company server are REST (HTTP). You set these parameters to send requests to the HTTP caching service, which then sends the queries to the The Weather Company server.

Parameter	Description
FILTER_METADATA	Boolean Default value is false. When a new model (Framework Manager or data module) is created, the import includes metadata for all products that are available through The Weather Company server. If this value is true, then the metadata includes only the products that the API key is entitled to query. The API key is specified in the password in the connection string.

In the following example, only the objects that are available to The Weather Company API key associated with the signon are imported. A query can use up to 250 MB of storage.

```
jdbc:twc://?FILTER_METADATA=true,CACHE_SIZE=250
```

Adding a new connection

You can create a new connection for an existing data source.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Data Source Connections**.
2. Click the data source for which you want to add a new connection.

   Tip: To remove a data source connection, select its check box and click the delete button.
3. Click the new connection button .
4. In the name and description page, type a unique name for the connection and, optionally, a description and screen tip, and then click **Next**.
5. Proceed with steps 5 to 10 in "Creating a data source connection " on page 116.

Results

If you created a signon, you can now modify it or add more signons. For more information, see "Data source signons" on page 124.

Modifying an existing connection

You can add new data source connections or edit existing connections.

You can add multiple connections to an existing data source. For example, you want a data source to have two or more connections to the same database that have different properties, such as different timeout values or access permissions. You can also add connections to a data source that point to different databases, but the databases must contain the same schema.

When you create a data source connection, you can create a signon that the Everyone group can use to access the database. Later, you can modify who can use this signon or create more signons. For example, you can control access to data by setting the permissions for each data source connection. For more information, see "Set access permissions for an entry" on page 179.

To add or modify a data source connection, you must have access to the required capabilities to administer data sources, see Chapter 13, "Capabilities," on page 185.

If you are creating an Oracle, IBM Db2, or Microsoft SQL Server data source, you can include database commands in the connection information. For more information, see "Passing IBM Cognos context to a database" on page 128.

For information about setting the maximum number of data source connections available to the report server, see "Changing connection settings" on page 123.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Data Source Connections**.
2. Click the data source for which you want to modify the connection.
3. Click the set properties button ▤ for the connection you want to modify.
4. Click the **Connection** tab.
5. If you want to change the data source type, click an item in the **Type** drop-down list.
6. Click the edit icon ✎ to modify the connection string.
7. Proceed with steps 5 to 10 in "Creating a data source connection " on page 116.

Changing connection settings

You can set the maximum number of available data source connections, the duration for retaining connections, and how data source connections are reused.

Each instance of the report server has an established pool of database connections. The connections are reused for new requests that match the database, user, and password. Entries remain in the pool until they are idle for a timeout period and then are closed. Once a pool is full, no further connections are added. This results in a request failure.

PoolSize

Specifies the maximum number of data source connections available to the report server.

Timeout

Specifies the time duration for retaining connections. Connections are examined once per minute and any connection that has been inactive longer than the timeout value is removed.

Default: 900 seconds

Reusable Data Connections

Data source connections are reusable only when the database credentials of the connection match those of the new request. Inactive data source connections can be claimed by a new request. This occurs when the maximum number of connections has been reached and none of the inactive connections can be used by the new request. In this case, the oldest inactive connection is terminated and a new connection is created.

When the maximum number of connections is reached, and all are active, then additional requests fail. The server must be configured to ensure that the concurrent report requests do not exceed the request pool size.

For more information about report service requests, see "Maximum Number of Processes and Connections" on page 60.

Procedure

1. On each computer where IBM Cognos Analytics is installed, open the *install_location*/configuration/CQEConfig.xml.sample file in a text editor.

   Ensure that your editor supports saving files in UTF-8 format.
2. Find the Timeout and PoolSize parameters and edit them as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration company="Cognos" version="#.#"
rendition="###">
  <component name="CQE">
    <section name="DBConnectionPool">
      <!-- Description: Database connection timeout.
       Default is 900 seconds (15minutes) -->
      <entry name="Timeout" value="number_of_seconds"/>
      <!-- -->
      <!-- Description: Database connection pool size. -->
      <!-- Maximum number of connections managed by the report
```

```
           server. Default=50 -->
      <entry name="PoolSize" value="number_of_connections"/>
    </section>
  </component>
</configuration>
```

3. Save the file as `CQEConfig.xml` to the *`install_location`*`/configuration` directory.
4. Using IBM Cognos Configuration, stop and then restart the IBM Cognos service.

   For information about stopping services, see the *IBM Cognos Analytics Installation and Configuration Guide*.

Dynamic connection parameters in JDBC connections

A JDBC connection to a data source specifies a static set of values that are passed by the query engine to the JDBC driver.

Environments such as Apache Hive or Cloudera Impala can support features such as identity delegation that require dynamic values to be passed by the query engine. You can specify session variables in the **JDBC URL** and **Connection properties** fields. For example, the **JDBC URL** field can include the following name-value pair:

```
hive.server2.proxy.user=#$account.defaultName#
```

When the query engine creates a new database connection, it replaces session variables with their corresponding value. If a session variable doesn't exist, the variable name is removed without any value in its place, which can cause the driver to reject the connection.

Note: You cannot use macro functions. Only references to session variables are supported.

Data source signons

You add signons to data source connections so that users do not have to enter database credentials when they run reports.

When you create a signon, you specify the users and groups that can access the signon. The user ID and password that make up the signon must already be defined in the database.

You can modify an existing signon if the credentials used to log on to the database change, or if you want to change who can use the signon.

For data source configurations that require each user to have their own signon, it can be unwieldy to administer them all. For information on how users can manage their own data source credentials, see "Manage Your Own Data Source Credentials" on page 183.

Creating a signon

The data source connection signon must be defined so that the query service can automatically access the data.

About this task

A data source connection must have at least one signon that the query service can use to connect to the data source. If the data source connection has two or more signons, one of the signons must be named `Dynamic Cubes`. This signon will be used by the query service to connect to the data source.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Data Source Connections**.
2. Click the data source, and then click the connection to which you want to add a new signon.
3. Click the new signon button .

4. In the name and description page, type a unique name for the data source signon and, if you want, a description and screen tip, and then click **Next**.
5. Type the **User ID** and **Password** to connect to the database, and click **Next**.

   The **Select the users** page appears.
6. To add users and groups that can use the signon, and click **Add**.

   - To choose from listed entries, click the appropriate namespace, and then select the check boxes next to the users, groups, or roles.
   - To search for entries, click **Search** and in the **Search string** box, type the phrase you want to search for. For search options, click **Edit**. Find and click the entry you want.
   - To type the name of entries you want to add, click **Type** and type the names of groups, roles, or users using the following format, where a semicolon (;) separates each entry:

     namespace/group_name;namespace/role_name;namespace/user_name;

     Here is an example:

     Cognos/Authors;LDAP/scarter;
7. Click the right-arrow button and when the entries you want appear in the **Selected entries** box, click **OK**.

   Tip: To remove entries from the **Selected entries** list, select them and click **Remove**. To select all entries in a list, in the title bar for the **Name** list, select the check box. To make the user entries visible, click **Show users in the list**.
8. Click **Finish**.

   The new data source signon appears under the connection.

Modifying a signon

You can modify an existing signon.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Data Source Connections**.
2. Click the data source, and then click the connection for which you want to modify the signon.

   Tip: To remove a signon, select its check box and click the delete button.
3. Click the set properties button ▤ for the signon you want to modify.
4. Click the **Signon** tab.

   A list of users and groups that can use the signon appears.
5. If you want to change the user ID and password that make up the signon click **Edit the signon**, type the new credentials, and click **OK**.
6. If you want to add users or groups to the signon list, click **Add**, and choose how to select users and groups:

   - To choose from listed entries, click the appropriate namespace, and then select the check boxes next to the users, groups, or roles.
   - To search for entries, click **Search** and in the **Search string** box, type the phrase you want to search for. For search options, click **Edit**. Find and click the entry you want.
   - To type the name of entries you want to add, click **Type** and type the names of groups, roles, or users using the following format, where a semicolon (;) separates each entry:

     namespace/group_name;*namespace/role_name*;*namespace/user_name*;

     Here is an example:

     Cognos/Authors;LDAP/scarter;

7. Click the right-arrow button and when the entries you want appear in the **Selected entries** box, click **OK**.

   Tip: To remove entries from the **Selected entries** list, select them and click **Remove**. To select all entries in the list, select the check box for the list. To make the user entries visible, click **Show users in the list**.
8. Click **OK**.

Isolation levels

You can specify isolation levels for data sources.

The isolation level specifies how transactions that modify the database are handled. By default, the default object gateway is used. Not all types of databases support each isolation level. Some database vendors use different names for the isolation levels.

Queries that are executed by reports and analysis are intended to be read-only operations. The queries execute with a unit of work at the data source known as a transaction with either a default or administrator-defined isolation level. Report authors should not assume that queries that execute stored procedures commit any data written by the procedure. In some environments, changes made by a procedure may be committed due to features of the database. A stored procedure that is marked for-write in Framework Manager commits changes but can only be used by Event Studio.

If you need specific queries to run with different isolation levels, you must define different database connections.

For OLAP data sources, including SAP BW, the transaction unit of work is read-only.

The following isolation levels are in increasing order of isolation:

- Read Uncommitted

  Changes made by other transactions are immediately available to a transaction.

Table 44. Read Uncommitted database types and equivalent isolation levels

Database type	**Equivalent isolation level**
Oracle	Not applicable
Db2	Uncommitted read
Microsoft SQL Server	Read uncommitted
Sybase Adaptive Server Enterprise	Read uncommitted
Informix	Dirty read

- Read Committed

  A transaction can access only rows committed by other transactions.

Table 45. Read committed database types and equivalent isolation levels

Database type	**Equivalent isolation level**
Oracle	Read committed
Db2	Cursor stability
Microsoft SQL Server	Read committed

Table 45. Read committed database types and equivalent isolation levels (continued)

Database type	**Equivalent isolation level**
Sybase Adaptive Server Enterprise	Read committed
Informix	Committed read

- Cursor Stability

  Other transactions cannot update the row in which a transaction is positioned.

Table 46. Cursor stability database types and equivalent isolation levels

Database type	**Equivalent isolation level**
Oracle	Not applicable
Db2	Not applicable
Microsoft SQL Server	Not applicable
Sybase Adaptive Server Enterprise	Not applicable
Informix	Cursor stability

- Reproducible Read

  Rows selected or updated by a transaction cannot be changed by another transaction until the transaction is complete.

Table 47. Reproducible read database types and equivalent isolation levels

Database type	**Equivalent isolation level**
Oracle	Not applicable
Db2	Read stability
Microsoft SQL Server	Repeatable read
Sybase Adaptive Server Enterprise	Repeatable read
Informix	Repeatable read

- Phantom Protection

  A transaction cannot access rows inserted or deleted since the start of the transaction.

Table 48. Phantom protection database types and equivalent isolation levels

Database type	**Equivalent isolation level**
Oracle	Not applicable
Db2	Not applicable
Microsoft SQL Server	Not applicable

Table 48. Phantom protection database types and equivalent isolation levels (continued)

Database type	Equivalent isolation level
Sybase Adaptive Server Enterprise	Not applicable
Informix	Not applicable

- Serializable

  A set of transactions executed concurrently produces the same result as if they were performed sequentially.

Table 49. Serializable database types and equivalent isolation levels

Database Type	Equivalent isolation level
Oracle	Serializable
Db2	Repeated read
Microsoft SQL Server	Serializable
Sybase Adaptive Server Enterprise	Serializable
Informix	Not applicable

Passing IBM Cognos context to a database

Database administrators want to know details about applications that connect to their database systems. This information can be used for auditing, workload management, and troubleshooting.

The information about IBM Cognos applications can be passed to the databases by using the data source connection command blocks.

Depending on the query mode, command blocks support these data source connections:

- In Compatible Query Mode (CQM), ORACLE (OR), IBM Db2 (D2), Teradata (TD), SQL Server (SS), and Netezza (NZ).
- In Dynamic Query Mode (DQM), all data source connections that are supported via JDBC.

For more information, see "Command blocks" on page 128.

For Db2, connection attributes can also be used as a means of passing information about the Cognos applications. For more information, see "Using IBM Db2 CLI Connection Attributes for Db2 " on page 134.

IBM Cognos software can provide information about its reporting applications and users who access the applications, including the default set of information about authenticated users that is retrieved from authentication providers. The information can be extended by specifying custom namespace mappings in IBM Cognos Configuration. For more information about the mappings, see the *IBM Cognos Analytics Installation and Configuration Guide*.

Command blocks

Connection command blocks are intended to change the session state on a connection that is opened on a data source. The statements that can be used in the command blocks depend on the statements supported by database vendors and user's permissions for those statements. Statements in command blocks can be parameterized by using IBM Cognos session variables and macro functions.

Command blocks are executed as IBM Cognos software opens and closes database connections or sessions on connections. You can use command blocks to run native SQL commands, for example, to run a stored procedure when a session is opened.

The following types of command blocks are available:

- **Open connection commands**
- **Open session commands**
- **Close session commands**
- **Close connection commands**

As an administrator, you must know when a command block is executed for a database connection. It is often best to define the database statements in an open session command block. Open database connections execute less frequently because IBM Cognos pools and reuses database connections. Use open session command blocks if the application context of a database connection changes frequently.

Command blocks should not include Cognos session variables or macros that change values frequently. These types of session variables or macros increase the command block execution frequency and number of data source caches, and reduce the result set cache reuse.

When creating your command blocks, consider the following database connection settings:

- What are the database connection pool settings specified for the report servers in the `CQEConfig.xml` file?
- Does the database have aggressive idle connection timeout settings?
- Does the query engine have aggressive idle connection timeout settings?
- Is the period between requests longer than the timeout settings?
- Are there any requests routed to different report servers that must create new connections?

The following diagram shows an example of interaction between the four types of command blocks. The interaction starts when a query for user one arrives. It is assumed that a connection to the database does not exist.

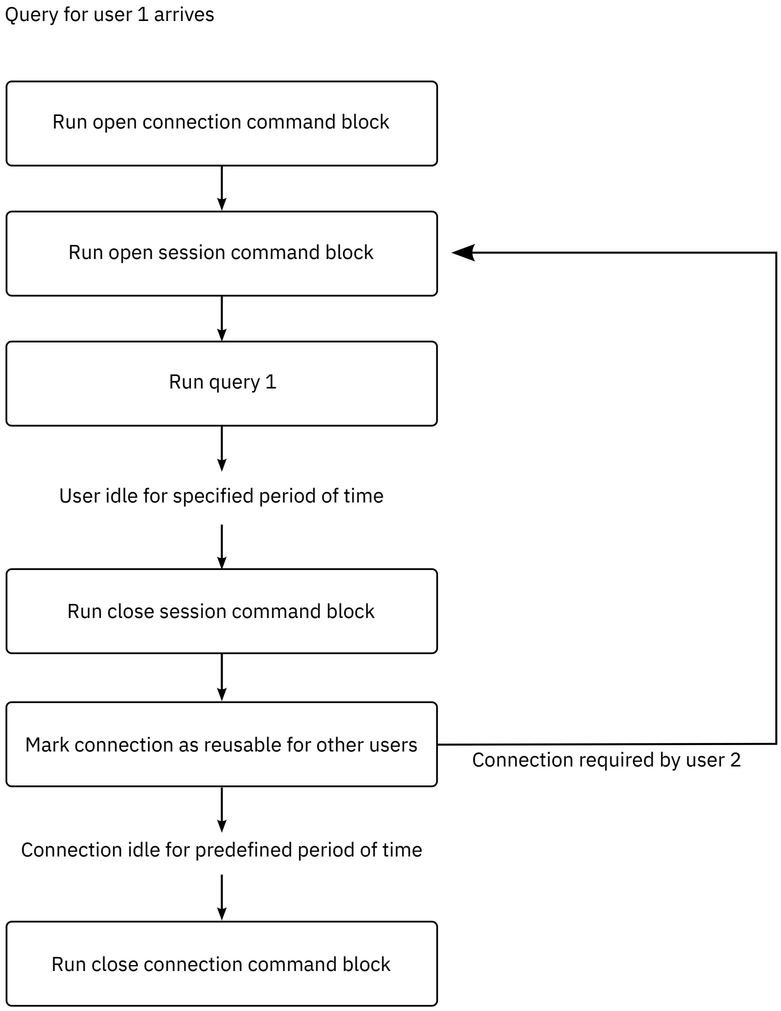

Query for user 1 arrives
Run open connection command block
Run open session command block
Run query 1
User idle for specified period of time
Run close session command block
Mark connection as reusable for other users
Connection required by user 2
Connection idle for predefined period of time
Run close connection command block

Figure 3. Example of interaction between command blocks

Macro functions

The macro functions available in IBM Cognos software can provide information in a command block about users and reporting application objects, such as packages, reports, or queries. All macro functions can return values when referenced from a command block, which allows for application context to be passed to the database from a command block. Macro functions that reference parameter maps in a model can also be used.

Considerations

- You cannot test the command blocks for connections that use the **Test the connection** link on the connection properties page. If Software Development Kit is installed, you can ensure that your XML code validates against the schema file *`c10_location`*`/webapps/p2pd/WEB-INF/classes/DataSource.xsd`.
- The command structure is the same for all data sources. However, the specific database commands can vary depending on which database you are using. In this section, the examples use Oracle and IBM Db2 commands.
- The commands in the blocks are vendor-specific and must be enclosed in the `<sqlCommand>` tag.
- Depending on your settings, the query engine might open new connections more rapidly than in a normally loaded application, which might create a false impression that information is reset for each request that is executed. To control this behavior, consider using the **(DQM) Cache is sensitive to connection command blocks** governor. For more information, see the topic about Framework Manager governors for the dynamic query mode in the *IBM Cognos Framework Manager User Guide*.

Example - Open Connection Command Block

Here is an example of using an open connection command block to set French as the language for an Oracle connection.

```
<commandBlock>
  <commands>
   <sqlCommand>
    <sql>ALTER SESSION SET NLS_LANGUAGE = FRENCH</sql>
   </sqlCommand>
  </commands>
</commandBlock>
```

Example - Close Connection Command Block

Here is an example of using a close connection command block to reset the language to English before disconnecting from an Oracle database.

```
<commandBlock>
  <commands>
   <sqlCommand>
    <sql>ALTER SESSION SET NLS_LANGUAGE = ENGLISH</sql>
   </sqlCommand>
  </commands>
</commandBlock>
```

Example - Passing Request Information

Here is an example of a IBM Db2 open session command block which, when executed, generates a set of parameters to be passed to a user-defined procedure.

The example combines macro functions to ensure that the values are generated as valid string literals and string concatenations with some literals. The modelPath variable is an example of how to access properties of a request that was processed when the block was executed.

```
<commandBlock>
    <commands>
        <sqlCommand>
            <sql> CALL myproc(#sq($current_timestamp) + ',' +
            sq($machine) + ',' +
            sq(#$modelPath}#) + 'Constant1''''#)
            </sql>
        </sqlCommand>
    </commands>
</commandBlock>
```

After the macro is expanded, the database administrator obtains the following information about the query:

CALL myproc('2009-05-27 08:13:33.425-05:00','USERCOMPUTERNAME','/content/package[@name=''EAPPS'']/model[@name=''model'']', 'Constant1', '')

Example - Using Parameter Maps

This IBM Db2 example shows how a database administrator can obtain model information.

An application standard might be to define a parameter map that appears in all models. The parameter map defines context information about the IBM Cognos application. This approach requires that any application that uses the connection must provide this information to avoid errors.

```
<commandBlock>
    <commands>
        <sqlCommand>
            <sql> CALL myproc(#sq($APP_INFO{APPNAME}) + ',' +
             sq($APP_INFO{'APPMAJOR'}) + ',' +
             sq($APP_INFO{'APPMINOR'}) + ',' +
             sq($APP_INFO{'APPCONTACT'}) + ', ''Constant1'' '#))
            </sql>
        </sqlCommand>
    </commands>
</commandBlock>
```

After the macro is expanded, the database administrator obtains the following information about the query:

```
CALL myproc('ApplicationName','10','1','TradingApp@email.com',
'Constant' )
```

Example - Passing Authentication Provider Details

This IBM Db2 example shows how to include session information, sourced from an authentication provider, into the information passed to the database.

The command block invokes the Db2 procedure SYSPROC.WLM_SET_CLIENT and passes down values derived from the available session variables. This information can be used by database administrators when defining workload management rules in the database that give higher priority to specific user groups when a database connection is shared by multiple user groups.

```
<commandBlock>
    <commands>
        <sqlCommand>
            <sql> CALL SYSPROC.WLM_SET_CLIENT_INFO
            (#$account.personalInfo.userName#,
             'UserComputerName',
#$account.parameters.var1#, 'ApplicationName', 'AUTOMATIC')
            </sql>
        </sqlCommand>
    </commands>
</commandBlock>
```

Example - Using Command Blocks for Proxy Connections

If you are using proxy connections, you can use an existing idle connection with signons for proxy connections.

The physical connection can be used by more than one user. Because the proxy connections run on top of the existing physical connection, fewer physical connections are required.

To create a proxy connection, you create open session command blocks in XML.

The following is a simple example of an open session command block that creates a proxy connection for User1 (Oracle) or switches to User1 (Db2). Note that the sessionStartCommand can only be used with Oracle and Db2.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>
```

Another example is a macro that can be substituted if authentication userNames are equivalent to the proxy userid or trusted context user.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>#$account.personalInfo.userName#
          </value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>
```

The following is a simple example of a close session command block for a proxy session. The current proxy connection is terminated. Note that sessionEndCommand ends an OCI_session in Oracle and switches the user back to the trusted context owner for Db2.

```
<commandBlock>
  <commands>
    <sessionEndCommand>
      <arguments/>
    </sessionEndCommand>
  </commands>
</commandBlock>
```

Example - Using Command Blocks for Virtual Private Databases for Oracle

Typically, Oracle uses signons to determine the database information that users can access. A virtual private database determines which users can access which information, without further signon information required.

You create a command block for the connection using macros that are substituted at run time for the logged on user. The macros identify the user so that the user need not re-enter signon information.

If all users who access the database are defined as database users and user accounts are used for connections, you can set up the context automatically when the connection is established. For example, the macro can be substituted for the userName.

The XML command block stores a series of commands that are run in the stated sequence. This may include the commands that are described in Appendix E, “Schema for Data Source Commands,” on page 433.

The following example shows an XML command block for a virtual private database.

This command block sets up a context (virtual private database) within the connection based on the passed parameter. The passed parameter is retrieved from the environment, which is related to the user's logon at the portal level. These variables can be modified in the configuration tool. Their values are user specific and obtained using the security control mechanism (CAM).

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql>BEGIN PKG_COUNTRY_CONTEXT.SP_SET_COUNTRY1
       (#$account.parameters.var1#);
END;</sql>
    </sqlCommand>
  </commands>
</commandBlock>
```

This example shows account parameter substitution. You must specify account information as custom properties. For information about session properties, see the Framework Manager *User Guide*.

Note: Command blocks for Oracle proxy connections and virtual private databases at the data source level apply to all connections to that data source.

Adding command blocks while creating a data source

You can add command blocks when you create data sources.

By default, connections acquire properties from the parent data source. You can modify individual connections later.

Procedure

1. On the **Configuration** tab in Cognos Administration, start creating a data source for a database that supports command blocks.
2. In the specify commands page, click **Set** next to the command that you want to specify.
3. In the set command page, add the XML code for the command block, and click **OK**.

   Tip: For IBM Db2 or Microsoft SQL Server, you can add a command block only for opening a session.
4. Continue adding command blocks, as needed, and then click **Finish**.

Adding or modifying command blocks for a connection

You can add, change, or remove command blocks for specific data source connections.

Connections acquire properties from their parent data source. If you add a command block for a data source, that command block is available to all connections for that data source.

Procedure

1. On the **Configuration** tab in Cognos Administration, choose one of the following options:
   - Access the data source properties if you want to modify the command blocks for all connections that this data source has.
   - Access the data source connection properties if you want to modify the command blocks for one connection.
2. Click the **Connection** tab, and in the **Commands** section, perform one of the following tasks:
   - To add the command block, click **Set** for one of the available command types and paste the XML code for the command block in the **XML database commands** box.
   - To modify a command block, click **Edit** for the selected command and modify or remove the XML code for the command block from the **XML database commands** box.

   You can reset command blocks by selecting the **Reset to parent value** or **Clear** check boxes.

   Tip: For IBM Db2 or Microsoft SQL Server, you can add command blocks only for opening a session.
3. Continue adding or modifying command blocks, as needed, and then click **Finish**.

Using IBM Db2 CLI Connection Attributes for Db2

Db2 Call Level Interface (Db2 CLI) is a callable SQL interface to Db2 LUW, Db2 for z/OS and Db2for I). IBM Cognos Analytics can change some of the Db2 CLI connection attributes to pass application context to Db2 in a format acceptable to the components of IBM Optim Integrated Data Management.

This information can later be retrieved from Db2 special registers using SQL statements.

To enable this functionality, you must modify a configuration file on each IBM Cognos report server computer that is configured in your IBM Cognos environment. Because this functionality is set up at the query level, the information that is associated with the connection attributes is automatically updated every time that the report runs.

The following list shows the Db2 CLI connection attributes that can be changed by IBM Cognos Analytics, and the type of information that these attributes can pass to Db2:

- SQL_ATTR_INFO_USERID

  Specifies the name of the user running a report.
- SQL_ATTR_INFO_WRKSTNNAME

  Specifies the address of the system on which the user's browser is installed.
- SQL_ATTR_INFO_APPLNAME

Specifies the package name associated with the query. If the string is longer than 32 characters, it overflows to $SLOT2 in the accounting string.

- SQL_ATTR_INFO_ACCTSTR

  Specifies the prefix or string that associates the request with IBM Cognos Analytics. The values are:

Table 50. Using Db2 CLI connection attributes for Db2

Value	Description
COG	Associates the request with IBM Cognos products in IBM Optim Integrated Data Management.
ccc	Associates the request with an IBM Cognos solution.
vr	Specifies the version of IBM Cognos product
Additional accounting information	This information is divided into the following fields (slots): – $SLOT2 - $packageName (overflow section for $SLOT1) – $SLOT3 - $reportName – $SLOT4 - $queryName – $SLOT5 - $reportPath Each slot has a fixed length that accepts strings containing no more than 46 bytes, padded with blanks if necessary. Because report paths, model paths, and so on, are often long, the strings may be shortened to adjust to the space limitations. **Note:** In Db2, values passed to the API cannot contain single quote characters, which are converted to spaces. If the character set encoding is using multiple bytes per character, the character is converted to "?" in order to avoid overflow. This is important where Unicode is used and a character may require more than 2 bytes.

Procedure

1. If you connect to your database with the compatible query mode, do the following steps:

   a) In the *install_location*/configuration directory, make a copy of the CQEConfig.xml.sample file and rename it to CQEConfig.xml.

   Tip: If the CQEConfig.xml file was used for other purposes, for example to disable session caching, it might exist in the *install_location*/configuration directory. In this situation, use the existing CQEConfig.xml file to perform the remaining steps.

   b) Open the *install_location*/configuration/CQEConfig.xml file in an editor.

   Ensure that your editor supports saving files in UTF-8 format.

   c) Locate the <section name="QueryEngine"> element and add the DB2WFM entry with a value of 1, as shown in the following example:

```
<section name="QueryEngine">
      <entry name=" DB2WFM" value="1"/>
</section>
```

   To disable this functionality, set the value to zero.

2. If you connect to your database with the dynamic query mode, do the following steps:

   a) In the *install_location*/configuration directory, make a copy of the xqe.config.xml file and rename it to xqe.config.xml.backup.

b) Open the *`install_location`*`/configuration/xqe.config.xml` file in an editor.

Ensure that your editor supports saving files in UTF-8 format.

c) Locate the `<setConnectionAttributes enabled="false">` element and change its value to `"true"`, as shown in the following example:

```
<setConnectionAttributes enabled="true">
```

To disable this functionality, set the value to `"false"`.

3. Save the file.
4. Repeat the steps for each report server computer that is configured in your IBM Cognos environment.
5. Restart the IBM Cognos service.

Using application context in Dynamic SQL

Database server administrators can log and analyze the dynamic SQL workload generated by IBM Cognos software.

As an IBM Cognos administrator, you can define a custom string that includes application context that is added as a comment marker within SQL generated by the application. You can use literals, macros, and session variables, such as a user name, server name, qualified report path, and so on, to customize the comment generated by Cognos software.

The Database administrator should check to see if their database client strips comments from statements prior to sending to the server. This option is probably configurable, check with your database client provider.

By using the applicable session variables, you can configure the format of the string for specific tools and products that can extract comments from dynamic SQL. IBM Cognos software includes the comments within any dynamic SQL it generates to a Relational Database Management System (RDBMS) if the vendor supports this functionality.

Use the CQEConfig.xml.sample file included with the product to customize the string specifications. The macro in this file shows the default entries that IBM Cognos software uses for generating the comments. However, you can add other entries as well.

The following example shows kinds of session variables you can specify in the macro in the CQEConfig.xml.sample file:

```
<configuration company="Cognos" version="0.1" rendition="cer2">
    <component name="CQE">
        <section name="QueryEngine">
            <entry name="GenerateCommentInNativeSQL" value="1"/>
            <!-- ( default(off)=0, on=1) -->
            <entry name="GenerateCommentInCognosSQL" value="1"/>
            <!-- ( default(off)=0, on=1) -->
            <!-- The content of the comments is controlled with two entries, their
defaults are specified in the value attribute -->
            <entry name="NativeCommentMacro" value="# 'NC user=' + $account.defaultName
+ 'report=' + $report + 'start=' + $startTime + 'modelPath='  +
$modelPath + 'reportPath=' + $reportPath + ' queryName=' + $queryName
+ ' REMOTE_ADDR=' + $REMOTE_ADDR + 'HTTP_HOST=' + $HTTP_HOST + 'SERVER_NAME='
+ $SERVER_NAME +' requestID=' + $requestID + 'sessionID=' + $sessionID
#"/>
            <entry name="CognosCommentMacro" value="# 'CC user=' + $account.defaultName
+ 'report=' + $report + 'start=' + $startTime + 'modelPath='  +
$modelPath + 'reportPath=' + $reportPath + ' queryName=' + $queryName
+ ' REMOTE_ADDR=' + $REMOTE_ADDR + 'HTTP_HOST=' + $HTTP_HOST + 'SERVER_NAME='
+ $SERVER_NAME +' requestID=' + $requestID + 'sessionID=' + $sessionID
#"/>
        </section>
    </component>
</configuration>
```

At run time, the macro used in the previous example would add the following comment to the automatically-generated SQL, or native SQL:

```
/* CC user=Anonymous report=REPORT1
start=2008-08-28T01:59:35.403Z modelPath=/content/package
[@name='New Package']/model[@name='model']
reportPath=/content/package[@name='New Package']/report[@name='REPORT1']
queryName=Query1 REMOTE_ADDR=127.0.0.1 HTTP_HOST=localhost
SERVER_NAME=localhost
requestID=wq2lshM9jGhqdMj9h92MqlqvdMlhyMlGq9lyG9sq
sessionID=010:0d159165-745a-11dd-ac9f-b741aeca4631:2789499633
*/
select distinct
       ALL_TIME.CALENDAR_WEEKDAY  as  CALENDAR_WEEKDAY
 from
       EAPPS..EAPPS.ALL_TIME ALL_TIME
```

Not all information in the generated comment is meaningful in all situations. The request and session ID information provides a link to the auditing facility, perfQFS performance information, and other traces in IBM Cognos. However, the name of a query in a report and the report itself may be meaningless, for example, when a user is performing an ad-hoc query or analysis as opposed to running a saved query, analysis or report.

By default, an anonymous user cannot see all session variables in the generated comments.

Adding application context for Dynamic Query Mode

To use comments in SQL for dynamic query mode you can configure the xqe.config.xml file, located in install_location/configuration.

You edit the following elements in the <queryPlanning> element.

```
<generateCommentsInNativeSQL enabled="true"/>
<NativeCommentMacro value="#'user=' + $account.defaultName + ' reportPath='
 + $reportPath +' queryName=' + $queryName + ' REMOTE_ADDR=' + $REMOTE_ADDR
 + ' SERVER_NAME=' + $SERVER_NAME + ' requestID=' + $requestID#"/>
```

Add Application Context to Dynamic SQL

Database server administrators can configure the CQEConfig.xml.sample file to log and analyze the dynamic SQL workload generated by IBM Cognos software. For Dynamic Query Mode, administrators configure the xqe.config.xml file.

Procedure

1. In the `*install_location*/configuration` directory, make a copy of the `CQEConfig.xml.sample` file and rename it to `CQEConfig.xml`.

   Tip: If the `CQEConfig.xml` file was used for other purposes, for example to disable session caching, it might already exist in the `*install_location*/configuration` directory. In this situation, use the existing `CQEConfig.xml` file to perform the remaining steps.
2. Open the `*install_location*/configuration/CQEConfig.xml` file in an editor.

   Ensure that your editor supports saving files in UTF-8 format.
3. Locate and uncomment the lines of code that begin with:

   `entry name="GenerateCommentInNativeSQL"...`

   `entry name="GenerateCommentInCognosSQL"...`

   `entry name="NativeCommentMacro"...`

   `entry name="CognosCommentMacro"...`
4. If you want, you can modify `NativeCommentMacro` and `CognosCommentMacro` by specifying the required parameter values and deleting the parameters that you do not need.

If you leave a parameter value empty, the parameter will not appear in the generated comment.

5. Save the `CQEConfig.xml` file.
6. Restart the IBM Cognos service.

Deploying updated PowerCubes

After you rebuild or update a PowerCube, you can use various methods to deploy the cube to the production environment.

To deploy an updated IBM Cognos Transformer PowerCube, use the Copy and Activate method in IBM Cognos Transformer (the recommended method), or copy the PowerCube yourself, and use the `pcactivate` command-line utility.

To deploy an updated Series 7 Transformer PowerCube, you must copy the PowerCube first. Then, use the `pcactivate` command-line utility to activate the cube.

For more information, see the section Copy and Activate a Newer Version of a Published PowerCube in the IBM Cognos Analytics Transformer *User Guide*.

Procedure

1. Copy the Transformer PowerCube to the production environment.

   - The name of the destination directory in the production environment must be the same as the PowerCube name. For example, if the cube is named `production.mdc`, the destination directory must be named production.
   - The destination directory must be in the same directory as the PowerCube. For example, if the data source connection specifies that the PowerCube location is `D:\Cubes\production.mdc`, the destination directory, named production, must be `D:\Cubes\production`.

   For example, copy the PowerCube to `D:\Cubes\production\production.mdc`.
2. At the command-line prompt, type the `pcativate` command using the following syntax:

   ```
   pcactivate cube_name.mdc
   destination_location destination_location
   ```

   You can type more than one destination location.

   For example, type

   - `pcactivate TheCube.mdc d:\deploy\cubes`
   - `pcactivate production.mdc D:\Cubes`
   - `pcactivate sales.mdc \\server_1\cubes \\server_2\cubes`
   - `pcactivate "Production Cube.mdc" "install_location\webcontent\cubes"`

   Note: If you include a path in the `cube_name` parameter, the path is removed and ignored.

Securing data sources

You can secure data sources using IBM Cognos security or data source-specific security.

The IBM Cognos security for a data source does not override security policies that already exist for the data source. For example, for IBM Cognos cubes, the security may be set at the cube level. For Microsoft Analysis Server data sources, the security may be set using cube roles.

Depending on the data source, one or more of the following authentication methods are available:

- No authentication

  IBM Cognos software logs on to the data source without providing any signon credentials.
- IBM Cognos service credentials

IBM Cognos software logs on to the data source using the logon specified for the IBM Cognos service. Users do not require individual database signons. For production environments, however, individual database signons are generally more appropriate.

- An external namespace

  IBM Cognos software logs on to the data source with the credentials used to authenticate to the specified authentication namespace. The namespace must be active, users must be logged on prior to accessing the data source, and the authentication credentials used for the namespace must be relevant for the data source authentication.

  If you select the **Transform user identifier** check box, the Cognos Analytics server removes the domain name from the user ID that is returned by the external namespace before establishing the database connection. The current implementation supports the user ID transformation for the following formats only:

  - *`domain_name\user_id`* - after transformation the user id would be *`user_id`*
  - `user_id@domain_name` - after transformation the user id would be `user_id`

  If you want to keep the domain name as part of the user ID, ensure that this check box is clear.

All data sources also support data source signons defined for the Everyone group or for individual users, groups, or roles, see Chapter 11, “Users, Groups, and Roles,” on page 167. If the data source requires a signon, but you do not have access to a signon for this data source, you are prompted for authentication each time you access the data source.

Chapter 7. Query Service Administration

The query service supports the IBM Cognos Analytics dynamic query mode.

For more information, see Chapter 6, “Data sources and connections,” on page 89.

Using Cognos Administration, you can perform the following query service administration tasks:

- set query service properties
- administer query service caching

In addition, you can set the audit logging level for the query service. For more information, see “Setting up audit reporting” on page 17.

You must have the required permissions to access **IBM Cognos Administration**. For more information, see Chapter 12, “Access Permissions and Credentials,” on page 173. You must also have the query service administration capability. For more information, see Chapter 13, “Capabilities,” on page 185.

Setting query service properties

The query service uses a number of environment, logging, and tuning configuration settings.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, select **System**.
2. In the **Scorecard** section, select the **All servers groups** view.

   Tip: To select a different view, in the **Scorecard** section, click the drop-down menu for the current view.
3. Click the server group under **System**.
4. From the **Actions** menu for the **QueryService - *dispatcher_name***, click **Set properties**
5. Click the **Settings** tab.
6. In the **Value** column, type or select the values for the properties that you want to change. The following list describes the properties that you can set for the query service.

   Advanced settings

   Click **Edit** to specify advanced configuration settings. Because an entry acquires advanced settings from a parent, editing these settings overrides the acquired advanced settings. For information about types of advanced settings, see the *IBM Cognos Analytics Administration and Security Guide*.

   Dynamic cube configurations

   Click **Edit** to add dynamic cubes to the query service.

   Audit logging level for query service

   Select the level of logging that you want to use for the query service.

   Enable query execution trace

   A query execution trace (run tree trace) shows queries that run against a data source. You use the trace to troubleshoot query-related issues.

   You can find execution trace logs in the following location: `install_location/logs/XQE/reportName/runtreeLog.xml`

   You can view and analyze these log files using IBM Cognos Dynamic Query Analyzer. For more information, see the *IBM Cognos Dynamic Query Analyzer User Guide*.

   Enable query planning trace

   Query plan tracing (plan tree) captures the transformation process of a query. You can use this information to gain an advanced understanding of the decisions and rules that are executed to produce an execution tree.

The query planning trace is logged for every query that runs using dynamic query mode. You can find planning trace logs in the following location: `*install_location*/logs/XQE/*reportName*/plantreeLog.xml`

Since planning logs are large, there is an impact on query performance when this setting is enabled.

Generate comments in native SQL
Specifies which reports are generating the SQL queries in the database.

Write model to file
Specifies whether the query service will write the model to a file when a query runs. The file is used only for troubleshooting purposes. Modify this property only with the guidance of IBM Software Support.

You can find the file in the following location: `*install_location*\logs\XQE\model\*packageName*.txt`

Idle connection timeout
Specifies the number of seconds to maintain an idle data source connection for reuse.

The default setting is 300. Valid entries are 0 to 65535.

Lower settings reduce the number of connections at the expense of performance. Higher settings might improve performance but raise the number of connections to the data source.

Do not start dynamic cubes when service starts
Prevents the dynamic cubes from starting when the query service starts.

Dynamic cube administration command timeout
Specify the amount of time to wait for a resource to be available for a dynamic cubes administration action. This action is canceled if the time period is exceeded.

Tip: Setting this value to zero causes the command to wait indefinitely.

Minimum query execution time before a result set is considered for caching
Specify the minimum amount of time to wait for a query before caching the results.

This setting only applies to dynamic cubes.

Initial JVM heap size for the query service
Specifies the initial size, in MB, of the Java Virtual Machine (JVM) heap.

JVM heap size limit for the query service
Specifies the maximum size, in MB, of the JVM heap.

Initial JVM nursery size
Specifies the initial size, in MB, that the JVM allocates to new objects. The nursery size is automatically calculated. You do not need to change the setting unless IBM Cognos customer support recommends a change.

JVM nursery size limit
Specifies the maximum size, in MB, that the JVM allocates to new objects. The nursery size is automatically calculated. You do not need to change the setting unless IBM Cognos customer support recommends a change.

JVM garbage collection policy
Specifies the garbage collection policy used by the JVM. You do not need to change the setting unless IBM Cognos customer support recommends a change.

Additional JVM arguments for the query service
Specifies other arguments that control the Java Virtual Machine (JVM). The arguments may vary depending on the JVM.

Number of garbage collection cycles output to the verbose log
Specifies the number of garbage collection cycles to be included in the verbose garbage collection. This controls the maximum size of the log file. Consult with IBM Cognos customer support to increase the setting and collect more logs.

Disable JVM verbose garbage collection logging
Controls JVM verbose garbage collection logging. You do not need to change the setting unless IBM Cognos customer support recommends a specialized change.

7. Start or restart the query service.

Results

A summary of the query service properties is displayed in the **Settings - Query Service** pane.

Query Service Caching Administration

Caching reuses previously executed results and, when possible, avoids new queries to the database.

Caching can improve performance when reports are re-run with small modifications, analyses are performed within the same cube, and repetitive master-detail requests are performed for large reports. The cache maintains the security permissions of the user who executes the request.

For more information about how the cache works, see The Cognos BI 10.1.1 Dynamic Query Cookbook (https://developer.ibm.com/tutorials/the-cognos-bi-1011-dynamic-query-cookbook/).

Clear everything in the cache

To avoid using outdated data that might be stored in the cache, you can clear the cache.

You might want to clear the cache manually if your data source metadata changes infrequently or if you want to clear the cache in between automatically scheduled cache clearing. When you clear the cache using the following steps, it clears everything in the cache.

If you want to clear the cache for a specific data source, catalog, or cube, create a query service administration task. You might also want to create a query service administration task if your data source metadata changes regularly. For example, you might want to set a schedule to clear the cache hourly, daily, or weekly. For more information, see "Creating and scheduling query service administration tasks" on page 144.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Query Service Caching**.
2. Select the server groups for cache clearing.
3. Click **Clear cache**.

   The status of the **Clear cache** command is displayed.

   If a cache is being used by one or more pending reports or queries, it is internally flagged as "stale" by this command and is automatically cleared as soon as this usage completes.
4. Click **Close**.

Analyzing cache usage

You can analyze cache usage by producing a time-stamped XML file showing the state of specified cube caches (number of cache hits and cache misses for different levels of a cube).

This is useful to find out which cubes are in the cache at any point in time. The file includes a list of the data source name, catalog name and cube name for cubes that are currently cached. This can help you decide when to clear the cache.

The report is stored in the *c8_location*/logs directory. The filename has the format SALDump_*prefix_datasource name_category name_cube name_timestamp*.xml.

You can also schedule the cache state writing to run automatically. For more information, see "Creating and scheduling query service administration tasks" on page 144.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Query Service Caching**.
2. Select the server groups for cache clearing.
3. Click **Write cache state**.

   The status of the **Write cache state** command is displayed.
4. Click **Close**.

Creating and scheduling query service administration tasks

Administrators can create and schedule query service tasks for data sources. Query service tasks control one or more cubes by clearing, writing, or refreshing its cache. For dynamic cubes, you can also schedule when cubes start, stop, or restart, and refresh security.

- schedule cache clearing and clear the cache to control memory usage by a specific data source or cube
- schedule the generation of a time-stamped report (write cache state)

You can also clear the entire cache manually and write the cache state to a report manually.

For more information, see “Clear everything in the cache” on page 143 and “Analyzing cache usage” on page 143.

You can create query service administration tasks and run them on demand. You can run them at a scheduled time Chapter 18, “Schedule Management,” on page 247 or based on a trigger, such as a database refresh or an email “Trigger-based Entry Scheduling” on page 262. You can schedule them as part of a job “Using jobs to schedule multiple entries” on page 260. You can also view the run history of query service administration tasks “Viewing the run history of entries” on page 243.

Before you begin

When you create and schedule tasks for dynamic cubes, you need to schedule start and stop tasks for source cubes and virtual cubes separately. There are other factors to consider when scheduling start and stop tasks for dynamic cubes:

- Source cubes that are a part of a virtual cube must be scheduled to start first.
- If source cubes are part of a virtual cube, then the virtual cube must be scheduled to stop before the source cubes.
- You need to provide enough time for source cubes to start before scheduling a virtual cube to start. The same consideration must be made when you schedule virtual and source cubes to stop.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Content Administration**.
2. Click the New Query service administration task button .
3. Specify a name, description, screen tip, and location. Click **Next**.
4. Select an operation, either **Clear Cache** or **Write Cache State**.
5. For Oracle Essbase and SAP BW data sources, enter the data source, catalog, and cube. Click **Next**.

   Enter an asterisk (*) as a wildcard to specify all.
6. For Dimensionally-Modeled Relational (DMR) data sources, enter either the name of a package name or the name of a data source. If you specify a data source name and chose the **Clear Cache** operation, the cache is cleared for all packages that involve that data source.
7. For dynamic cube tasks, select the **Server Group**, **Dispatcher**, and **Cubes**, and then click **Next**.
8. Choose the action that you want:

   - To run the task now or later, click **Save and run once** and click **Finish**. Specify a time and date for the run, and then click **Run**. Review the run time and click **OK**.

- To schedule the task at a recurring time, click **Save and schedule** and click **Finish**. Then, select frequency and start and end dates. Click **OK**.

  Tip: To temporarily disable the schedule, select the **Disable the schedule** check box.

  Note: To view the schedule status, see "Managing scheduled activities" on page 259.
- To save the task without scheduling or running, click **Save only** and click **Finish**.

What to do next

You must remember to delete a scheduled task if you delete the associated cube from the query service. Otherwise, your scheduled tasks will point to nonexistent cubes.

Query service command-line API

You can manage the cache manually or automatically with a command-line API in addition to using IBM Cognos Administration.

The command-line utility is in the `*install_location*\bin` directory and is called **`QueryServiceAdminTask.sh`** or **`QueryServiceAdminTask.bat`**, depending on your operating system.

Type `QueryServiceAdminTask -help` in a command shell to display instructions on how to use the utility.

The command-line utility makes an immediate task request and does not use the job scheduler and monitoring service. As a result, commands affect only the IBM Cognos Analytics server on which they are run.

Queries on uploaded files and data sets

Queries on uploaded files and data sets are processed by the **Query service** and the **Compute service**. This type of co-processing increases performance of queries.

The **Compute service** processes the queries entirely or partially, and returns the result to the query service. Potentially, the whole query can be processed by the **Compute service**, and the query service might only need to perform additional, local processing of the result.

Tip: The **Compute service** and **Query service** reside on the same computer, and by default communicate with each other by using an ephemeral port requested from the operating system.

Upgrading data to the new Parquet format

The Parquet format that is used to store 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 the **Compute service** performance gains. If a query uses data that wasn't converted, the query service internally initiates the conversion 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 that are run by the compute service use the converted data.

For more information, see the upgrade section in the *IBM Cognos Analytics Configuration Guide*.

Best practices for improving query performance on uploaded files and data sets

Use the following best practices when working with queries based on uploaded files and data sets:

- Save frequently calculated expressions as columns.

  This practice reduces the amount of expression evaluation at run time. Projecting, comparing, and sorting simple column references and simple values (literals) is more efficient than evaluating expressions.

- Avoid storing large numbers of columns that are never used by queries.

  While data is both compressed and encoded to reduce the amount of storage, it’s still recommend to avoid storing redundant or unnecessary columns.

- Sort the input on the column that is most frequently used in filters.

  For large uploaded files and data sets, sorting the input can enhance the evaluation of predicates. Sorting the data on the common column that is used in a filter, for example `Country` or `Store`, groups rows with the same value. If a query includes predicates on that column, the query can determine more efficiently which blocks of data it can ignore as it navigates the data. Use the sort option when creating a data set, and sort the input prior to uploading a file.

Data types to store data from uploaded files and data sets

The data in uploaded files and data sets is stored in the following data types:

- All integer types (small, integer, and bigint) are stored as bigint.
- All approximate numeric types (real, float, and double) are stored as double.
- All precise numeric values are stored as decimal to the maximum precision of 38.
- All character types (char, nchar, varchar, nvarchar, clob, nlclob) are stored as national varchar with no maximum precision.
- All temporal types (date, timestamp, time, timestamp/time with time zone) are stored as timestamp.
- Interval types are stored in a format understood to be an interval. In previous releases, the value was stored as a string. Report server renders interval values.

If a source value is a decimal data type with a precision > 38, the query service attempts to store the value as a decimal type with a precision of 38. If a value is too large, the query service returns an error indicating the source column, value, and logical row number in the input data.

Trailing spaces are removed from any character values.

Timestamps and times with time zones are normalized to a value based on the coordinated universal time (UTC).

Configuring the Compute service

The **Query service** advanced settings are used to configure the **Compute service** that is used to process data from uploaded files and data sets.

The following **Query service** advanced settings can be specified:

qs.queryExecution.flintServer.queryTimeoutInterval

Specifies the maximum amount of time, in seconds, that a query can be executed before it is timed out. Timeouts may occur when concurrent loads compete for system resources, for example, CPU, Memory and Disk, or slow devices (Disk).

The value can be `300` (default), or a positive integer less than or equal to `3600` (one hour).

qs.queryExecution.flintServer.loadingPolicy

Specifies the loading policy for the Compute service. This service can be started when the query service starts, or be deferred until a query that requires the Compute service is needed.

If a Cognos Application tier server uses a large percentage of available RAM and there is no workload that uses uploaded files or data sets, delaying the process until the server starts provides a small memory saving.

The following value can be used:

- `eager` (default) - the Compute service starts when the query service starts.
- `lazy` - the Compute service is deferred until a query that requires this co-process is needed.

qs.queryExecution.flintServer.maxHeap

Specifies the maximum amount of memory that the Compute service is allowed to use.

The value can be 4096 (default), or a positive integer greater than 4096. Using a higher value might be required when workloads need more memory to complete.

qs.queryExecution.flintServer.minHeap

The minimum amount of memory that the Compute service is allowed to use.

The value can be 1024 (default), or a positive integer greater than 1024.

qs.queryExecution.flintServer.sparkThreads

Specifies the maximum number of threads the Compute service can use to service queries. The specified value must be a positive integer greater than 1.

qs.queryExecution.flintServer.extraJavaOptions

Specifies additional arguments for the Compute service.

Procedure

1. From **Manage** > **Administration console**, open **Cognos Administration**.
2. On the **Configuration** tab, click **Dispatchers and Services**, and click your dispatcher name.
3. In the list of services, locate the **Query service**, and click its properties icon ▤.
4. On the **Settings** tab, under **Category**, select **Environment**.
5. Next to **Advanced settings**, click **Edit**.
6. Select the **Override the settings acquired from the parent entry** check box.
7. Type or copy the parameter names and their values, as specified earlier in this topic.
8. Click **OK**.
9. Restart the **Query service**.

Chapter 8. Back Up Data

We recommend that you regularly back up your IBM Cognos software data and configuration settings, and your Framework Manager projects and models. This prevents the loss of your data should your computer be damaged or stolen. After your computer is operational, you can restore your data.

Because backing up consumes system resources, if IBM Cognos software is running while the database is backed up, its performance will be affected.

If you changed the location of the encryption and signing key settings from the default location, ensure that you back up the directory that contains them. Also, if the key stores are secured with passwords, ensure that you retain these passwords.

Data you back up is meant to be restored to the same computer. For information about moving data from one computer to another, see Chapter 19, “Deployment,” on page 267.

For information about backing up data before you upgrade your software, see the upgrade topic in the IBM Cognos Analytics *Installation and Configuration Guide*.

If you use a source control system to store your Framework Manager projects, you do not need to back up your projects.

If you customized any information in IBM Cognos Configuration or in the content store, ensure that it is backed up correctly.

Back Up the Content Store

You can back up the content store.

Procedure

1. Back up the content store.

   For more information, see your database documentation.
2. Copy the *install_location*/configuration directory to the backup location.

   This directory contains the configuration settings.

Results

If you must ever restore the configuration settings, you can copy the backed-up directory to the correct location.

For information about restoring the content store, see your database documentation.

Back Up Framework Manager Projects and Models

You can back up Framework Manager projects and models.

Procedure

Copy the Framework Manager project directory and its subdirectories to the backup location.

By default, the projects and models are located in My Documents/My Projects.

Results

If you must ever restore the Framework Manager projects and models, you can copy the backed-up directories to the correct location.

Chapter 9. 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.

The software supports an IBM FileNet Content Manager with IBM FileNet CMIS external repository. If you already have IBM Filenet CMIS version 1 of the software installed, you must upgrade this software with fix pack, version 2. Content archival can also be configured to use your file system.

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.

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.

Importing custom classes definitions and properties into IBM FileNet Content Manager

To use IBM Cognos content archival, you must import a set of custom classes and properties files into IBM FileNet Content Manager.

Custom classes definitions and properties include FileNet specific metadata. You can install custom classes and properties files at any time.

Procedure

1. If you have FileNet archiving set up, go to `*install_location*/configuration/repository/filenet/upgrade/`directory.
2. If FileNet archiving is not already set up, go to `*install_location*/configuration/repository/filenet/new/` directory.
3. Copy the `CMECMIntegrationObjects_CEExport._xxx.xml` files to a local folder on the FileNet server.
4. Open the FileNet Enterprise Manager Administration tool and connect to the domain for the FileNet external repository.
5. Select a target Object Store, and click **Import All Items** to import the definitions into the object store.
6. In the Import Options pane, click **Import Manifest File** and browse to where the `CMECMIntegrationObjects_CEExport._xxx.xml` files are located.
7. Select the `CMECMIntegrationObjects_CEExport_Manifest.xml` file and click **Import**.
8. Restart the FileNet Content Engine and FileNet CMIS application to apply the changes to your environment.

   Note: It might take a long time for changes to be updated across all FileNet nodes.

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 = ClbFolder,COGNOSSREPORT,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).
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 either `CM_FILENET.xml` or `CM_CM8.xml`, depending on whether you archive your content to an IBM FileNet Content Manager repository or an IBM Content Manager 8 repository.

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. Do one of the following steps:
   - If you archive your content to FileNet, open the file named `CM.FILENET.xml` in a text editor.
   - If you archive your content to IBM Content Manager 8, 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*.

Administer content archival

Administration of your content archival includes creating archival tasks and specifying archival locations.

Report output can be archived to an external report repository for long-term storage. For more information, see "External Repository data source connections" on page 107.

Specifying an external repository for report output

You must specify a repository at the folder and package level before content can be archived to the repository.

To specify a repository, a connection to the repository must exist and you must have sufficient privileges to select the repository. You must have execute permission for the secured feature **Manage repository connections** for the **External Repositories** capability. When a connection is specified, any new report output versions are automatically copied to the external repository.

If a data source connection to an external repository is specified already, it can be overridden and another repository selected. If you no longer want to archive content in the package or folder, you can remove the reference to the connection using the **Clear** option. Here is an example. A subfolder acquires a repository connection from the parent folder by default. However, either you do not want the contents of the subfolder to be archived, or you do not want the contents of the subfolder archived to the repository specified for the parent folder. To exclude the contents of a subfolder from being archived, use the **Clear** option. To use a different repository from the parent folder, specify a connection for the subfolder.

You can also create a data source connection to an external repository for a folder or package if the repository exists and you have sufficient permission to create a repository connection. For more information, see "External Repository data source connections" on page 107.

Procedure

1. With a folder or package selected, click Set properties icon.
2. On the **General** tab, go to the **Report repository** section.
3. To specify a data source or change an existing data source, select **Override the report repository acquired from the parent entry**.
4. Under **Connection**, click **Select a connection**.
5. In the **Select the data source (Navigate)** window, select the data source.

Creating content archival content maintenance tasks

Create a content archival content maintenance task to move report output within folders and packages for archiving to your external repository.

About this task

You can create and schedule a content archival task to mark report output versions, which are in folders and packages, for archival. Content that is marked for archival is copied and saved in your external repository.

Folders and packages that are marked for archival cannot be deleted from the content store until successfully moved and saved in the external repository.

Procedure

1. Launch IBM Cognos Administration.
2. On the **Configuration** tab, click **Content Administration**.
3. On the toolbar, click the new content maintenance icon, and then click **Content Archival**.
4. Type a name for the content archival task and, optionally, a description and screen tip. Click **Next**.
5. Select the recording level.
6. Click **Add**
7. Select folders, packages, namespaces or namespace folders that you want to mark for archival and click **Add**.
8. Click **OK**.
9. Click **Next**.
10. Choose one of the following:
    - To run once now or later, click **Save and run once**. Click **Finish**, specify the time and date for the run, then click **Run**. Review the run time and click **OK**.
    - To schedule at a recurring time, click **Save and schedule**. Click **Finish**, and then select frequency and start and end dates. Click **OK**.
    - To save without scheduling or running, click **Save only** and click **Finish**.

Creating a retention rule update maintenance task

Create a retention rule update maintenance task to globally modify the number of report output versions, document content versions, and report history that are currently kept in the content store.

About this task

Administrators use the retention rule update task to specify the number of reports, queries, analyses, and document objects to keep in the content store. You can specify how long to keep the history and output versions in the content store. Anything that is older than the date you specify is deleted from the content store. This update task marks output versions to be deleted from the content store if the output versions do not follow the defined retention rule. A background task in content manager deletes the marked objects from the content store. To reduce the content in the content store, consider keeping a maximum of two versions in the content store and archiving older versions in your external repository.

Important: Run this task only after creating and running the content archival task. If you run it before, content that was not marked for archival is permanently deleted from the content store.

Procedure

1. Launch IBM Cognos Administration.
2. On the **Configuration** tab, click **Content Administration**.
3. On the toolbar, click the new content maintenance icon, and then click **Retention Rule Update**.

4. Type a name for the retention rule update task and, optionally, a description and screen tip. Click **Next**.
5. Select the folders and packages that you want to include.
6. For **Run history** retention settings, do one of the following:
   - To keep the run history for a specific number of occurrences, click **Number of occurrences** and type the number. To save an unlimited number of report outputs, set this value to 0.
   - To keep run history for a specific length of time, click **Duration** and click either **Days** or **Months**. Type the appropriate value in the box.
7. For **Output versions** retention settings, do one of the following:
   - To keep report output for a specific number of occurrences, click **Number of occurrences** and type the number. To save an unlimited number of report outputs, set this value to 0.
   - To keep report output for a specific length of time, click **Duration** and click either **Days** or **Months**. Type the appropriate value in the box.
8. Select the recording level, and click **OK**.
9. Choose one of the following:
   - To run once now or later, click **Save and run once**. Click **Finish**, specify the time and date for the run, then click **Run**. Review the run time and click **OK**.
   - To schedule at a recurring time, click **Save and schedule**. Click **Finish**, and then select frequency and start and end dates. Click **OK**.
   - To save without scheduling or running, click **Save only** and click **Finish**.

Creating a content removal content maintenance task

Create a new content removal content maintenance task to mark history objects and report output versions, which are in folders and packages, for deletion.

About this task

You can specify how long to keep the history and output versions in the content store. Anything that is older than the date you specify is deleted from the content store.

Important: Consider the following circumstances when running content removal content maintenance tasks:

- Run this task only after creating and running the content archival task. If you run it before, content that was not marked for archival is permanently deleted from the content store.
- The content marked for deletion is deleted only in IBM Cognos Analytics. The content is not deleted in your external repository.

Procedure

1. Launch IBM Cognos Administration.
2. On the **Configuration** tab, click **Content Administration**.
3. On the toolbar, click the new content maintenance icon, and then click **Content Removal**.
4. Type a name for the content removal task and, optionally, a description and screen tip.
5. Click **Select another location** if you want to edit the location. Navigate to select the folder or click **New Folder** to add a new location. Click **OK**.
6. Click **Next**.
7. Select the folders and packages that you want to include.
8. For **Run history** settings, click the **Run history** check box, type the appropriate value in the box, and then select either **Days** or **Months**.
9. For **Output versions** settings, click the **Output versions** check box, type the appropriate value in the box, and then click either **Days** or **Months**.
10. Select the recording level, and click **OK**.

11. Choose one of the following:

    - To run once now or later, click **Save and run once**. Click **Finish**, specify the time and date for the run, then click **Run**. Review the run time and click **OK**.
    - To schedule at a recurring time, click **Save and schedule**. Click **Finish**, and then select frequency and start and end dates. Click **OK**.
    - To save without scheduling or running, click **Save only** and click **Finish**.

Finding content in your external repository

Your archived content can be viewed in IBM Cognos Analytics or in your external repository.

After your content is moved and archived, it is stored in the location specified when you created the data source connection to your external repository.

Searching archived content

You can access content stored in the IBM Cognos content store and in an external repository. By viewing search results for recent and archived content, users can make critical comparisons between current data and historical data.

When performing searches for archived content, users can search on an element in a report name or on a data element in a report. The archived content can be viewed by clicking the links in the search results.

Content that is stored in a report repository is not available to IBM Cognos Workspace. When a search is performed in IBM Cognos Workspace, archived report output is not reported.

Chapter 10. Security Model

IBM Cognos software security is designed to meet the need for security in different environments. You can use it in everything from a proof of concept application where security is rarely enabled to a large scale enterprise deployment.

The security model can be easily integrated with the existing security infrastructure in your organization. It is built on top of one or more authentication providers. You use the providers to define and maintain users, groups, and roles, and to control the authentication process. Each authentication provider known to IBM Cognos software is referred to as a namespace .

In addition to the namespaces that represent the authentication providers, IBM Cognos software has a built-in namespace named “ Cognos Namespace” on page 163. The Cognos namespace enhances your organization security policies and deployment ability of applications.

Security in IBM Cognos software is optional. If security is not enabled it means that no authentication providers are configured, and therefore all user access is anonymous. Typically, anonymous users have limited, read-only access.

Authentication Providers

User authentication in IBM Cognos software is managed by authentication providers. Authentication providers define users, groups, and roles used for authentication. User names, IDs, passwords, regional settings, personal preferences are some examples of information stored in the providers.

If you set up authentication for IBM Cognos software, users must provide valid credentials, such as user ID and password, at logon time. In an IBM Cognos software environment, authentication providers are also referred to as namespaces, and they are represented by namespace entries in the user interface.

IBM Cognos software does not replicate the users, groups, and roles defined in your authentication provider. However, you can reference them in IBM Cognos software when you set access permissions to reports and other content. They can also become members of Cognos groups and roles.

The following authentication providers are supported in this release:

- Active Directory
- OpenID Connect
- Custom Java Provider
- OpenID Connect Authentication Proxy
- IBM Cognos Series 7
- LDAP
- SAP
- SiteMinder

You configure authentication providers using IBM Cognos Configuration. For more information, see the *Installation and Configuration Guide*.

Multiple Namespaces

If multiple namespaces are configured for your system, at the start of a session you must select one namespace that you want to use. However, this does not prevent you from logging on to other namespaces later in the session. For example, if you set access permissions, you may want to reference entries from different namespaces. To log on to a different namespace, you do not have to log out of the namespace you are currently using. You can be logged on to multiple namespaces simultaneously.

Your primary logon is the namespace and the credentials that you use to log on at the beginning of the session. The namespaces that you log on to later in the session and the credentials that you use become your secondary logons.

When you delete one of the namespaces, you can log on using another namespace. If you delete all namespaces except for the Cognos namespace, you are not prompted to log on. If anonymous access is enabled, you are automatically logged on as an anonymous user. If anonymous access is not enabled, you cannot access the logon page. In this situation, use IBM Cognos Configuration to enable anonymous access.

Hiding Namespaces

You can hide namespaces from users during logon. This lets you have trusted signon namespaces without showing them on the namespace selection list that is presented when users log on.

For example, you may want to integrate single signon across systems, but maintain the ability for customers to authenticate directly to IBM Cognos software without being prompted to choose a namespace.

You can hide Custom Java Provider and eTrust SiteMinder namespaces that you configured.

For more information, see the *Installation and Configuration Guide*.

Deleting or Restoring Unconfigured Namespaces

You can preserve namespaces and all their contents in the content store even if they are no longer configured for use in IBM Cognos software. When a namespace is not configured, it is listed as inactive in the directory tool.

An inactive namespace is one that was configured, but later deleted in IBM Cognos Configuration. The namespace can be deleted from the content store by members of the System Administrators role. You cannot log on to an inactive namespace.

If a new version of IBM Cognos software detects a previously configured namespace that is no longer used, the namespace appears in the directory tool as inactive. You can configure the namespace again if you still require the data. If the namespace is not required, you can delete it.

When you delete a namespace, you also delete all entries in My Folders that are associated with that namespace, and their contents.

An active namespace cannot be deleted, but can be updated.

To recreate a namespace in IBM Cognos Configuration, you must use the original ID of the namespace. For information about configuring and recreating namespaces, see the *Installation and Configuration Guide*.

Deleting an inactive namespace

If a namespace was removed from IBM Cognos Configuration and is no longer required, a member of the System Administrators role can delete it permanently in the directory tool. Deleting a namespace also deletes all the entries in My Folders that are associated with the namespace.

To access the directory administration tool, you must have execute permissions for the **Data Source Connections** secured feature and traverse permissions for the administration secured function.

Procedure

1. In **IBM Cognos Administration**, on the **Security** tab, click **Users, Groups, and Roles**.

   If the namespace you want to delete does not have a check mark in the **Active** column, it is inactive and can be deleted.
2. In the **Actions** column, click the delete button.

   If the namespace is active, the delete button is not available.

Results

The namespace is permanently deleted. To use the namespace again in IBM Cognos software, you must add it using IBM Cognos Configuration.

Authorization

Authorization is the process of granting or denying access to data, and specifying the actions that can be performed on that data, based on a user identity.

IBM Cognos software authorization assigns permissions to users, groups, and roles that allow them to perform actions, such as read or write, on content store objects, such as folders and reports. The content store can be viewed as a hierarchy of data objects. These objects include not only folders and reports, but packages for report creation, directories, and servers.

When IBM Cognos administrators distribute reports to users, they can set up folders in which reports and other objects can be stored. They can then secure those folders so that only authorized personnel can view, change, or perform other tasks using the folder contents.

For information about setting access permissions to the IBM Cognos entries, see Chapter 12, “Access Permissions and Credentials,” on page 173. For information about the Content Manager hierarchy of objects and the initial access permissions, see Appendix C, “Initial access permissions ,” on page 391.

Cognos Namespace

The Cognos namespace is the IBM Cognos software built-in namespace. It contains the IBM Cognos objects, such as groups, roles, data sources, distribution lists, and contacts.

During the content store initialization, built-in and predefined security entries are created in this namespace Chapter 15, “Initial security,” on page 201. You must modify the initial security settings for those entries and for the Cognos namespace immediately after installing and configuring IBM Cognos software “Security settings after installation” on page 215.

You can rename the Cognos namespace using IBM Cognos Configuration, but you cannot delete it. The namespace is always active.

When you set security in IBM Cognos software, you may want to use the Cognos namespace to create groups and roles that are specific to IBM Cognos software. In this namespace, you can also create security policies that indirectly reference the security entries in authentication providers so that IBM Cognos software can be more easily deployed from one installation to another “Security and Deployment” on page 268.

The Cognos namespace always exists in IBM Cognos software, but the use of Cognos groups and roles it contains is optional. The groups and roles created in the Cognos namespace repackage the users, groups, and roles existing in the authentication providers to optimize their use in the IBM Cognos environment. For example, in the Cognos namespace, you can create a group called HR Managers and add to it specific users and groups from your corporate IT and HR organizations defined in your authentication provider. Later, you can set access permissions for the HR Managers group to entries in IBM Cognos software.

IBM Cognos Application Firewall

IBM Cognos Application Firewall (CAF) is a security tool used to supplement the existing IBM Cognos software security infrastructure at the application level. The IBM Cognos Application Firewall analyzes, modifies, and validates HTTP and XML requests before the gateways or dispatchers process them, and before they are sent to the requesting client or service. It acts as a smart proxy for the IBM Cognos product gateways and dispatchers, and prevents the IBM Cognos components 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 other Web sites.

The IBM Cognos Application Firewall provides IBM Cognos components with security features that include data validation and protection , logging and monitoring, and output protection. For more information, see “Data Validation and Protection” on page 164 and “Logging and Monitoring” on page 164.

The IBM Cognos Application Firewall is enabled by default, and should not be disabled.

You can update the IBM Cognos Application Firewall independently of the other IBM Cognos components.

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

Data Validation and Protection

Validation of input data ensures that the data is in the expected format, based on a set of pre-defined variable rules. HTML variables, XML data, cookie values, and parameters are checked against this set of rules.

IBM Cognos Application Firewall (CAF) performs positive validation of parameters instead of only searching for known script injection tags or common SQL injection signatures. Each parameter is validated against a rule that expects a certain data type in a certain format. If the data does not match the CAF rule, it is rejected.

To provide even stronger validation, CAF matches regular expression patterns to protect data inputs that use complicated formats.

A common type of attack is to trick a user into going to a harmful site by modifying the form parameters. The back button and error URL features of a product provide a prime target for this type of attack.

CAF limits the list of hosts and domains that a back URL can access. CAF can be configured with a list of host names, including port numbers and domains. If a back URL contains a host or a domain that does not appear in the list, the request is rejected. By default, the host name of the dispatcher is added to the list. You can configure the list using IBM Cognos Configuration.

For more information, see the *Installation and Configuration Guide*.

Logging and Monitoring

IBM Cognos Application Firewall (CAF) can monitor and log all access to IBM Cognos gateways and dispatchers. Use logging to track possible attacks or misuse of your IBM Cognos applications.

You can configure CAF to log access to a specific file or to use IBM Cognos log application (IPF) logging. If logging is enabled, all requests that fail validation by CAF are logged.

For more information, see the *Installation and Configuration Guide*.

You can use the Web server request log to obtain detailed information about the IP address of the source client in a suspected attack.

Cross-Site Scripting (XSS) Encoding

Many customers use other applications, such as eTrust SiteMinder, to check for cross-site scripting vulnerabilities. These products block HTTP get requests that contain specific characters.

CAF encodes characters in Cascading Style Sheets (CSS) with URLs to prevent other cross-site scripting tools from blocking the characters.

The CAF XSS encoding feature applies only to customers who use the IBM Cognos Analytics portal.

CAF XSS encoding is disabled by default. To enable this feature, use IBM Cognos Configuration.

For more information, see the *Installation and Configuration Guide*.

Filtering of Error Messages

Some error messages may contain sensitive information, such as server names. By default, error message details in IBM Cognos software are routed to IPF log files, and the secure error message option is enabled. The information presented to users indicates only the occurrence of an error, without any details.

You can specify who can retrieve full error details that may include sensitive information by changing the **Detailed Errors** capability in IBM Cognos administration. Typically, this capability is assigned to directory administrators, but you can assign it to other users as well. For more information, see Chapter 13, “Capabilities,” on page 185.

For information about retrieving full error details, see “View Full Details for Secure Error Messages” on page 17.

Parameter Signing

Parameter signing protects parameter values against tampering when they are sent to a Web browser. CAF can sign parameters or specific parts of data. Signing is used only in specific situations. It is enabled when CAF is enabled.

Chapter 11. Users, Groups, and Roles

Users, groups, and roles are created for authentication and authorization purposes.

You can use groups and roles created in IBM Cognos software, and users, groups, and roles created in authentication providers. The groups and roles created in IBM Cognos software are referred to as Cognos groups and Cognos roles.

Users

A user entry is created and maintained in an authentication provider to uniquely identify a human or a computer account. You cannot create user entries in IBM Cognos software.

Information about users, such as first and last names, passwords, IDs, locales, and email addresses, is stored in the providers. However, this may not be all the information required by IBM Cognos software. For example, it does not specify the location of the users' personal folders, or format preferences for viewing reports. This additional information about users is stored in IBM Cognos software, but when addressed in IBM Cognos software, the information appears as part of the external namespace.

Series 7 Users

If you configured the IBM Cognos Series 7 authentication provider, a user from that namespace must belong to at least one Access Manager user class for the user to be usable in IBM Cognos software. For more information, see “Authentication Providers” on page 161.

For example, if you create a new user in Series 7 Access Manager and assign the user to a user class, but then remove the user from that user class, you cannot log on as that user in IBM Cognos software.

Deleting and Recreating Users

For Series 7 authentication providers, you cannot maintain associated properties and items when you delete and re-create a user. For example, if a user creates an object in **My Folders**, and then that user is deleted, the **My Folders** objects are no longer associated with that user. If a user with the same name is re-created, the objects are not reinstated.

If you use an LDAP server, the stability of **My Folders** objects depends on how you use the IDs. If the configuration of the LDAP provider uses the default attribute of dn for the Unique identifier parameter, a reinstated user with the same name keeps the **My Folders** objects of the original user. If you change the Unique identifier parameter to a unique attribute set by the LDAP server, for example, nsuniqueid for Sun Java System, the association of **My Folders** objects is lost for a deleted user and a new **My Folders** will be created for a user of the same name.

You can delete, copy, and change user profiles. For more information, see Chapter 21, “Managing User Profiles,” on page 295.

User Locales

A locale specifies linguistic information and cultural conventions for character type, collation, format of date and time, currency unit, and messages. You can specify locales for individual products, content, servers, authors, and users in IBM Cognos software.

User locale refers to the product and content locales for each IBM Cognos user. Requests from users arrive with an associated locale. IBM Cognos software must determine the language and locale preferences of users and enforce an appropriate response locale when you distribute reports in different languages.

A user locale specifies the default settings that a user wants to use for formatting dates, times, currency, and numbers. IBM Cognos software uses this information to present data to the user.

IBM Cognos software obtains a value for user locale by checking these sources, in the order listed:

- user preference settings

  If the user sets the user preference settings, IBM Cognos software uses these settings for the user's product and content locale and for default formatting options. The user preference settings override the values obtained from the authentication provider.
- authentication provider

  If the authentication provider has locale settings that are configured, IBM Cognos software uses these values for the user's product and content locale.
- browser setting

  Anonymous and guest users cannot set user preference settings. For these users, IBM Cognos software obtains a user locale from the browser stored on the user's computer.

Groups and Roles

Groups and roles can be defined as follows.

Groups 👥 and roles represent collections of users that perform similar functions, or have a similar status in an organization. Examples of groups are Employees, Developers, or Sales Personnel. Members of groups can be users and other groups. When users log on, they cannot select a group they want to use for a session. They always log on with all the permissions associated with the groups to which they belong.

Roles 👥 in IBM Cognos software have a similar function as groups. Members of roles can be users, groups, and other roles.

The following diagram shows the structure of groups and roles.

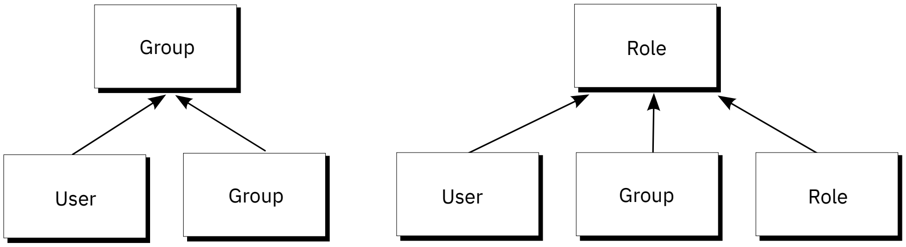


Figure 4. Structure of groups and roles

Users can become members of groups and roles defined in IBM Cognos software, and groups and roles defined in authentication providers. A user can belong to one or more groups or roles. If users are members of more than one group, their access permissions are merged.

You create Cognos groups and roles when

- you cannot create groups or roles in your authentication provider
- groups or roles are required that span multiple namespaces
- portable groups and roles are required that can be deployed

  Create the required groups and roles in your authentication provider, and add them to the appropriate Cognos groups and roles.
- you want to address specific needs of IBM Cognos administration
- you want to avoid cluttering your organization security systems with information used only in IBM Cognos software

Series 7 Roles

If you have configured the IBM Cognos Series 7 authentication provider, user collections known as user classes in Series 7 appear as roles in IBM Cognos software. You can access Series 7 and IBM Cognos software using a single logon. If you start your session by logging on to Series 7, and then access IBM Cognos software, you automatically assume the roles that were in effect for you in Series 7 when you first logged on. You cannot assume different Series 7 roles. For more information on configuring the authentication provider, see “Authentication Providers” on page 161.

Users can assume different roles in Series 7 after they access IBM Cognos software.

Roles Used to Run Reports and Jobs

The roles used to run reports and jobs are associated with the users who run the reports interactively , who are the report owners, and whose credentials are used to run scheduled reports and jobs . Depending on the options selected to run reports, different roles can be assumed by the process.

- When a report runs that has the run as the owner option selected, the process assumes all the roles associated with the report owner.
- When a scheduled report or job runs, the session assumes all the roles associated with the user whose credentials were used to process the request “Trusted credentials” on page 181.

Distribution Lists as Members of Groups and Roles

In some namespaces, such as Microsoft Active Directory, a distribution list may appear on the **Members** tab of the **Set properties** page for a group or role. However, you cannot add distribution lists to a group or role membership, and you cannot use them to set access permissions for entries in the IBM Cognos user interface.

You can add an IBM Cognos distribution list to a Cognos group or role membership using the Software Development Kit. However, the Software Development Kit cannot be used to add an Active Directory distribution list to an Active Directory group. The Active Directory management tools must be used to do this.

IBM Cognos Controller Groups and Roles

For IBM Cognos software, use IBM Cognos Controller groups and roles to configure security. For information about using these groups and roles to configure security, see the IBM Cognos Controller *Installation and Configuration Guide*.

Creating a Cognos group or role

You can add entries from multiple namespaces, created both in the authentication providers and in IBM Cognos software, as members of Cognos groups. You can also create empty groups that do not have any members.

The members of Cognos groups can be users or other groups. The members of Cognos roles can be users, groups, or other roles.

If you plan to create groups or roles that reference entries from multiple namespaces, you must log on to each of those namespaces before you start your task. Otherwise, you will not have full administrative rights for the entries you want to reference.

We recommend that you use the Cognos groups and roles when you set up access permissions to entries in IBM Cognos software because it simplifies the process of deployment. For more information, see “Security and Deployment” on page 268.

When you delete a Cognos group or role, users' access permissions based on it are no longer active. You cannot restore access permissions by creating a group or role with the same name.

To administer users, groups, and roles, you must have execute permissions for the **Users, Groups, and Roles** secured feature, and traverse permissions for the **Administration** secured function. For more information, see Chapter 13, “Capabilities,” on page 185.

Procedure

1. In **IBM Cognos Administration**, on the **Security** tab, click **Users, Groups, and Roles**.
2. Click the **Cognos** namespace.

   Tip: If you want to delete a Cognos group or role, select the check box next to it and click the delete button.
3. On the toolbar, click the new group or new role button.
4. In the **Specify a name and description** page, type a name and, if you want, a description for the new group or role, and then select a destination folder and click **Next**.
5. If you want to create a group without members, click **Finish**.
6. If you want to add members to the new group or role, click **Add** and choose how to select the users, groups, or roles:

   - To choose from listed entries, click the appropriate namespace, and then select the check boxes next to the users, groups, or roles.
   - To search for entries, click **Search** and in the **Search string** box, type the phrase you want to search for. For search options, click **Edit**. Find and click the entry you want.
   - To type the name of entries you want to add, click **Type** and type the names of groups, roles, or users using the following format, where a semicolon (;) separates each entry: *namespace/group_name*;*namespace/role_name*;*namespace/user_name*;

     Here is an example:

     Cognos/Authors;LDAP/scarter;
7. Click the right-arrow button and when the entries you want appear in the **Selected entries** box, click **OK**.

   Tip: To remove entries from the **Selected entries** list, select them and click **Remove**. To select all entries in the list, select the check box for the list. To make the user entries visible, click **Show users in the list**.
8. Click **Finish**.

Adding or removing members of a Cognos group or role

You can modify the membership of a Cognos group or role by adding or removing members.

When you remove users, groups, or roles from a Cognos group or role, you do not delete them from the authentication provider or from IBM Cognos software.

If you plan to modify groups or roles that reference entries from multiple namespaces, you must log on to each of those namespaces before you start your task. Otherwise, you will not have full administrative rights for the entries you want to modify.

To administer users, groups, and roles, you must have execute permissions for the **Users, Groups, and Roles** secured feature, and traverse permissions for the **Administration** secured function. For more information, see Chapter 13, “Capabilities,” on page 185.

Procedure

1. In **IBM Cognos Administration**, on the **Security** tab, click **Users, Groups, and Roles**.
2. Click the **Cognos** namespace.

3. In the **Actions** column, click the properties button for the group or role whose membership you want to modify.
4. Click the **Members** tab.
5. If you want to add members, click **Add** and choose how to select members:

   - To choose from listed entries, click the appropriate namespace, and then select the check boxes next to the users, groups, or roles.
   - To search for entries, click **Search** and in the **Search string** box, type the phrase you want to search for. For search options, click **Edit**. Find and click the entry you want.
   - To type the name of entries you want to add, click **Type** and type the names of groups, roles, or users using the following format, where a semicolon (;) separates each entry:

     `namespace/group_name;namespace/role_name;namespace/user_name;`

     Here is an example:

     Cognos/Authors;LDAP/scarter;
6. Click the right-arrow button and when the entries you want appear in the **Selected entries** box, click **OK**.

   Tip: To remove entries from the **Selected entries** list, select them and click **Remove**. To select all entries in the list, select the check box for the list. To make the user entries visible, click **Show users in the list**.
7. To remove members from a Cognos group or role, in the **Set Properties** page, specify which users, groups, or roles to remove, and click **Remove**.
8. Click **OK**.

Chapter 12. Access Permissions and Credentials

You use access permissions and credentials to secure your organization's data. You specify which users and groups have access to a specific report or other content in IBM Cognos software. You also specify the actions they can perform on the content.

When you set access permissions, you can reference both authentication provider users, groups, and roles and Cognos groups and roles. However, if you plan to deploy your application in the future, we recommend that you use only the Cognos groups and roles to set up access to entries in IBM Cognos software to simplify the process.

Permissions and Permitted Actions

The following table describes the access permissions that you can grant or deny.

Table 51. Permissions and permitted actions

Permissions	**Icons**	**Permitted Actions**
Read	📖 ⊕📖 ⊘📖	View all the properties of an entry, including the report specification, report output, and so on, which are properties of a report.
Write	✏ ⊕✏ ⊘✏	Modify properties of an entry. Delete an entry. Create entries in a container, such as a package or a folder. Modify the report specification for reports created in Reporting and Query Studio. Create new outputs for a report.
Execute	🔄 ⊕🔄 ⊘🔄	Process an entry. For entries such as reports, agents, and metrics, the user can run the entry. For data sources, connections, and signons, the entries can be used to retrieve data from a data provider. The user cannot read the database information directly. The report server can access the database information on behalf of the user to process a request. IBM Cognos software verifies whether users have execute permissions for an entry before they can use the entry. For credentials, users can permit someone else to use their credentials. **Note:** Users must have execute permissions for the account they use with the run as the owner report option.

Table 51. Permissions and permitted actions (continued)

Permissions	Icons	Permitted Actions
Set policy	👤 ⊕👤 ⊘👤	Read and modify the security settings for an entry.
Traverse	👤 ⊕👤 ⊘👤	View the contents of a container entry, such as a package or a folder, and view general properties of the container itself without full access to the content. **Note:** Users can view the general properties of the entries for which they have any type of access. The general properties include name, description, creation date, and so on, which are common to all entries.

Access Permissions for Users

Users must have at least traverse permissions for the parent entries of the entries they want to access. The parent entries include container objects such as folders, packages, groups, roles, and namespaces.

Permissions for users are based on permissions set for individual user accounts and for the namespaces, groups, and roles to which the users belong. Permissions are also affected by the membership and ownership properties of the entry.

IBM Cognos software supports combined access permissions. When users who belong to more than one group log on, they have the combined permissions of all the groups to which they belong. This is important to remember, especially when you are denying access.

Tip: To ensure that a user or group can run reports from a package, but not open the package in an IBM Cognos studio, grant the user or group execute and traverse permissions on the package. Users also require read permissions on the package to launch studios.

Access Permissions Required for Actions

To perform specific actions, each user, group, or role needs the correct combination of access permissions granted for the entry, its parent entry, and its source and target entry. The following table lists permissions required for specific actions.

Table 52. Access permissions required for actions

Action	Permissions required
Add an entry	Write permissions for a parent entry
Query the entry properties	Read permissions for an entry
View the children of the entry	Traverse permissions for an entry
Update an entry	Write permissions for an entry
Delete an entry	Write permissions for an entry, and write permissions for a parent entry

Table 52. Access permissions required for actions (continued)

Action	Permissions required
Copy an entry	Read permissions for an entry and any child entries, traverse permissions for all of the children, and write and traverse permissions for the target parent entry
Move an entry	Read and write permissions for an entry, write permissions for both the source parent entry and the target parent entry, and traverse permissions for the target parent entry

Permissions and permitted actions for Cognos Workspace reports

Cognos Workspace users can or cannot perform actions, depending on their permissions and combinations of permissions for a report, report part, report folder, or workspace objects. The owner of an object is automatically granted read, write, traverse, and execute permissions. If an object is disabled, you must be granted write access in order to see and edit it.

For reports, users with the following access permissions and combinations of permissions can perform the following actions:

Table 53. Report access permissions and permitted actions

Permissions	Permitted actions
Read	Users can view the report in the content pane. Users cannot expand the report to show the report parts. Users cannot drag the report.
Read and Traverse	Users can view the report in the content pane. Users cannot expand the report to show the report parts. If saved output exists, users can drag the report onto the canvas and view the saved output. If saved output does not exist, users cannot drag the report. If they attempt this action, users see the error message in the widget:`The content cannot be displayed. It may have been deleted or you may not have sufficient privileges.` Users can view saved output in the workspace. Users cannot run a live report in a workspace. If they attempt this action, users see the error message: `RSV-CM-0006. The user does not have execute permission on this report.`

Table 53. Report access permissions and permitted actions (continued)

Permissions	**Permitted actions**
Execute	Users can view the report in the content pane. Users cannot expand the report to show the report parts. Users can execute the report, but interactions are not available. Interactions are not available if: • a report is dragged to the canvas • if a user with execute permissions saves a report, and other users open the report • if a user with execute permissions opens a workspace created by other users When saved output cannot be viewed in a workspace, users see the error message: `The content cannot be displayed. It may have been deleted or you may not have sufficient privileges.`
Read and execute	Users can view the report in the content pane. Users can expand the report to show the report parts. Users can execute the report and interactions are available. In the content pane, users cannot save report changes. If users add the report to the workspace and save it, report changes can be saved. If the report is added to the workspace by a person who is not the report owner, that user cannot save changes. The user sees the error message: The `content cannot be saved. You do not have sufficient privileges.`
Read, execute, traverse	Users can view the report in the content pane. Users can expand the report to show the report parts. In the content pane, users can execute the report and interactions are available. Users can add the report to the canvas as either live or saved output. The type of report that is added depends on the default action specified in the report's properties.
Read, write, execute, traverse	Users can view the report in the content pane. Users can expand the report to show the report parts. Users can add the report to the workspace. Users can execute the report and interactions are available. Users can change and save the report. Users can add the report to the canvas as either live or saved output. The type of report that is added depends on the default action specified in the report's properties.

Table 53. Report access permissions and permitted actions (continued)

Permissions	Permitted actions
Read, execute, set policy	Users can view the report in the content pane. Users can expand the report to show the report parts. Users can execute the report and interactions are available. In the content pane, users cannot save report changes. If users drag the report to the workspace and save it, report changes can be saved. This action creates a copy of the report. The copied workspace report inherits the permissions from the original report when the user has the set policy permission.

For report parts, users with the following access permissions and combinations of permissions can perform the following actions:

Table 54. Report part access permissions and permitted actions

Permissions	Permitted actions
Read and execute	Users can view the report. Users can expand the report to show the report parts. Users can drag the report part onto the canvas and can execute the report part.

For folders, users with the following access permissions and combinations of permissions can perform the following actions:

Table 55. Folder access permissions and permitted actions

Permissions	Permitted actions
Read	Users can view the folder in the content pane and can read folder properties. Users cannot drag the folder onto the canvas. Users cannot expand the folder to show the contents. Users cannot save workspace objects in this folder.
Traverse	Users can drag the folder onto the canvas. Users can expand the folder to show the contents. Users cannot save workspace objects in this folder.
Write and traverse	Users can drag the folder onto the canvas. Users can expand the folder to show the contents. Users can save workspace objects in this folder.

For workspaces, users with the following access permissions and combinations of permissions can perform the following actions:

Table 56. Workspace access permissions and permitted actions

Permissions	Permitted actions
Read	Users can view the workspace. Users cannot open the workspace.
Read and traverse	Users can open the workspace. With the Traverse permission, users can view the workspace widgets.
Read, write, and traverse	Users can view, open, and save the workspace.

Ownership of Entries

If the user is an owner of an entry, the user has full access permissions for the entry. This ensures that users can always access and modify the entries they own. By default, the owner of the entry is the user who creates the entry. However, any other user who has set policy permissions for the entry can take ownership of the entry.

Granted and Denied Access

You can grant access or deny access to entries. An icon that represents the type of access appears next to the entry name on the **Permissions** tab. For example, when a group has execute permissions for a report, this icon appears next to the group name on the **Permissions** tab for the report. When a group has execute permissions denied for a report, this icon appears next to the group name.

Denied access has precedence over granted access. When you deny specific users or groups access to an entry, you replace other security policies that grant access to the entry.

If the grant and deny permissions are in conflict, access to the entry is always denied. For example, a user belongs to two groups. One group has access granted to a report and the other group has access denied to the same report. Access to this report is denied for the user.

Deny access only when it is really required. Typically, it is a better administrative practice to grant permissions than to deny them.

Parent and Child Permissions

If access permissions are not defined, the entry usually acquires permissions from its parent entry. You can replace parent permissions by defining permissions for the child entry.

Note: If you create a Framework Manager package but do not define its security, its default access permissions do not match those of its parent folder. To ensure that a new package's access permissions match those of its parent, follow these steps:

1. Edit the file `*installation_directory*\configuration\fm.ini`
2. Change the line

   ```
   <Preference Name="SetPolicyPackage">TRUE</Preference>
   ```

   to

   ```
   <Preference Name="SetPolicyPackage">FALSE</Preference>
   ```

For more information, see "Chapter 7: Publishing packages" in the *IBM Cognos Analytics Framework Manager User Guide*.

Objects that exist only as children of other objects always acquire permissions from their parents. Examples of such objects are report specifications and report outputs. They are visible through the Software Development Kit. You cannot set permissions specifically for those objects.

Permissions and Deployment

Capabilities Permissions

If you are an administrator, you set access to the secured functions and features by granting execute permissions for specified namespaces, users, groups, or roles. For more information, see Chapter 13, “Capabilities,” on page 185.

Deleting Cognos Groups and Roles

When you delete a Cognos group or role, access permissions based on it are also deleted. You cannot restore them by creating a new group or role with the same name because this entry has a different internal ID.

If your groups or roles are created by authentication providers, check how your authentication provider deals with such situations. Typically, you cannot recreate access permissions if they are based on IDs but you can if they are based on names.

Accessing Entries Associated with Data Sources Secured Against Multiple Namespaces

Data sources in IBM Cognos software can be secured against multiple namespaces. In some environments, the namespace used to secure the data source is not the primary namespace used for access to IBM Cognos Analytics. When you try to access an entry, such as a report, a query, or an analysis, that is associated with a data source secured against multiple namespaces, and you are not logged on to all of the required namespaces, a prompt for authentication appears. You must log on to the namespace before you can access the entry.

When single signon (SSO) is enabled, the prompt for authentication does not appear. You are automatically logged on to the namespace.

This functionality applies to IBM Cognos Viewer only. If a similar situation occurs in an IBM Cognos studio, you must quit your task and log on to all the namespaces that you want to use in the current session.

Set access permissions for an entry

Setting access permissions for an entry includes creating new permissions or updating existing permissions. You can specify access permissions for all entries in IBM Cognos software. Some examples of such entries are reports, queries, analyses, packages, agents, metrics, namespaces, groups, users, or dispatchers. You can reference users, group and roles from different namespaces in a security policy for an entry.

If you plan to reference entries from multiple namespaces, log on to each namespace before you start setting access permissions. Otherwise, entries in namespaces to which you are not logged on are shown as **Unavailable**.

Entries referenced by a security policy may also be shown as **Unavailable** when

- the entries were recently deleted from an external namespace.

  IBM Cognos software has no control over the content of security providers.

- the entries are associated with an external namespace that was recently deleted.

  To avoid this issue, run the consistency check type of content maintenance task selecting the option **References to external namespaces**. Content Manager deletes entries associated with the deleted namespaces from security policies.

  For more information, see "Content store maintenance tasks" on page 54.

To administer security, you must have set policy permissions. For more information, see Chapter 12, "Access Permissions and Credentials," on page 173.

Note for Cognos Analytics on Demand users:

- The Standard built-in groups and roles in the Cognos namespace do not exist.
- You cannot change the capabilities of a user, group, or role. Capabilities are determined by the user's on Demand subscription level.

Procedure

1. In IBM Cognos software, locate the entry for which you want to set access permissions.
2. In the **Actions** column, click the set properties button ▤ for the entry.
3. In the **Set properties** page, click the **Permissions** tab.
4. Choose whether to use the permissions of the parent entry or specify permissions specifically for the entry:
   - To use the permissions of the parent entry, clear the **Override the access permissions acquired from the parent entry** check box, then click OK if you are prompted to use the parent permissions. Click **OK**.
   - To set access permissions for the entry, select the **Override the access permissions acquired from the parent entry** check box, then proceed to step 5.
5. If you want to remove an entry from the list, select its check box and click **Remove**.

   Tip: To select all entries in the list, select the check box for the list.
6. To specify the entries for which you want to grant or deny access, click **Add**, then choose how to select entries:
   - To choose from listed entries, click the appropriate namespace, and then select the check boxes next to the users, groups, or roles.
   - To search for entries, click **Search** and in the **Search string** box, type the phrase you want to search for. For search options, click **Edit**. Find and click the entry you want.
   - To type the name of entries you want to add, click **Type** and type the names of groups, roles, or users using the following format, where a semicolon (;) separates each entry:

     namespace/group_name;*namespace/role_name*;*namespace/user_name*;

     Here is an example:

     Cognos/Authors;LDAP/scarter;
7. Click the right-arrow button and when the entries you want appear in the **Selected entries** box, click **OK**.

   Tip: To remove entries from the **Selected entries** list, select them and click **Remove**. To select all entries in the list, select the check box for the list. To make the user entries visible, click **Show users in the list**.
8. For each entry in the list, in the box next to the list, select or clear check boxes to specify what type of access you want to grant or deny.
9. Click **OK**.

   In the **Permissions** column, an icon appears next to the user, group, or role. This icon represents the type of access granted or denied to the entry.

10. If you want to remove access permissions that were previously set for the child entries so that the child entries can acquire permissions set for this entry, in the **Option** section, select the **Delete the access permissions of all child entries** check box.

    This option appears only with entries that are containers. You can use it to restrict access to a hierarchy of entries.

    Warning: Select this option only when you are certain that changing access permissions of the child entries is safe.
11. Click **OK**.

Trusted credentials

Trusted credentials are used for users who must perform a task or process, but do not have sufficient access permissions for entries that contain sensitive data, such as database signons and group memberships. Users with more extensive access permissions, who own the entries, can authorize a trusted user to use their credentials to access the entries.

Trusted credentials are also used to run scheduled requests when users are not logged on to IBM Cognos software, for example, overnight. When the request runs, a user session is created. The trusted credential is used to log on to IBM Cognos software as the user the trusted credential represents and the user's access permissions are used to run the report or the job.

Trusted credentials can consist of one or more credential pairings (user ID and password). The number of trusted credentials depends on the number of namespaces you log in to during your session, when you create or renew your credentials. The account that the trusted credentials is applied to is the first namespace you log into for that session, also known as the primary namespace.

Trusted credentials are stored as part of the account object in the namespace.

By default, trusted credentials are automatically renewed once a day. An administrator can change the default renewal frequency by specifying the **`expiryRenewedTC`** property in IBM Cognos Configuration, under **Security** > **Authentication** > **Advanced properties**. Only integers, which represent number of days, can be used as values for this property. The minimum value is 1.

If you change your password during the day after your credentials are automatically renewed in a Cognos Analytics session, you must renew them manually to prevent any schedules that are using the credentials from failing later in the day. For example, you log in to Cognos Analytics in the morning. The automatic renewal happens. In the afternoon, you change your password and log into Cognos Analytics again. The automatic renewal already took place in that 24 hour period, so it will not happen again until the next renewal period. In this case you must renew manually to ensure any schedules later that day do not fail.

Creating trusted credentials

You can create trusted credentials when you want to authorize other users to use your credentials because those users do not have sufficient access permissions to perform specific tasks.

For users to use trusted credentials, traverse permissions must be granted for the namespace.

Procedure

1. Click the my area options button 👤, **My Preferences**.
2. On the **Personal** tab, under **Credentials**, if you have not created credentials before, click **Create the Credentials**.

    Tip: If your trusted credentials are already created, you might only need to renew them by clicking **Renew the credentials**.
3. Select the users, groups, or roles that you want to authorize to use your credentials.

    If you are prompted for your credentials, provide your user ID and password.
4. If you want to add entries, click **Add** and choose how to select entries:

- To choose from listed entries, click the appropriate namespace, and then select the check boxes next to the users, groups, or roles.
- To search for entries, click **Search** and in the **Search string** box, type the phrase you want to search for. For search options, click **Edit**. Find and click the entry you want.
- To type the name of entries you want to add, click **Type** and type the names of groups, roles, or users using the following format, where a semicolon (;) separates each entry:

  `namespace/group_name;namespace/role_name;namespace/user_name;`

  Here is an example:

  Cognos/Authors;LDAP/scarter;

5. If you want to remove an entry from the list, select the check box next to it and click **Remove**.

Results

The users, groups, or roles that can use your credentials are now listed in the **Credentials** section.

Renewing trusted credentials automatically

Setting your IBM Cognos Analytics environment to renewing trusted credentials automatically can eliminate failed activities caused by changed or expired user credentials. When a user logs in to Cognos Analytics with a user name and password, the trusted credential used to run their scheduled jobs is also refreshed.

Before you begin

This setting works only if your IBM Cognos Analytics environment uses basic authentication (when a user provides a user name and password to log in). If your environment uses single sign-on (SSO), you can work around this limitation by configuring the REMOTE_USER environment variable for SSO. For more information about how to configure the REMOTE_USER environment variable, see *Enabling single signon between Active Directory Server and IBM Cognos Components to use REMOTE_USER* in *Cognos Analytics Installation & Configuration*.

Procedure

1. Open IBM Cognos Configuration.
2. In the **Explorer** window, under **Security**, click **Authentication**.
3. In the **Automatically renew trusted credential** field, select one of the following values:

   Primary namespace only

   Your primary namespace for the Cognos Analytics session is the namespace of the first session you log in to. The account you logged in to is considered the container for the trusted credentials you create or renew for that session. If you have trusted credentials for that account, the credentials are updated for it. All other credentials for other namespaces that you log in to are not updated.

   This is the default value.

   OFF

   Credentials are not updated in any namespace.

   All namespaces

   When you log in to the first namespace, your credentials are updated as described for the **Primary namespace only** value. When you log in to more namespaces, if the trusted credentials associated with the primary namespace account contain login information for the additional namespaces, then those trusted credentials are also updated. For example, you want to run a scheduled consistency check that spans multiple namespaces.

   ⚠ **CAUTION:** This is a system-wide setting so use it only when necessary.

Note: Do not select this value if you have users that authenticate into secondary namespaces with different user IDs. If you select this value, it can cause conflicts in the credentials that are renewed for the namespace.

4. From the **File** menu, click **Save**.

Manage Your Own Data Source Credentials

It is important to manage data source credentials for your users because these credentials are required for certain tasks.

You may be prompted for your data source credentials when you perform the following actions:

- view, run, or open an entry
- use a schedule or a job
- select the data sources that can be used to create a package

You may also be prompted for data source credentials when you use Framework Manager (see the Framework Manager *User Guide*).

If you are an administrator, you can also create or modify data source signons, but if you have a lot of users, it can be unwieldy for data source configurations that require each user to have their own signon since the credentials for each user must be done individually. You can also view the data source credentials for other users.

Note that credentials are checked in the following order:

- first, the signons that you create as an administrator are checked
- if no credentials are found for the user, the user's profile is checked to see if they have stored their own credentials
- if no credentials for the user are found in either place, the user is prompted for credentials

This is important because if you create credentials after a user has saved their own credentials, they get data associated with the credentials that you created for them, which might not be what they are expecting.

Before you begin

If you are a user, your administrator must give you execute permissions for the **Manage own data source signons** capability and traverse permissions for its ancestors. You must also have read and traverse permissions on your account. You can then save credentials to your personal profile, as long as you do not have access to any predefined signons for the data source. You are not prompted for your credentials if you have permission to access an existing data source credential and you have saved the personal credential in your profile. You can view and delete your data source credentials from the **My Preferences** page.

To view another user's credentials, you must have read and traverse permissions on the user's account. To remove data source credentials, you must have read, write, and transverse permissions on the user's account.

Save Data Source Credentials

You can save your data source credentials so that you are not prompted for them every time.

Procedure

1. When you are prompted to enter your data source credentials, enter your user ID and password.
2. Select the **Remember my user ID and password when connecting to this data source** check box.
3. Click **OK**.

Results

The next time you perform an action that requires those data source credentials, you are not prompted for them unless they have been removed or deleted, or have expired.

View and Remove Your Data Source Credentials

You can view and delete your data source credentials.

Procedure

1. Click **My Area Options**, **My Preferences**.
2. Click the **Personal** tab.

   Your data source credentials are listed under **Data source credentials**. You can sort the list by **Data Source Name** or **Data Source Connection Name**.
3. To remove a data source credential, select the check box for it, then click **Remove**.

Chapter 13. Capabilities

The capabilities within the functions, which are also referred to as secured functions and secured features, control access to different administration tasks and different functional areas of the user interface in IBM Cognos software.

Examples of the secured functions are **Administration** and **Reporting**. Examples of the secured features are **User Defined SQL** and **Bursting**.

Content Manager reads the users' permissions at logon time. Depending on the permissions for the secured functions and features, users can access specific components and perform specific tasks in IBM Cognos software.

When a content store is initialized, the initial permissions for the secured functions and features are created. The permissions define which of the predefined and built-in Cognos groups and roles have access to which secured functions and features, and the type of access. The initial permissions grant unrestricted access to IBM Cognos software because the built-in role System Administrators includes the group Everyone in its membership. You must remove the group Everyone from the membership of System Administrators before you start setting access to capabilities.

When running a report using the **Run as the owner** option, the capabilities of the owner are used for bursting and report layout properties in the HTML format. All other capabilities are based on the user who runs the report.

For instructions about how to assign capabilities to users, groups, and roles, see "Setting access to capabilities" on page 194.

Users can see a list of the secured functions and features available to them in **My Preferences** on the **Personal** tab.

For more information, see "Initial access permissions for capabilities" on page 393.

Note: You must select **Manage** > **People** > **Capabilities** to see the complete list of capabilities. Although many of the capabilities also appear in the Administration console, we recommend that you use the **Manage** component when you assign capabilities.

Adaptive Analytics

This secured function controls access to the reports packaged using Adaptive Analytics.

Administration

This secured function contains the secured features that control access to the administration pages that you use to administer IBM Cognos software. System administrators can use this capability to delegate administration tasks to different administrators.

The following secured features are associated with this function:

- **Adaptive Analytics Administration**

  Users can access Adaptive Analytics to perform administrative tasks.
- **Administration tasks**

  Users can access **Content Administration** on the **Configuration** tab in **IBM Cognos Administration** to administer exports, imports, consistency checks, and report updates.
- **Collaboration Administration**

  Users can access the ability to create and control collaboration platforms.
- **Configure and manage the system**

Users can access **System** on the **Status** tab and **Dispatchers and Services** on the **Configuration** tab in **IBM Cognos Administration** to configure dispatchers and services, and to manage the system.

- **Controller Administration**

  Users can use the administrative functions of IBM Cognos Controller.

- **Data Source Connections**

  Users can access **Data Source Connections** on the **Configuration** tab in **IBM Cognos Administration** to define data sources, connections, and signons. In IBM Cognos Analytics on Cloud, they can also access the **Secure Gateway** page from the **Manage** menu.

- **Distribution Lists and Contacts**

  Users can access **Distribution Lists and Contacts** on the **Configuration** tab in **IBM Cognos Administration** to manage distribution lists and contacts.

- **Manage Visualizations**

  This secured function specifies that the user can control access rights to custom visualizations for individual users, groups, and roles.

- **Mobile Administration**

  Users can administer IBM Cognos Analytics Mobile Reports services and applications.

- **Planning Administration**

  Users can access IBM Cognos Planning Contributor Administration Console and IBM Cognos Planning Analyst to perform administration tasks.

- **PowerPlay Servers**

  User is given limited access to the IBM Cognos Administration pages. This includes access to the PowerPlay page and the ability to set PowerPlay properties.

- **Printers**

  Users can access **Printers** on the **Configuration** tab in **IBM Cognos Administration** to manage printers.

- **Query Service Administration**

  Users can access the **Status** > **Data Stores** page in **IBM Cognos Administration** to manage dynamic cubes. Users can perform operations on cubes, such as starting and stopping cubes, refreshing the data cache, and creating and scheduling query service tasks.

- **Run activities and schedules**

  Users can access **Current Activities**, **Past Activities**, **Upcoming Activities** and **Schedules** on the **Status** tab in **IBM Cognos Administration** to monitor the server activities and manage schedules. To grant access to the scheduling functionality independently from the monitoring functionality, use the Scheduling capability.

- **Set capabilities and manage UI profiles**

  Users can access **Capabilities** and **User Interface Profiles** on the **Security** tab in **IBM Cognos Administration** to manage the secured functions and features and the Reporting user interface profiles.

- **Styles and portlets**

  Users can access **Styles** and **Portlets** on the **Configuration** tab in **IBM Cognos Administration** to manage styles and portlets.

- **Users, Groups and Roles**

  Users can access **Users, Groups and Roles** on the **Security** tab in **IBM Cognos Administration** to manage namespaces, users, groups, and roles.

AI

This capability allows designated users to access AI functionality. The roles granted with Execute permissions by default are listed in the AI capability section.

The following secured features are associated with this function:

- 11.1.6 **Learning**

  This secured function allows the system to learn from an assignee's product usage.
- 11.1.5 **Use Assistant**

  This secured function allows designated users to use the Assistant.

Analysis Studio

This secured function controls access to IBM Cognos Analysis Studio. Users with access to this studio explore, analyze, and compare dimensional data, find meaningful information in large data sources, and answer business questions.

Attach Outputs

11.1.7 This capability allows a user to attach outputs in an email when setting a schedule, running a report in the background, or setting job steps.

.

Cognos Analytics for Mobile (on Demand only)

11.1.7 This capability allows users access to Cognos Analytics via the Cognos Analytics for Mobile app. The roles granted with Execute permissions by default are listed in the "Cognos Analytics for Mobile capability" section of Initial access permissions for capabilities.

Cognos Insight

This secured function controls access to IBM Cognos Insight. Users with access to this tool work with complicated data sources to discover, visualize, and plan in easy to use workspaces.

Cognos Viewer

This secured function controls access to IBM Cognos Viewer, which you use to view reports.

The secured features associated with this function are

- **Context Menu**

  Users can use the context menu in IBM Cognos Viewer.

  Note: To see the context menu, users must have access to both the **Selection** and **Context Menu** secured features.
- **Run With Options**

  Users can change the default run options. When users have no execute permissions for this feature, they cannot see the **Run with options** ▶ icon for reports.
- **Selection**

  Users can select text in lists and crosstabs.
- **Toolbar**

  Users can see the IBM Cognos Viewer toolbar.

Collaborate

This secured function controls access to IBM Connections from within IBM Cognos.

The secured features associated with this function are:

- **Launch Collaboration Tools**

The secured feature allows users to launch IBM Connections from any Launch menu within the IBM Cognos Analytics environment, including the Cognos Workspace Getting Started Page, and the Actions Menu. The links will go to the user's IBM Connections home page, if it is configured, or to Activities.

- **Allow Collaboration Features**

  This secured feature controls access to the **Collaborate** icon and to IBM Connections Search Results within Cognos Workspace. Users must have access to create or view activities from within Cognos Workspace.

Controller Studio

This secured function controls access to IBM Cognos Controller.

Dashboard

This secured function controls access to view Dashboards and Stories. Users require Execute permissions for the Dashboard capability to view both dashboards and stories. The roles granted with Execute permissions by default are listed in the "Dashboard capability" on page 405 section.

Data Manager

This secured function controls access to Data Manager.

Data sets

This secured function controls access to the **Create data set** menu that is available from the package and data module context menus.

Desktop Tools

This secured function controls access to Cognos Desktop Tools products. Users with this capability are members of the Analytics Explorers role. This allows them to access Cognos Analysis For Microsoft Excel, Cognos Framework Manager, Cognos Cube Designer and Dynamic Query Analyzer, Transformer, and TM1 Writeback to bundled FLBI TM1 server.

Detailed Errors

This secured function controls access to viewing detailed error messages in the Web browser.

Develop Visualizations

This secured function specifies that the user can develop custom visualizations.

Drill Through Assistant

This secured function controls access to the drill-through debugging functionality in the drill-through **Go To** page and the drill-through definitions. Users who have this capability see additional information in the **Go To** page for each drill-through target. This information can help to debug a drill-through definition, or can be forwarded to the Cognos Software Services representative.

Event Studio

This secured function controls access to Event Studio.

Email

11.1.7 This capability allows a user to send an email when scheduling or sharing content. The roles granted with Execute permissions by default are listed in the "Email capability" section of Initial access permissions for capabilities.

The following secured features are associated with this capability:

Email Delivery Option

This secured function allows a user to choose email delivery when setting a schedule, running a report in the background, or setting job steps.

Include link in email

This secured function allows a user to link to content from an email when sharing content, setting a schedule, or running a report in the background.

Share using email

This secured function allows a user to share annotated screen captures via email from **Share** > **Send**.

Type in external email

This secured function allows a user to enter external recipients in an email. If the secured function is not granted, the user can only select recipients from their authenticated namespaces.

Execute Indexed Search

This secured function controls access to the search of indexed content. This secured function does not appear until the Index Update Service has been started.

By default, Execute Indexed Search allows enhanced indexed search. When Execute Indexed Search is disabled, basic indexed search is provided.

Executive Dashboard

This secured function controls access to IBM Cognos Workspace. Users who have access to this function are granted basic permissions for the workspaces in Cognos Workspace. With this type of permissions, users can view the workspaces, drill up and down on the workspace data, add comments, print the workspaces, use slider filters, and select value filters if these filters are included in the workspace.

The following secured features, which are associated with the **Executive Dashboard** function, grant more extensive permissions for the workspace:

- **Use Advanced Dashboard Features**

  Use this feature to grant the users maximum permissions for the workspace.
- **Use Interactive Dashboard Features**

  Use this feature to grant the users permissions to access the workspace functions that allow interaction with the widget data. This includes access to the on-demand toolbar in the widget that provides options for interacting with the report data, such as sorting, deleting, resetting, swapping rows and columns, and changing the report display type.

Exploration

This secured function controls access to the **New** > **Exploration** function. Users require Execute permissions for the Exploration capability both to create or view explorations. The role is granted with Execute permissions by default, as listed in the “Exploration capability” on page 412 section.

External Repositories

This secured function controls access to external repositories. External repositories provide long-term storage for report content. When a connection to an external repository is specified for a package or folder, report output versions are copied to the repository automatically.

The secured features associated with this function are

- **Manage repository connections**

  Users can set a repository connection on a package or folder if a data source connection already exists.

- **View external documents**

  Users can view the report output stored in an external repository.

Generate CSV Output

With permissions for this secured function, users can generate report output in the delimited text (CSV) format. Without this capability, users do not see an option in the user interface to run reports in the CVS format.

Generate PDF Output

With permissions for this secured function, users can generate report output in the PDF format. Without this capability, users do not see an option in the user interface to run reports in the PDF format.

Generate XLS Output

With permissions for this secured function, users can generate report output in the Microsoft Excel spreadsheet (XLS) formats. Without this capability, users do not see an option in the user interface to run reports in the XLS formats.

Generate XML Output

With permissions for this secured function, users can generate report output in XML format. Without this capability, users do not see an option in the user interface to run reports in the XML format.

Glossary

This secured function controls access to the IBM InfoSphere Business Glossary.

Hide Entries

This secured function specifies that a user can hide entries and view hidden entries in IBM Cognos software.

The **Hide this entry** check box appears on the **General** tab of the entries' properties pages. The **Show hidden entries** check box appears on the **Preferences** tab in user profiles, and on the **General** tab in My Area Options 👤, **My Preferences**.

Import Relational Metadata

Specifies that a group can import relational metadata into a Framework Manager or Dynamic Cube Designer project using dynamic query mode.

By default, the System Administrator, Directory Administrator, and Report Administrators groups belong to this secured function.

If other groups require the ability to import relational metadata to a dynamic query mode project they must be added to the capability. For example, if you create a Framework Manager Users group and add your Framework Manager users to that group, you also need to add the group to the Import relational metadata secured function.

Job

This secured function controls the ability for a user to be able to create jobs.

Lineage

This secured function controls access to the **Lineage** action. Use this to view information about data or metadata items from IBM Cognos Viewer, or from the source tree in Reporting, Query Studio, and Analysis Studio.

Manage content

This secured functions controls access to the **Content** tab in **Manage**.

Manage Own Data Source Signons

This secured function controls the ability to manage data source credentials on the **Personal** tab in **My Preferences**.

Mobile

This secured function controls access to IBM Cognos Analytics Mobile Reports.

Notebook

This secured function controls access to the **New** > **Notebook** option. Users require Execute permissions for the Notebook capability to create Notebooks.

Planning Contributor

This secured function controls access to IBM Cognos Planning Contributor and IBM Cognos Planning Analyst.

PowerPlay Studio

This secured function controls access to PowerPlay Studio.

Query Studio

This secured function controls access to the Query Studio, which you use to create simple, ad hoc reports.

The secured feature associated with this function is

- **Create**

  Create new reports and use the Save as option for new reports and custom views.

- **Advanced**

  Use advanced authoring features, such as creating complex filters, formatting style, and multilingual support.

Report Studio

This secured function controls access to the Reporting user interface and to the underlying report execution functionality. Users need execute permissions on this secured function to access the Reporting user interface. Traverse or read permissions on this secured function might be needed to use the associated secured features, for example, to run reports created with custom SQL or embedded HTML.

The secured features associated with this function are:

- **Allow External Data**

  Users can use external data in reports.
- **Bursting**

  Users can author and run burst reports.
- **Create/Delete**

  Users can create new reports, use the Save as option for new reports and report views, and change models.
- **HTML Items in Report**

  Users can use the HTMLItem button and hyperlink elements of the report specification when authoring reports.
- **User Defined SQL**

  Users can edit the SQL statements directly in the query specification and run the query specifications that contain the edited SQL statements.

  Tip: Restrictions on who can use this feature are not enforced in Framework Manager. For example, a Framework Manager user who does not have **User Defined SQL** rights in **IBM Cognos Administration** can still create a query subject and use manually created SQL queries to search a database.

Save to Cloud

11.1.5 This capability allows designated users to save their report output to the cloud. Users require Execute permissions for the Save to Cloud capability to view the **Save to cloud** check box as a delivery option for saved report outputs. The roles granted with Execute permissions by default are listed in the Save to Cloud capability section.

The following secured feature is associated with this function:

- **Manage Connections**

  This secured feature allows Directory Administrators to access the **Manage** > **Storage** page to create and manage connections to external Cloud Object Storage services. Designated users can then access the **Save to cloud** feature.

Scheduling

The Scheduling capability allows a user to schedule items that can be run, such as reports. Users must have the Scheduling capability to see the **My schedules and subscriptions** option in the Personal menu 👤. For more information, see "My schedules and subscriptions" in the *IBM Cognos Analytics Getting Started Guide*.

The secured features associated with this capability are

- **Schedule by day**

  Users can schedule entries daily.
- **Schedule by hour**

  Users can schedule entries by the hour.
- **Schedule by minute**

  Users can schedule entries by the minute.

  If a user is denied access to the **Schedule by minute** capability, 'by minute' scheduling is also denied for other capabilities that allow 'by minute' scheduling, for example, the **Schedule by month** capability.
- **Schedule by month**

  Users can schedule entries monthly.

- **Schedule by trigger**

  Users can schedule entries based on a trigger.
- **Schedule by week**

  Users can schedule entries weekly.
- **Schedule by year**

  Users can schedule entries yearly.
- **Scheduling Priority**

  Users can set up and change the processing priority of scheduled entries.

  Note: A user who schedules an item (that is, a report, event, job and so on) without the **Scheduling Priority** capability cannot schedule an item with a priority other than 3. A different priority may be set, and displayed, in the schedule by a user with the appropriate access. However, the report will still run with a priority of 3 unless its ownership is also changed to a user with the appropriate access to the **Scheduling Priority** capability.

Self Service Package Wizard

This secured function controls the ability to select which data sources can be used to create a package.

Set Entry-Specific Capabilities

This secured function specifies that a user can set up capabilities at an entry level.

The **Capabilities** tab appears in the **Set properties** pages for packages and folders for users who have this capability and who have set policy permissions for the entry or who own the entry.

Share Pin Board (on Demand only)

11.1.7 Users who are assigned this capability can share a pin board that they created using Cognos Analytics for Mobile.

Specification Execution

This secured function allows a user or Software Development Kit application to use an inline specification. The Specification Execution secured function is counted as an Analytics Administrators licence role.

IBM Cognos Analytics studios and some services use inline specifications internally to perform tasks. The service running the specification tests a number of capabilities to ensure that the user is entitled to use the inline specification. For more information, see the runSpecification method in the *Developer Guide*.

Upload files

This secured function controls access to the **Upload files** function. Users who have this capability can upload data files.

Visualization Alerts (on Demand only)

11.1.7 Users who are assigned this capability can create an alert for a pin board in Cognos Analytics for Mobile.

Watch Rules

This secured function controls access to the **Rules** tab in **My Watch Items**. Use this secured function to create and run watch rules.

Web-based modeling

This secured function controls access to the web-based modeling function. Users who have this capability can create data modules from the **New** > **Data module** menu.

Setting access to capabilities

You set access to the capabilities, also known as secured functions and features, by granting Execute and Traverse permissions for them to specified namespaces, users, groups, or roles.

Note: A user must have Execute and Traverse permissions on a capability for it, or any of its sub-capabilities, to appear in the Personal menu 👤 under **My preferences** > **Personal** > **Advanced** > **My Capabilities** > **View details**.

Before you begin

You must have set policy permissions to administer secured functions and features. Typically, this is done by directory administrators.

Before you start setting permissions on capabilities, ensure that the initial security settings are already changed.

Procedure

1. From **Manage** > **People**, click **Capabilities**.

   A list of available secured functions appears.

2. For the secured function that you want to modify, click the More icon ⋯ and then click **Properties**.
3. Click the **Access** tab.
4. Choose whether to use the permissions of the parent entry or specify different permissions:
   - To use the permissions of the parent entry, clear the **Override parent access** check box, and click **Apply**.
   - To set access permissions explicitly for the entry, select the **Override parent access** check box, and then perform the remaining steps.
5. If you want to remove an entry from the list, click the Remove member icon ⊖.
6. If you want to add new entries to the list, click the Add member icon ⊕ and choose how to select entries:
   - To choose from listed entries, click the appropriate namespace, and then click the users, groups, or roles that you want. Click **Add** when you are done.
   - To select multiple entries at once press Ctrl-click.
   - To search for entries, type text in the 🔍 **Find** field.

     Note: You can click the Search Method icon ☰ to find entries that either contain, start with, or are an exact match with the text that you type.

   - Click the filter ▼ icon to narrow the view of entries.
   - To type the name of entries you want to add, click **Type** and type the names of groups, roles, or users using the following format, where a semicolon (;) separates each entry:

     `namespace/group_name;namespace/role_name;namespace/user_name;`

     Here is an example:

     Cognos/Authors;LDAP/scarter;

7. Select the box in the **Permissions** column next to the entry for which you want to set access to the function or feature.
8. Select one of the following Permissions: **Access**, **Assign**, **Manage**, or **Custom**.

   For more information, see “Permission levels” on page 393.
9. Click **Apply**.
10. Click **OK** when you are done.

Chapter 14. Object Capabilities

Object capabilities specify the secured functions and features that users, groups, or roles can use with different packages. For example, the capabilities define the studio to open a package and the studio features available while working with this package.

The secured functions and their features, also referred to as global capabilities, control access to the different components and functionality in IBM Cognos software. For object capabilities to work, you must combine them with applicable global capabilities. For example, when setting up object capabilities for a package that contains Reporting and Query Studio reports, ensure that the user also has access to the **Reporting** and **Query Studio** secured functions and their applicable secured features.

Republishing an existing package from a client tool, such as Framework Manager, does not overwrite or modify object capabilities previously specified.

Control object capabilities with the **Set Entry-Specific Capabilities** secured function "Set Entry-Specific Capabilities" on page 193.

You can set up the following object capabilities for individual packages "Set Up Object Capabilities for a Package" on page 199.

Adaptive Analytics

This secured function controls access to the reports packaged using Adaptive Analytics.

Administration

This secured function controls access to the administrative pages in IBM Cognos software. You can specify object capabilities for the following secured features within **Administration**.

- **Adaptive Analytics Administration**

  Users can access Adaptive Analytics to perform administrative tasks.
- **Planning Administration**

  Users can access IBM Cognos Planning Contributor Administration Console and IBM Cognos Planning Analyst to perform administration tasks.

Event Studio

This secured function controls access to Event Studio.

Glossary

This secured function controls access to the IBM InfoSphere Business Glossary.

Planning Contributor

This secured function controls access to IBM Cognos Planning Contributor and IBM Cognos Planning Analyst.

PowerPlay Studio

This secured function controls access to PowerPlay Studio.

Query Studio

This secured function controls access to the Query Studio, which you use to create simple, ad hoc reports.

The secured feature associated with this function is

- **Create**

  Create new reports and use the Save as option for new reports and custom views.

- **Advanced**

  Use advanced authoring features, such as creating complex filters, formatting style, and multilingual support.

Report Studio

This secured function controls access to the Reporting user interface and to the underlying report execution functionality. Users need execute permissions on this secured function to access the Reporting user interface. Traverse or read permissions on this secured function might be needed to use the associated secured features, for example, to run reports created with custom SQL or embedded HTML.

The secured features associated with this function are:

- **Allow External Data**

  Users can use external data in reports.

- **Bursting**

  Users can author and run burst reports.

- **Create/Delete**

  Users can create new reports, use the Save as option for new reports and report views, and change models.

- **HTML Items in Report**

  Users can use the HTMLItem button and hyperlink elements of the report specification when authoring reports.

- **User Defined SQL**

  Users can edit the SQL statements directly in the query specification and run the query specifications that contain the edited SQL statements.

  Tip: Restrictions on who can use this feature are not enforced in Framework Manager. For example, a Framework Manager user who does not have **User Defined SQL** rights in **IBM Cognos Administration** can still create a query subject and use manually created SQL queries to search a database.

Lineage

This secured function controls access to the **Lineage** action. Use this to view information about data or metadata items from IBM Cognos Viewer, or from the source tree in Reporting, Query Studio, and Analysis Studio.

Specification Execution

This secured function allows a user or Software Development Kit application to use an inline specification. The Specification Execution secured function is counted as an Analytics Administrators licence role.

IBM Cognos Analytics studios and some services use inline specifications internally to perform tasks. The service running the specification tests a number of capabilities to ensure that the user is entitled to use the inline specification. For more information, see the runSpecification method in the *Developer Guide*.

Watch Rules

This secured function controls access to the **Rules** tab in **My Watch Items**. Use this secured function to create and run watch rules.

Set Up Object Capabilities for a Package

Use this functionality to specify the secured functions and features that users, groups, or roles can use with specific packages.

You can specify object capabilities at the package level or, if the package is stored in a folder, at the folder level. Capabilities specified at the folder level apply only to packages in that folder and in its sub-folders, and not to any other entries, including reports. For example, if a folder contains packages, reports and a subfolder that contains other packages and reports, only the packages in the folder and in the subfolder are affected by the capabilities settings.

The following capabilities are applied globally; they cannot be set on a folder by folder basis:

- Generate CSV Output
- Generate PDF Output
- Generate XLS Output
- Generate XML Output

Before you begin

To use object capabilities, the users must

- have access to the secured functions and features associated with the package Chapter 13, "Capabilities," on page 185
- have access to the **Object Capabilities** secured function "Set Entry-Specific Capabilities" on page 193
- have set policy permissions for the package Chapter 12, "Access Permissions and Credentials," on page 173 or own the package

When setting up object capabilities for the first time after installing IBM Cognos software, we recommend that you start with **Public Folders**, and that the capabilities for **Public Folders** mirror the global capabilities. This provides an accurate baseline on which object capabilities can be further refined.

Procedure

1. Open the package or folder properties page.

   Tip: When setting up object capabilities for **Public Folders**, click the properties button in the product toolbar. **Public Folders** are replaced by **Team content** in Cognos Analytics version 11.0.x.
2. Click the **Capabilities** tab.
3. Select the **Override the capabilities acquired from the parent entry** check box.
4. In the **Name** and **Capabilities** list, select the check box next to the user, group, or role for which you want to specify object capabilities.

   If the user, group, or role is not in the list, click **Add**. If you want to remove the user, group, or role from the list, select its check box, and click **Remove**.

   For more information about adding or removing entries from this list, see the steps in "Set access permissions for an entry" on page 179.
5. In the **Grant** and **Deny** list, select or clear the applicable check boxes to grant or deny the required object capabilities for users, groups, or roles.

   An icon that represents a granted or denied capability appears next to the name of the user, group, or role. When you deny access to a secured function, you automatically deny access to all its secured features.
6. If applicable, select the **Delete the capabilities of all child entries** check box.

   Use this option to specify object capabilities for a hierarchy of entries, for example, for all packages in a folder.

7. Click **OK**.

Chapter 15. Initial security

When a content store is initialized, a set of security objects is created and stored in the Cognos namespace. These objects are designed to simplify the IBM Cognos administration.

The initial security policies grant unrestricted access to all objects in the content store to all users. The security administrator must modify the initial security settings to secure the content store. For more information, see "Security settings after installation" on page 215.

To see a summary of the initial access permissions for the Content Manager objects, see Appendix C, "Initial access permissions ," on page 391.

Built-in entries

The built-in entries include the Anonymous user account, the groups All Authenticated Users and Everyone, and the roles System Administrators and Tenant Administrators. You cannot delete the built-in entries. They appear in both secured and non-secured environments.

Anonymous

This entry represents a user account shared by members of the general public who can access IBM Cognos software without being prompted for authentication. For example, this type of access is useful when distributing an online catalog.

Anonymous users can see only those entries for which access permissions are not set, or are set specifically for this account or for the Everyone group.

You can disable the Anonymous user account by changing the configuration parameters in the configuration tool.

All Authenticated Users

This group represents users who are authenticated by authentication providers. The membership of this group is maintained by the product and cannot be viewed or altered.

You cannot deploy this group. For more information, see "Including Cognos Groups and Roles" on page 273.

Everyone

This group represents all authenticated users and the Anonymous user account. The membership of this group is maintained by the product and cannot be viewed or altered.

You can use the Everyone group to set default security quickly. For example, to secure a report, you grant read, write, or execute permissions to the report for the Everyone group. After this security is in place, you can grant access to the report to other users, groups, or roles, and remove the group Everyone from the security policy for this report. Then, only users, groups, and roles that you specified have access granted to the report.

You can use the Everyone group to apply security during deployment, see "Security and Deployment" on page 268, but you cannot deploy the group itself. For more information, see "Including Cognos Groups and Roles" on page 273.

System Administrators

This is a special role in IBM Cognos software. Members of this role are considered root users or super users. They may access and modify any object in the content store, regardless of any security policies set for the object. Only members of the System Administrators role can modify the membership of this role.

The System Administrators role cannot be empty. If you do not want to use System Administrators, you can create an empty group in the Cognos namespace or in your authentication provider, and add this group to the membership of the System Administrators role.

When this role is created during the content store initialization, the group Everyone is included in its membership. This means that all users have unrestricted access to the content store. Immediately after installing and configuring IBM Cognos software, you must modify the initial security settings for this role and remove the group Everyone from its membership. For more information, see “Security settings after installation” on page 215.

You can deploy this role, including Cognos Groups and Roles. For more information, see “Including Cognos Groups and Roles” on page 273.

Tenant Administrators

This role is used in a multitenant IBM Cognos environment. Members of this role can administer multiple tenants.

When this role is created during the content store initialization, it has no members and capabilities. Only System Administrators can add members and assign access permissions and capabilities for this role.

Predefined roles

Predefined roles include several IBM Cognos roles. Each role has a specific set of access permissions and can be used to secure different components and functions in IBM Cognos software. You can use the predefined roles, or delete them.

When the predefined roles are created during the content store initialization, the group Everyone is a member of the System Administrator role. Some of such roles are Consumers, Query Users, Analysis Users, and Authors. If you want to use the predefined roles, you should modify their initial membership immediately after installing and configuring IBM Cognos software. For more information, see “Security settings after installation” on page 215.

There are two types of predefined Cognos roles: standard roles and license roles.

Standard roles

The table in this section lists the predefined standard Cognos roles. Standard roles each have specific capabilities that allow users to perform different tasks in IBM Cognos Analytics.

References:

- For a list of default capabilities assigned to each standard role, see “Initial access permissions for capabilities” on page 393.
- To modify the membership of standard roles, see “Securing System Administrators and predefined roles” on page 216.
- Another type of role is a license role. Based on license entitlements, there are four license names: **Analytics Administrator**; **Analytics Explorer**; **Analytics User**; and **Analytics Viewer**. For more information, see “License roles” on page 204.

Table 57. Predefined Cognos standard roles

Standard role	Description
Analysis Users	Members have the same access permissions as Consumers. They can also use the IBM Cognos Analysis Studio.

Table 57. Predefined Cognos standard roles (continued)

Standard role	**Description**
Authors	Members have the same access permissions as Query Users and Analysis Users. They can use Reporting, Query Studio, and Analysis Studio, and save public content, such as reports and report outputs.
Consumers	Members can read and execute public content, such as reports.
Directory Administrators	Members can administer the contents of namespaces. In the Cognos namespace, they administer groups, accounts, contacts, distribution lists, data sources, and printers.
Library Administrators	Members can access, import, and administer the contents of the **Library** tab in IBM Cognos Administration.
Mobile Users	Members can access IBM Cognos content, such as reports, through IBM Cognos Analytics Mobile Reports.
Mobile Administrators	Members can administer IBM Cognos Analytics Mobile Reports.
Modelers	Members can use the modeling user interface to create and manage data modules.
Portal Administrators	Members can administer the Cognos portlets and other portlets. This includes customizing portlets, defining portlet styles, and setting access permissions for portlets. Portal administrators can also upload extensions that allow users, for example, to add images to reports or dashboards.
Planning Contributor Users	Members can access the Contributor Web client, Contributor Add-in for Microsoft Excel, or Analyst.
Planning Rights Administrators	Members can access Contributor Administration Console, Analyst, and all associated objects in the application.
Query Users	Members have the same access permissions as Consumers. They can also use the IBM Cognos Query Studio.
Readers	Members have read-only access to IBM Cognos software. They can navigate some portions of the content store, view saved report outputs in the portal, select cells in saved report outputs in Cognos Viewer, and use Cognos Viewer context menu to perform actions, such as drill-through.
Report Administrators	Members can administer the public content, for which they have full access. They can also use IBM Cognos Analytics - Reporting and IBM Cognos Query Studio.
Server Administrators	Members can administer servers, dispatchers, and jobs.
System Administrators	Members can access and modify any object in the content store, regardless of any security policies set for the object. Only members of the System Administrators role can modify the membership of this role.

License roles

To help you map capabilities to licensing requirements, Cognos Analytics also provides predefined roles that are based on license entitlements.

Note: Another type of role is a standard role. Standard roles have specific capabilities that allow users to perform different tasks. For more information, see "Standard roles" on page 202.

The following table lists the predefined license roles.

Table 58. Predefined Cognos license roles

License role	**Description**
Analytics Administrator	Members have the same access permissions as Analytics Explorers. They can also access IBM Software Development Kit; and components in the **Manage** menu, including IBM Cognos Administration.
Analytics Explorer	Members have the same access permissions as Analytics Users. They can also access Exploration, Planning Analytics for Microsoft Excel, Cognos Framework Manager, Cognos Cube Designer and Dynamic Query Analyzer, Jupyter Notebook, and Transformer.
Analytics User	Members can create new reports, dashboards, explorations, stories, new jobs, data server/source connections, or data modules. They can execute reports, respond to prompts, and upload files. They can also access Cognos for Microsoft Office, Cognos Workspace, Cognos Event Studio, Cognos Query Studio, and Cognos Analysis Studio.
Analytics Viewer	Members can read public content. For example, they can subscribe to reports and view dashboards and stories. However, members cannot execute public content. Therefore, they cannot schedule reports.

Default permissions based on licenses

In IBM Cognos Analytics, the licence counter in **Manage** > **Licences** is driven by the capabilities that are granted to a user, group or role.

Note: If you make changes to the default permissions, a user can move up to a different licence than the one that they were granted by default.

For information about how to restrict users based on their licence entitlements, see "Assigning capabilities based on license roles" on page 211.

The following table maps the capabilities that are granted for each license. Capabilities are divided into secured features. A checkmark (✓) indicates that a permission is granted for a specific secured feature. Capabilities marked as "Not Applicable" count as an Analytics Viewer Licence.

Table 59. Cognos Analytics 11.1 capabilities by license roles

Capability	**Secured feature**	**Analytics Viewer**	**Analytics User**	**Analytics Explorer**	**Analytics Administrator**	**Comments**
Adaptive Analytics		✓	✓	✓	✓	Not Applicable

Table 59. Cognos Analytics 11.1 capabilities by license roles (continued)

Capability	Secured feature	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrator	Comments
Administration			✓	✓	✓	
	Adaptive Analytics Administration				✓	Not Applicable
	Administration tasks				✓	
	Collaboration Administration				✓	
	Configure and manage the system				✓	
	Controller Administration				✓	You need a separate IBM Controller Licence
	Data Source Connections		✓	✓	✓	
	Distribution Lists and Contacts				✓	
	Manage Visualizations				✓	
	Metric Studio Administration				✓	You need a separate Metrics Licence
	Mobile Administration				✓	
	Planning Administration				✓	You need a separate IBM Planning Contributor Licence
	PowerPlay Servers				✓	You need a separate PowerPlay license

Table 59. Cognos Analytics 11.1 capabilities by license roles (continued)

Capability	Secured feature	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrator	Comments
	Printers				✓	
	Query Service Administration				✓	
	Run Activities and Schedules				✓	
	Set Capabilities and Manage UI Profiles				✓	
	Styles and Portlets				✓	
	Users, Groups, and Roles				✓	
AI			✓	✓	✓	
	Learning	✓	✓	✓	✓	
	Use Assistant		✓	✓	✓	
Analysis Studio			✓	✓	✓	
11.1.7 Attach Outputs			✓	✓	✓	
Cognos Insight			✓	✓	✓	Not Applicable
Cognos Viewer		✓	✓	✓	✓	
	Context Menu	✓	✓	✓	✓	
	Run with Options		✓	✓	✓	
	Selection	✓	✓	✓	✓	

Table 59. Cognos Analytics 11.1 capabilities by license roles (continued)

Capability	**Secured feature**	**Analytics Viewer**	**Analytics User**	**Analytics Explorer**	**Analytics Administrator**	**Comments**
	Toolbar	✓	✓	✓	✓	
Collaborate		✓	✓	✓	✓	You need separate entitlement of IBM Connections
	Allow collaboration features	✓	✓	✓	✓	You need separate entitlement of IBM Connections
	Launch collaboration tools	✓	✓	✓	✓	You need separate entitlement of IBM Connections
Controller Studio			✓	✓	✓	You need a separate IBM Controller Licence
Dashboard		✓	✓	✓	✓	
	Create/Edit		✓	✓	✓	
Data Manager		✓	✓	✓	✓	Not Applicable
Data sets			✓	✓	✓	
Desktop Tools				✓	✓	
Detailed Errors		✓	✓	✓	✓	
Develop Visualizations			✓	✓	✓	
Drill Through Assistant			✓	✓	✓	
11.1.7 Email		✓	✓	✓	✓	

Table 59. Cognos Analytics 11.1 capabilities by license roles (continued)

Capability	Secured feature	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrat or	Comments
	Email Delivery Option		✓	✓	✓	
	Include link in email	✓	✓	✓	✓	
	Share using email	✓	✓	✓	✓	
	Type in external email	✓	✓	✓	✓	
Event Studio			✓	✓	✓	
Execute Indexed Search		✓	✓	✓	✓	
Executive Dashboard			✓	✓	✓	
	Use Advanced Dashboard Features		✓	✓	✓	
	Use Interactive Dashboard Features		✓	✓	✓	
Exploration			✓	✓	✓	
External Repositories		✓	✓	✓	✓	
	Manage Repository Connections		✓	✓	✓	
	View External Documents	✓	✓	✓	✓	
Generate CSV Output			✓	✓	✓	
Generate PDF Output			✓	✓	✓	
Generate XLS Output			✓	✓	✓	

Table 59. Cognos Analytics 11.1 capabilities by license roles (continued)

Capability	Secured feature	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrator	Comments
Generate XML Output			✓	✓	✓	
Glossary		✓	✓	✓	✓	Integration with IBM InfoSphere Business glossary. Can use directly from Viewer
Hide Entries		✓	✓	✓	✓	
Import relational metadata				✓	✓	
Job			✓	✓	✓	
Lineage		✓	✓	✓	✓	
Manage content					✓	
Manage own data source signons			✓	✓	✓	
Metric Studio			✓	✓	✓	You need a separate Metrics Licence
	Edit View		✓	✓	✓	You need a separate Metrics Licence
Mobile		✓	✓	✓	✓	
Notebook				✓	✓	IBM Cognos Analytics for Jupyter Notebook Server must be installed for Notebook features to be available

Table 59. Cognos Analytics 11.1 capabilities by license roles (continued)

Capability	Secured feature	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrator	Comments
Planning Contributor		✓	✓	✓	✓	You need separate entitlement of IBM Planning Contributor
PowerPlay Studio			✓	✓	✓	You need a separate PowerPlay license
Query Studio			✓	✓	✓	
	Advanced		✓	✓	✓	
	Create		✓	✓	✓	
Report Studio			✓	✓	✓	
	Allow External Data		✓	✓	✓	
	Bursting		✓	✓	✓	
	Create/ Delete		✓	✓	✓	
	HTML Items in Report		✓	✓	✓	
	User Defined SQL		✓	✓	✓	
Save to Cloud			✓	✓	✓	
	Manage Connections				✓	
Scheduling			✓	✓	✓	
	Schedule by Day		✓	✓	✓	
	Schedule by Hour		✓	✓	✓	

Table 59. Cognos Analytics 11.1 capabilities by license roles (continued)

Capability	Secured feature	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrator	Comments
	Schedule by minute		✓	✓	✓	
	Schedule by month		✓	✓	✓	
	Schedule by trigger		✓	✓	✓	
	Schedule by week		✓	✓	✓	
	Schedule by year		✓	✓	✓	
	Schedule by Priority		✓	✓	✓	
Self Service Package Wizard				✓	✓	
Set Entry-Specific Capabilities			✓	✓	✓	
Snapshots			✓	✓	✓	
Specification Execution					✓	
Upload files			✓	✓	✓	
Watch Rules			✓	✓	✓	
Web-based modeling			✓	✓	✓	

Assigning capabilities based on license roles

You can assign capabilities based on license role entitlements. This allows you to restrict users to perform only the functions to which they are entitled.

You must perform the tasks in this order:

1. □ Assign yourself to the System Administrators role
2. □ Restrict access to members of the Cognos namespace
3. □ Remove the Everyone group from the System Administrators role
4. □ Assign users to their predefined roles
5. □ Remove Analytics Viewer capabilities to match license requirements

6. □ Grant Dashboard capabilities to specific roles and users (11.1.4 only)

For information about usage restrictions, see the License Information Documents (http://www-03.ibm.com/software/sla/sladb.nsf/searchlis/?searchview&searchorder=4&searchmax=0&query=(IBM+Cognos+Analytics+11.1) for your program.

1. Assign yourself to the System Administrators role:

As administrator, you must first ensure that your personal userid and any applicable administrative groups are members of the System Administrators role.

Only after you have completed this task can you remove the Everyone group from the System Administrators role.

Procedure

1. Log on to Cognos Analytics using the administrator userid and password.
2. Click **Manage** > **People** > **Accounts**.
3. Select the **Cognos** namespace.
4. Click the More icon ⋯ next to the **System Administrators** role and then click **View members**.
5. Click **Select**.
6. Add your personal userid, and any applicable administrative groups, to the **System Administrators** role.

2. Restrict access to members of the Cognos namespace:

You or the installer can configure access to Cognos Analytics so that only users who are members of any group or role in the **Cognos** namespace can access the application.

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**.

3. Remove the Everyone group from the System Administrators role:

Important: Ensure that you have assigned your userid to the **System Administrators** role before you remove the Everyone group from the System Administrators role. Otherwise, that role will be locked out and no one will be able to make any further administrative changes.

The **Everyone** group is a Cognos group that comprises every userid in the Cognos namespace. By default, after installation the Everyone group is assigned to the System Administrators role. This initial configuration gives every user, even those who are not targeted as administrators, full access to all capabilities.

Purpose

This task removes, from all users, all the capabilities that they were initially assigned from a default installation. After completing this task, your next step will be to assign users and groups to their predefined roles. Users will then have access only to the capabilities that they require for their own role.

Procedure

1. Log on with your personal userid, which you previously assigned to the System Administrators role.
2. Click **Manage** > **People** > **Accounts**.
3. Select the **Cognos** namespace.
4. Click the More icon ⋯ next to the **System Administrators** role and then click **View members**.

5. Click the Remove member icon ⊖ next to **Everyone** group and then click **OK**.

4. Assign users to their predefined roles:

You can now assign users and groups to their predefined roles. These roles are as follows:

- **Analytics Explorers**
- **Analytics Users**
- **Analytics Viewers**

About this task

By assigning each user to their predefined role, you are effectively granting them the capabilities that are associated with their role. To see a matrix of the default capabilities that are available to each predefined role, see "Default permissions based on licenses" on page 204.

Procedure

1. Log on as the System Administrator.
2. Click **Manage** > **People** > **Accounts**.
3. Select the **Cognos** namespace.
4. Click the More icon ⋯ next to the **Analytics Explorers** role and then click 👥 **View members**.
5. Click **Select**.
6. Add the applicable users and groups as members of the **Analytics Explorers** role.
7. Repeat steps **4-6** for these roles:
   - **Analytics Users**
   - **Analytics Viewer**

5. Remove Analytics Viewer capabilities to match license requirements:

About this task

Certain capabilities count toward an Analytics User license that are not intended for Analytics Viewer licensees. By default, however, these capabilities are granted to the **Everyone** group. In this task, you narrow the list of users granted these capabilities to only those who are appropriately licensed. The net effect is that the capabilities are removed from Analytics Viewer licensees, moving in line with their license entitlements.

This task has two parts:

1. Add specific roles to each of these capabilities:
   - **Generate CSV Output**
   - **Generate PDF Output**
   - **Generate XLS Output**
   - **Generate XML Output**
   - **Data sets**
2. Remove the Everyone group from the capabilities listed above. As a result, only the roles that were added in part 1 retain the capabilities.

Procedure

1. Log on as a System Administrator.
2. Click **Manage** > **People** > **Capabilities**.
3. Click the More icon ⋯ next to the **Generate CSV Output** capability and then click **Customize access**.
4. Click the Add member icon ⊕.

5. Click the **Cognos** namespace.
6. Press Ctrl-click to multi-select **Analytics Users**, **Analytics Explorers**, **Authors**, **Modelers**, and **Report Administrators**.
7. Click **Add** and then click **Close**.
8. In the **Permissions** column, for each role you added, select **Access**.
9. Click the Remove member icon ⊖ next to the **Everyone** group and then click **OK**.
10. Repeat steps **3**-**9** for the remaining capabilities:
    - **Generate PDF Output**
    - **Generate XLS Output**
    - **Generate XML Output**
    - **Data sets**
11. Scroll to the **External Repositories** capability.
    a. Click the More icon ⋯.
    b. Click **Customize access**.
    c. Click the Remove member icon ⊖ next to the **Everyone** group.
    d. Click **OK**.
12. Scroll to the **Snapshots** capability.
    a. Click the More icon ⋯.
    b. Click **Customize access**.
    c. Click the Remove member icon ⊖ next to the **Everyone** group.
    d. Click **OK**.

6. Grant Dashboard capabilities to specific roles and users (11.1.4 only):

11.1.4 In Cognos Analytics 11.1.4 only, you must customize the **Dashboard** capability and the **Dashboard** > **Create/Edit** secured feature.

Procedure

1. Log on as a System Administrator.
2. Click **Manage** > **People** > **Capabilities**.
3. Scroll to the **Dashboard** capability.
    a. Click the More icon ⋯.
    b. Click **Customize access**.
    c. Click the Add member icon ⊕.
    d. Click the **Cognos** namespace.
    e. Select **Analytics Viewer**.
    f. Click **Add** and then click **Close**.
    g. In the **Permissions** column for **Analytics Viewer**, select **Access**.
4. Expand the **Dashboard** capability and then click the More icon ⋯ next to **Create/Edit**.
    a. Click **Customize access**.
    b. Click the Remove member icon ⊖ next to the **Analytics Viewer** role.
    c. Click the Add member icon ⊕.

d. Navigate to your namespace, select the appropriate groups or users, and then click **Add**.

e. Click the Add member icon ⊕.

f. Navigate to the **Cognos** namespace.

g. Press Ctrl-click to multi-select **Analytics Users**, **Analytics Explorers**, **Authors**, **Modelers**, and **Report Administrators**.

h. Click **Add** and then click **Close**.

i. In the **Permissions** column, for each user, group, and role that you added, select **Access**.

Upgrade scenario: If your customized roles have the same names as the newer Cognos license roles

If you previously created roles with the same names as the newer Cognos license roles and you are planning an upgrade, consider which capabilities you want to apply to the roles after you upgrade.

For more information, see “License roles” on page 204

- If you want to continue using capabilities that you previously assigned to those roles, you can perform the upgrade without losing those capabilities.
- However, if you want to adopt the capabilities of the new license roles, you must first delete or rename your existing roles **before you upgrade**.

Security settings after installation

Your IBM Cognos software installation must already be configured to use an authentication provider, which is documented in the IBM Cognos Analytics Installation and Configuration Guide.

When the predefined roles are created during the content store initialization, the group **Everyone** is a member of the **System Administrators** role. This means that all users have full access to the content store. To limit that access, you must add trusted users as members of this role, and then remove the group Everyone from its membership.

You must also modify the membership of the predefined roles that include the group **Everyone**, such as **Consumers**, **Query Users**, and **Authors**. Make similar modifications for them as you do for the **System Administrators** role. These modifications should also take the license terms into consideration.

If you do not want to use the predefined roles, you can delete them.

To secure the **Cognos** namespace, modify its initial access permissions by granting access for the required users.

When you set access permissions, you should not explicitly deny access to entries for the group Everyone. Denying access overrides any other security policies for the entry. If you denied access to the entry for Everyone, the entry would become unusable.

To maintain a secure installation, users should be granted only the permissions and capabilities required to allow them to complete their assigned tasks. For example, **Readers** would normally be restricted to read and traverse permissions for **Public Folders** and not be allowed to create reports using any studio. Consumers would normally be restricted to read, traverse and execute permissions.

Certain capabilities, such as **HTML Item In Report** and **User Defined SQL** should be tightly managed. These capabilities are checked during the authoring process as well as when running reports. If a consumer needs to run a report that requires these capabilities, you may be able to use the **Run as Owner** feature to limit the number of system users that require these capabilities. The **Run as Owner** feature uses the report owner's credentials to perform some capability checks and to access data.

For information about granting capabilities for packages, see Object Capabilities.

Securing System Administrators and predefined roles

As one of the first steps when setting up security for the IBM Cognos environment, modify the initial membership of the System Administrators role and other predefined roles.

If the group **Everyone** is a member of a predefined role, remove the group from the role membership.

Procedure

1. From **Manage** > **Administration console**, open **IBM Cognos Administration**.
2. On the **Security** tab, click **Users, Groups, and Roles**.
3. Click the **Cognos** namespace.
4. For the role that you want to modify, in the **Actions** column, click the set properties button.
5. On the **Members** tab, modify the role membership:
   - Ensure that one or more users defined in your authentication provider are members.
   - Remove the group **Everyone** if this group is a member of the role.
   - Click **OK**.
6. On the **Permissions** tab, set access permissions for this role to prevent unauthorized users from creating, updating, or deleting the content, and then click **OK**.
7. For each role that you want to modify, repeat steps 3 to 6.

Securing the Cognos namespace

You can setup the Cognos namespace as follows.

Procedure

1. From **Manage** > **Administration console**, open **IBM Cognos Administration**.
2. On the **Security** tab, click **Users, Groups, and Roles**.
3. In the **Actions** column next to the Cognos namespace, click the set properties button.
4. On the **Permissions** tab, set access permissions for the **Cognos** namespace to prevent unauthorized users from creating, updating, or deleting the content.

   We recommend that you remove the group Everyone. However, you may leave it, depending on your requirements.
5. If you want, select the **Delete the access permissions of all child entries** check box.
6. Click **OK**.

Securing the content store

To ensure its security and integrity, the content store is accessed by the Content Manager service using single database sign-on specified in IBM Cognos Configuration. The database sign-on is encrypted according to your encryption standards. However, the content store security relies not only on the IBM Cognos Analytics security but also on the native database security, operating system security, and network security.

For securing your database, follow these guidelines:

- Secure the database and the database API using the mechanisms provided by the database, the network, and the operating system.
- Assign a limited number of users to maintain the database.
- Use your database native security to grant only minimum permissions to the user accounts that access the database, as follows:
  - Microsoft SQL Server

Users must have create and drop table permissions for the database. Ensure that the user account is a member of the db_ddladmin, db_datareader, and db_datawriter roles, and the owner of their default schema.

- ORACLE

  Users must have permissions to connect to the database. Also, they must be able to create, alter, and drop tables, triggers, views, procedures, and sequences, as well as insert, update, and delete data in the database tables. The permissions must be granted to the user account directly, and not through a group or role membership.

- IBM Db2

  Users must have the create, drop table, CREATETAB, CONNECT and IMPLICITSCHEMA permissions for the database. Also, they must have USE permissions for the USER TEMPORARY tablespace and other appropriate tablespaces associated with the database.

- Sybase Adaptive Server Enterprise

  Users must have create, drop table, create default, create procedure, create rule, create table, and create view permissions for the database.

- Limit the number of users who have read or write access for the Content Manager tables.
- Follow other recommendations on securing the database. For information, see the database documentation.

Chapter 16. Entry Properties

You can control the way an entry appears and behaves by modifying its properties. The properties for entries vary depending on the type of entry and your privileges. For example, reports have properties to control run options while folders do not. If a property is not applicable to the type of entry you are customizing, it will not appear in the **Set properties** page.

General Properties

General properties appear on the **General** tab of the **Set properties** page.

The following table describes the general properties that are available.

Table 60. General entry properties

Property	**Description**
Type	The type of entry.
Owner	The owner of the entry. By default, the owner is the person who created the entry. When the owner no longer exists in the namespace, or is from a different namespace than the current user, the owner shows as `Unavailable`. If you have Set policy permissions, click **Make me the owner** to become the owner of the entry.
Contact	The person responsible for the entry. Click **Set the contact** and then click **Select the contact** to set the contact for the entry or click **Enter an email address** to enter the contact's email address.
Location	The location of the entry in the portal and its ID. Click **View the search path, ID and URL** to view the fully qualified location and the ID of the entry in the content store. Entries are assigned a unique identification (ID) number.
Created	The date the entry was created.
Modified	The most recent date that the entry was modified.
Icon	The icon for the entry. Click **Edit** to specify an alternative icon.
Indexed	The timestamp indicating when the entry was last indexed. The property does not appear if the entry has not been indexed.
Disable this entry	When selected, users that do not have write permissions for this entry cannot access it. The entry is no longer visible in the portal. If an entry is disabled and you have write access to it, the disabled icon appears next to the entry.

Table 60. General entry properties (continued)

Property	Description
Hide this entry	Select this property to hide reports, packages, pages, folders, jobs, and other entries. Hide an entry to prevent it from unnecessary use, or to organize your view. The hidden entry is still accessible to other entries. For example, a hidden report is accessible as a drill-through target. A hidden entry remains visible, but its icon is faded. If you clear the **Show hidden entries** check box in my area options 👤, **My Preferences**, the entry disappears from your view. You must have access to the **Hide Entries** capability granted by your administrator to see this property.
Language	A list of languages that are available for the entry name, screen tip, and description according to the configuration set up by your administrator. Click **Remove values for this language** to remove the entry name, screen tip, and description for a specified language.
Name	The name of the entry for the selected language.
Screen tip	An optional description of the entry. The screen tip appears when you pause your pointer over the icon for the entry in the portal. Up to 100 characters can be used for a screen tip.
Description	An optional description of the entry. It appears in the portal when you set your preferences to use the details view. Details view appears only in Public Folders and My Folders.
Run history	The number of occurrences or period of time to retain run histories for the entry.
Report output versions	The number of occurrences or period of time to keep report outputs. Setting this value to zero (0) saves an unlimited number of versions.
Package	The package that is associated with the entry. If the source package was moved or deleted, the text reads `Unavailable`. Click **Link to a package** to link the entry to a different package.
URL	A URL to either a file or Web site address. This field is visible only if you have read permissions for the entry. If you have write permissions without read permissions, this property is not visible.
Source report	A path to the source entry for a report view. If the source entry was moved or deleted, the text reads `Unavailable`. Click **Report Properties** to view the properties of the source report. Click **Link to a report** to link the entry to a different package.

Table 60. General entry properties (continued)

Property	Description
Source agent	A path to the source entry for an agent view. If the source entry was moved or deleted, the text reads `Unavailable`. Click **Agent Properties** to view the properties of the source report. Click **Link to an agent** to link the entry to a different package.
Advanced routing	Routing tags can be applied to data objects, such as packages, data modules, and uploaded files, and to user groups and roles. These tags, in combination with server groups, are used to specify routing rules for dispatchers.
Gateway	The location of the web server where the originating IBM Cognos product resides. Applies only to Series 7 PowerPlay reports.

Report, Query, Analysis, and PowerPlay Report Properties

Report properties appear on the following tabs of the **Set properties** page:

- the **Report** tab for Reporting reports
- the **Query** tab for Query Studio reports
- the **Analysis** tab for Analysis Studio reports
- the **PowerPlay Report** tab for Series 7 PowerPlay reports

You can select the available paper sizes. In **IBM Cognos Administration** click **Configuration** > **Dispatchers and Services**. Click the define paper sizes button. To add new paper sizes, click **New**. To delete paper sizes, click **Delete**.

The following table describes the report properties that are available.

Table 61. Report, Query, Analysis, and PowerPlay Report properties

Property	Description
Default action	The default action when the report is run.
Formats	The output format to use when the report runs.
PDF options	The options, such as orientation, paper size, and password to open the report, to use when producing PDF output.
Enable accessibility support	Whether to create report output that supports accessibility. Enabling support creates report output that can be read by a screen reader.
Languages	The default language to use for the report data when the report runs.
Prompt values	When the check box is selected, users are prompted to select values to filter data when the report is run.
Current values	The values that are used to filter data when a report is run. For more information, see "Specify the Default Prompt Values for a Report" on page 327.

Table 61. Report, Query, Analysis, and PowerPlay Report properties (continued)

Property	**Description**
Run History	Specifies how long to keep run histories. You can keep run histories for a specific number of runs or for a specific number of days or months.
Report output versions	Specifies how long to keep report output histories. You can keep report output for a specific number of runs or for a specific number of days or months.
Rows per page in HTML Reports	The number of rows you want to appear per Web page in HTML reports
Run as the owner	Whether to use the owner credentials when the report is run. For more information, see "Trusted credentials" on page 181.
Run as the owner: Capabilities only	Whether to use only the owner capabilities and not the owner credentials when the report is run.
HTML options: Open in design mode	Whether to open an HTML-format Series 7 PowerPlay report in design mode.

Job Properties

Job properties appear on the **Job** tab of the **Set properties** page.

The following table describes the job properties that are available.

Table 62. Job properties

Property	**Description**
Steps	A list of steps in the job.
Submission of steps	Whether to run job tasks all at once or in sequence.
Defaults for all steps	Set default values at the job level. Click **Set**, then specify the defaults for all steps of the job. If no defaults are set, the defaults for the individual steps are used.
Run history details level	Click **All** to save the complete history details for the job steps when the run activity completes successfully. The complete history details for the job steps includes **Name**, **Request time**, **Start time**, **Completion time**, **Status**. Click **Limited** to save limited run history details for the job. The limited run history details include the job start time, completion time, status and messages. If the job run fails, the complete history details are saved. The default is **All**. The Run history details level setting for the job overrides the settings of the job steps.

Agent Properties

Agent properties appear on the **Agent** tab of the **Set properties** page.

The following table describes the agent properties that are available.

Table 63. Agent properties

Property	**Description**
Tasks	A list of tasks in the agent.
Default action	The default action when the agent is run.
Prompt values	The values that are used to filter data when an agent is run.
Run as the owner	Whether to use the owner credentials when the agent is run. For more information, "Trusted credentials" on page 181.
Run as the owner: Capabilities only	Whether to use only the owner capabilities and not the owner credentials when the report is run.
Alert list	Whether to allow users to add themselves to the alert list for an agent.

Rule Properties

Use the rule properties to define or modify a watch rule. You can access the rule properties from the **My Watch Items**, **Rules** tab by clicking the set properties icon for a watch rule entry. The properties are located on the **Rule** tab of the **Set Properties** page.

The rule properties specify conditions in saved HTML report output so that when the report is saved and the conditions are satisfied, you are alerted.

The following table describes the rule properties that are available.

Table 64. Rule properties

Property	**Description**
Disable the rule	Whether to disable the watch rule. When disabled, the watch rule is not applied when report output is generated.
Send an alert when the report *reportname* contains:	The name of the report and the rule defined for the watch rule. To edit the definition, click the existing filter condition, such as greater than (>), and in the list that appears, click a different condition. Specify a different value in the box.
For the selected context	The objects in the report to which the rule applies.
Alert type	The type of alert you receive when the rule is satisfied. You can be alerted by email or news item.

Chapter 17. Managing scheduled activities

You can view a list of users' scheduled activities that are current, past, or upcoming on a specific day.

You can filter the list so that only the entries that you want appear. A bar chart shows you an overview of daily activities, by hour. You can use the chart to help choose the optimum date for rescheduling activities. You can set run priority for entries. You can also view the run history for entries, specify how long to keep run histories, and rerun failed entries.

You can see who ran each entry and perform actions on entries as required. For example, you may want to cancel or suspend a user's large job if it is holding up important entries in the queue. You can also override the priority of an entry instance or you can change it permanently for an entry itself.

If you switch views, you must refresh to see current data. For example, if you switch from **Past Activities** to **Upcoming Activities**, you must refresh to see current data in the panes.

Administrators can use the **Manage** > **Activities** administration function, or **IBM Cognos Administration** to manage activities for all user entries.

Scheduling a report

11.1.7 You schedule a report to run it at a later time or at a recurring date and time.

If you no longer need a schedule, you can delete it. You can also disable it without losing any of the scheduling details. You can then enable the schedule at a later time.

If you want, you can change the current schedule owner by changing the credentials for a scheduled entry. For more information, see "Taking ownership of a schedule" in the *Managing User Guide*.

Before you begin

To use this functionality, you must have the required permissions for the **Scheduling** capability. You can see which capabilities are available with your assigned license role in the topic "Default permissions based on licenses" in the *Managing User Guide*.

To schedule a report, you also require the following access permissions for any data sources used by the report:

- dataSource - Execute and Traverse
- dataSourceConnection - Execute and Traverse

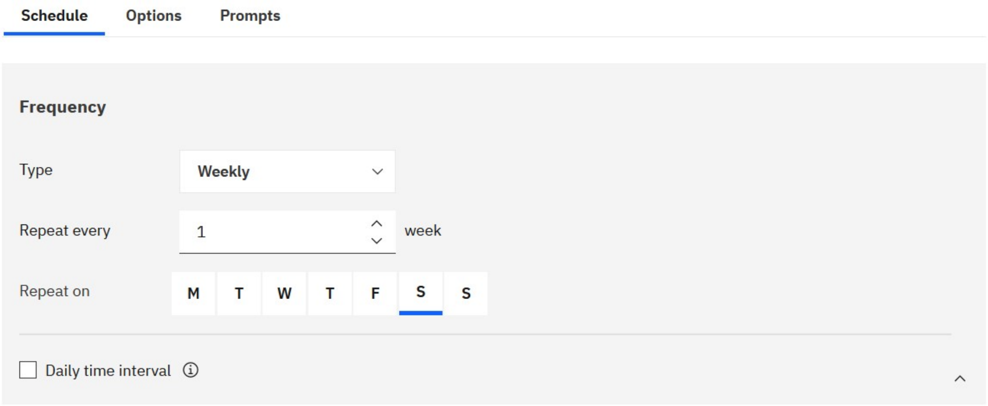
  With only Execute access, you are prompted to log on to the database.
- dataSourceSignon - Execute

To schedule reports to run in the restricted CVS, PDF, XLS, or XML output formats, you require the generate output capability for the specific format. For more information, see *Report formats* in the *Administration and Security Guide*.

To set priority for an entry, you must have the required permissions for the **Scheduling priority** secured feature. For more information, see Capabilities.

Procedure

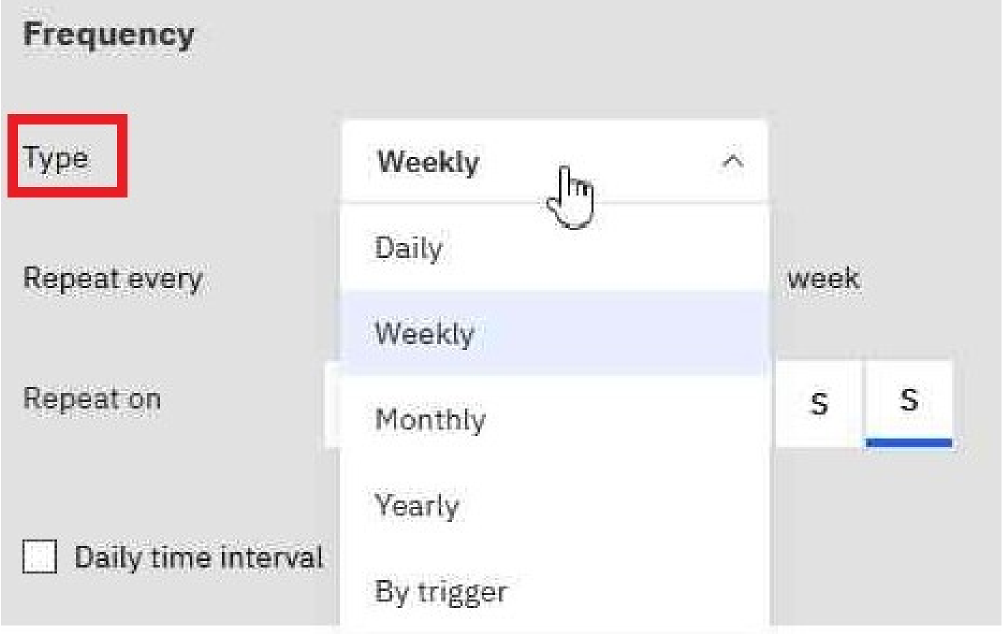
1. Click the report's More icon ⋯, and then click **Properties**.
2. In the **Properties** pane, click the **Schedule** tab, and then:
   - Click **Create schedule**.



Tip: Available options change with each selection. Wait until the pane is updated before you choose additional settings.

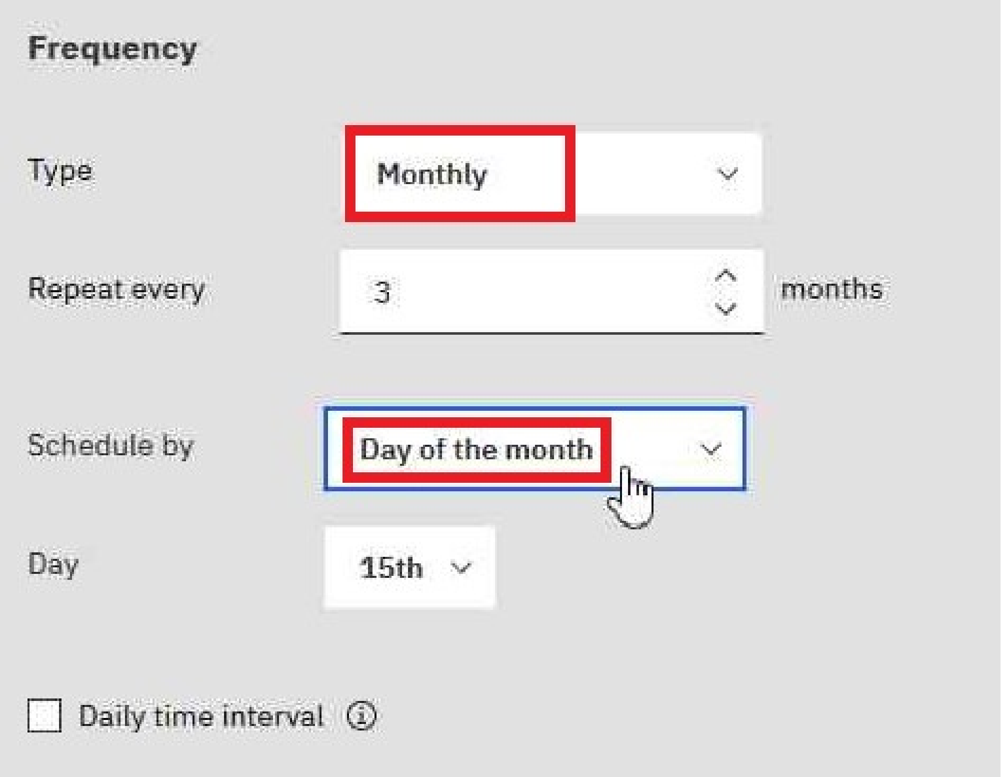
3. In the **Frequency** section, specify when and how frequently the report runs:

   - Select the **Type** of time unit to measure the interval between meetings.



Tip: Try selecting different **Type** values and then watch how the other fields change. For example, selecting **Daily**, **Weekly**, or **Monthly** allows you to select a **Repeat every** *integer*. You can therefore choose an interval which is a multiple of the time unit that you chose, for example, "every 3 weeks".

   - If you are selecting a **Type** value of **Monthly**,



Frequency

Type: Monthly

Repeat every: 3 months

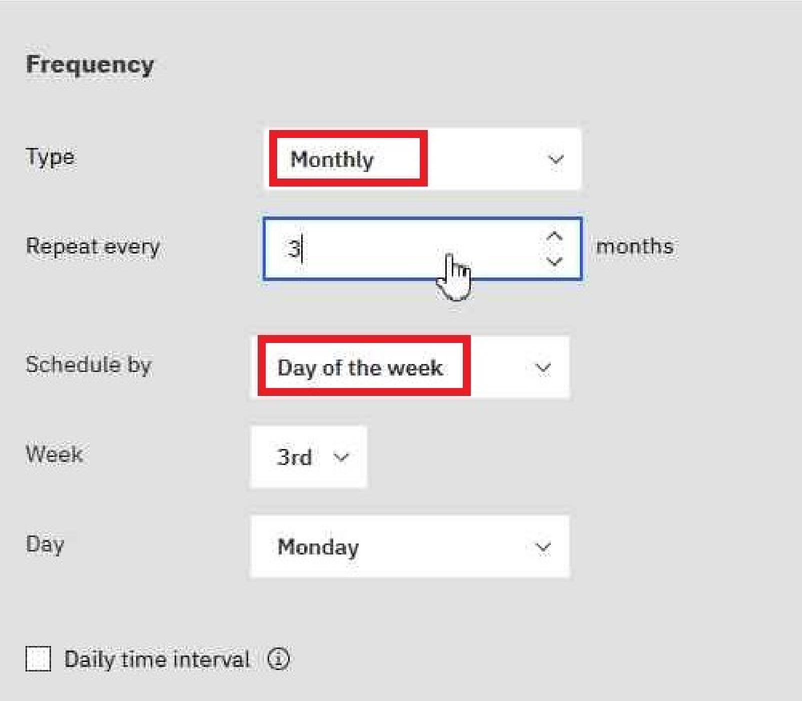
Schedule by: Day of the month

Day: 15th

□ Daily time interval

–

Select **Day of the Month** in the **Schedule by** field so that you can choose, for example, "Repeat every 3 months on the 15th of the month" (see figure above).



Frequency

Type: Monthly

Repeat every: 3 months

Schedule by: Day of the week

Week: 3rd

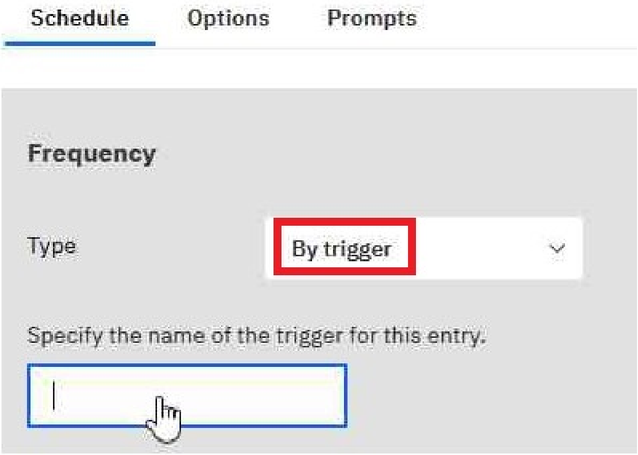
Day: Monday

□ Daily time interval

–

Select **Day of the week** in the **Schedule by** field so that you can choose, for example, "Repeat every 3 months on the 3rd Monday of the month" (see figure above).

- If you are selecting a **Type** value of **By trigger**,



Frequency

Type: By trigger

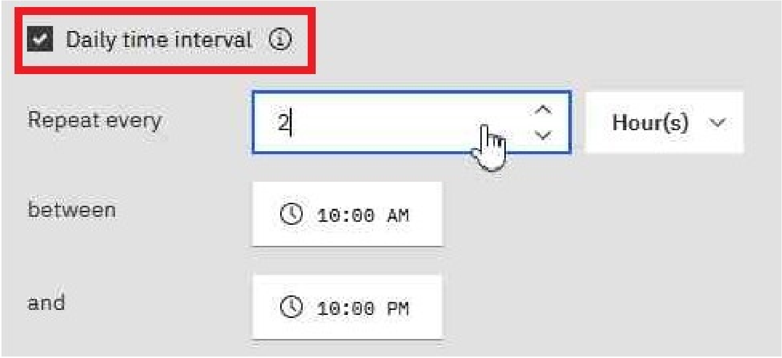
Specify the name of the trigger for this entry.

Tip: If a report is scheduled by a trigger, it can run only if you have already set up a trigger occurrence. For more information, see "Set Up a Trigger Occurrence on a Server" in the *Administration and Security Guide*.

In the field pictured above, enter the name of the trigger occurrence, for example, `trigger.bat`.

4. If you want to select a daily frequency for your scheduled entries:

   - Select the **Daily time interval** check box.



☑ Daily time interval

Repeat every: 2 Hour(s)

between: 10:00 AM

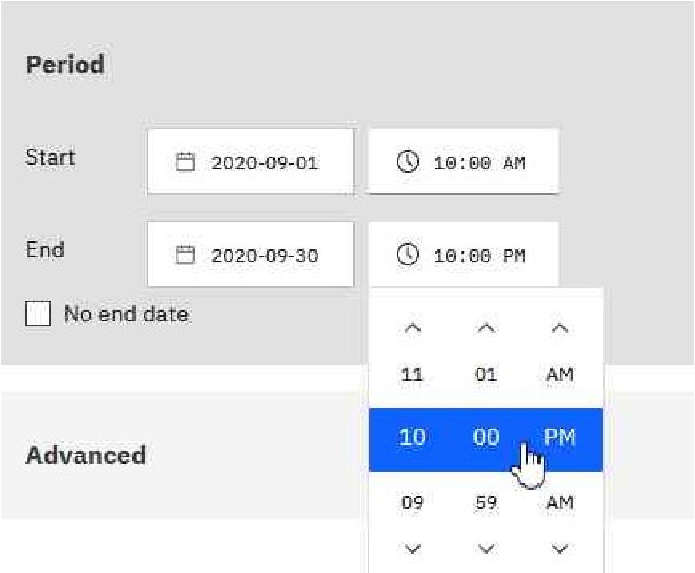
and: 10:00 PM

Tip: Specify the frequency and the period during the day in which the report runs. For example, "every 2 hours between 10:00 AM and 10 PM" (see figure above).

We recommend that you select an hourly frequency that divides evenly into the 24-hour clock. This ensures that your report runs at the same times each day. If you select an hourly frequency that does not divide evenly into the 24-hour clock, your report runs at different times on subsequent days.

5. If you want to set the time period within which the first and last runs of the report will take place:

   - Scroll to the **Period** section.



Period

Start 2020-09-01 10:00 AM

End 2020-09-30 10:00 PM

□ No end date

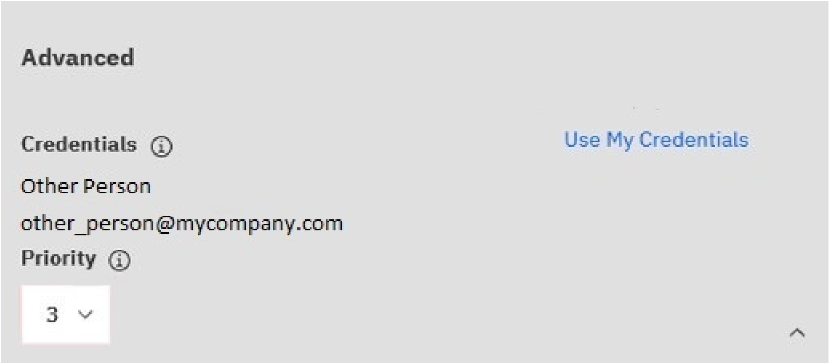
Tip: In the example shown above, the first report run will occur on September 1 at 10:00 AM and the last report run will end on September 30 at 10:00 PM.

Set the date and time for both the start and the end of the period.

If you don't enter anything in the **Period** section, by default the period begins as soon as you save the schedule and there is no end date.

6. If you want to change the credentials or priority of the schedule:

   - Click the **Advanced** section.



Advanced

Credentials

Other Person

other_person@mycompany.com

Priority 3

Tip:

About the Credentials field

Credentials show the current schedule owner. If you are not already the schedule owner, you can click **Use My Credentials** and make temporary changes to the schedule.

For more information, see " Taking ownership of a schedule" in the *Managing User Guide*.

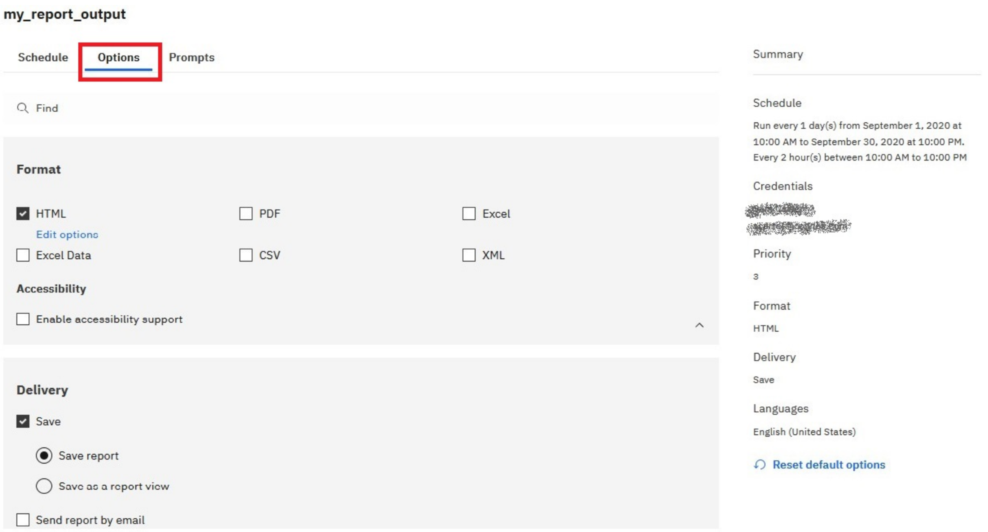
About the Priority field

If you are assigned the Scheduling Priority capability, you can select a priority from 1 to 5 for the scheduled entry to run. Priority 1 runs first.

For more information, see " Changing the entry run priority" in the *Managing User Guide*.

7. To see the default format, delivery method, and language of your report:

   - Click the **Options** tab.



my_report_output

Schedule | Options | Prompts

Find

Format

☑ HTML
Edit options
☐ PDF
☐ Excel
☐ Excel Data
☐ CSV
☐ XML

Accessibility

☐ Enable accessibility support

Delivery

☑ Save

● Save report
○ Save as a report view

☐ Send report by email

Summary

Schedule
Run every 1 day(s) from September 1, 2020 at 10:00 AM to September 30, 2020 at 10:00 PM. Every 2 hour(s) between 10:00 AM to 10:00 PM

Credentials
[redacted]

Priority
3

Format
HTML

Delivery
Save

Languages
English (United States)

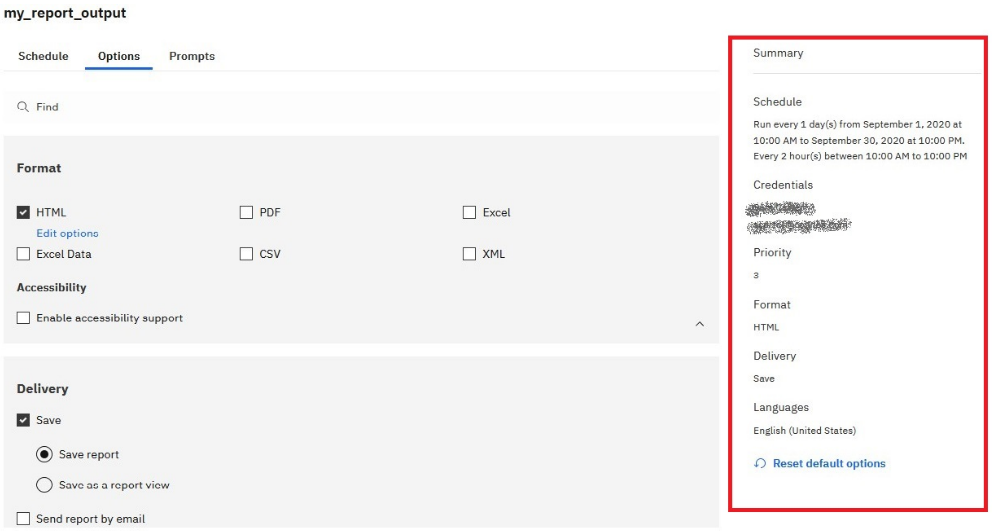
Reset default options

Tip:

The default options are displayed:

- **Format**: HTML only, accessibility support disabled
- **Delivery**: Save report only
- **Languages**: English only

- Did you notice the **Summary** pane?



my_report_output

Schedule | Options | Prompts

Find

Format

☑ HTML
Edit options
☐ PDF
☐ Excel
☐ Excel Data
☐ CSV
☐ XML

Accessibility

☐ Enable accessibility support

Delivery

☑ Save

● Save report
○ Save as a report view

☐ Send report by email

Summary

Schedule
Run every 1 day(s) from September 1, 2020 at 10:00 AM to September 30, 2020 at 10:00 PM. Every 2 hour(s) between 10:00 AM to 10:00 PM

Credentials
[redacted]

Priority
3

Format
HTML

Delivery
Save

Languages
English (United States)

Reset default options

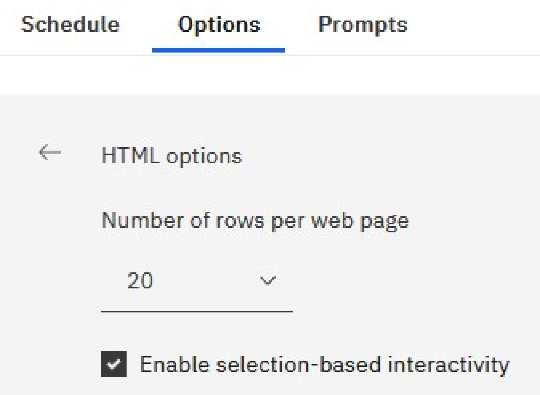
Tip:

As you build your schedule, the **Summary** pane on the right of your window uses natural language to describe all of your selections in real time.

At any time, you can click **Reset default options** to clear the options that you set on every tab.

8. If you want, change the **Format** options:

- If you select HTML format, you can click **Edit options**.



Schedule | Options | Prompts

HTML options

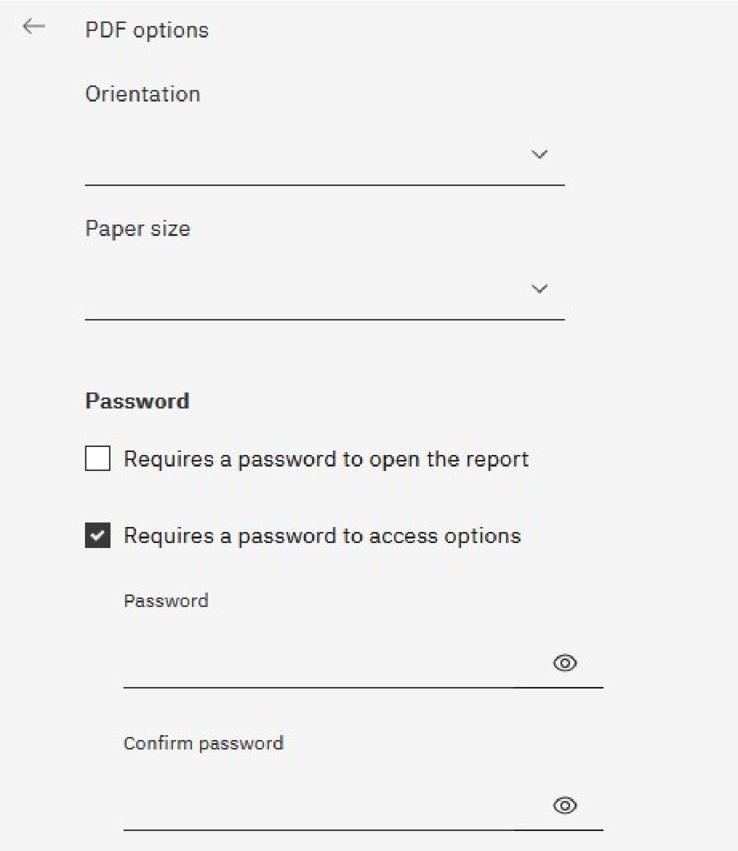
Number of rows per web page: 20

☑ Enable selection-based interactivity

Tip:

If you want to drill up and down in a report or drill through to other reports, you must select the **Enable selection-based interactivity** check box. However, if your report is very large, you may want to deselect the check box to shorten the time that it takes the report to run.

- If you select PDF format, you can click **Edit options**.



PDF options

Orientation

Paper size

Password

☐ Requires a password to open the report

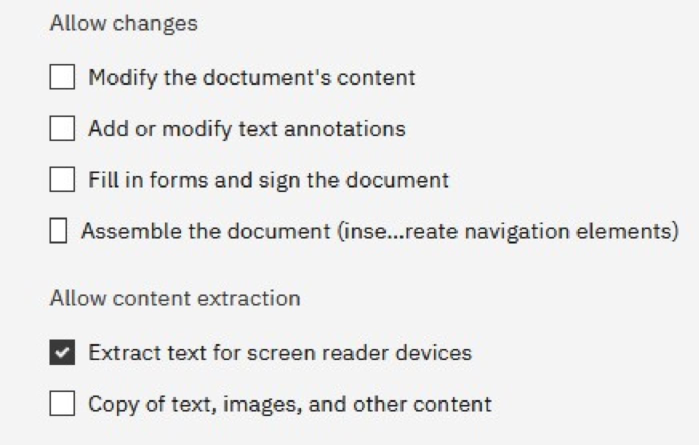
☑ Requires a password to access options

Password

Confirm password

Figure 5. PDF options - part 1

Tip: You can create a password to add extra security to your report. This is in addition to the permissions that users are granted by their capabilities.



Allow changes

□ Modify the doctument's content

□ Add or modify text annotations

□ Fill in forms and sign the document

□ Assemble the document (inse...reate navigation elements)

Allow content extraction

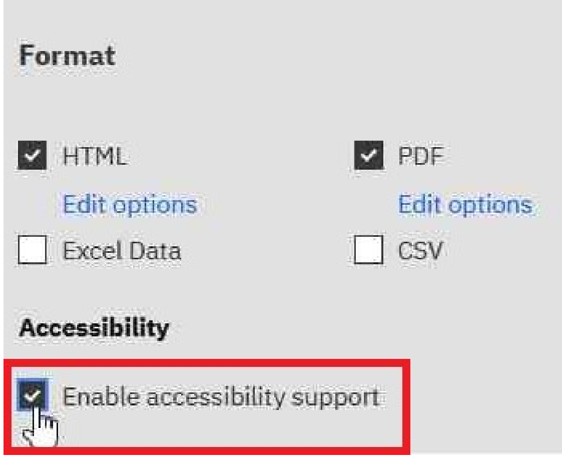
☑ Extract text for screen reader devices

□ Copy of text, images, and other content

Figure 6. PDF options - part 2

Tip: You can limit the types of changes that other users can make to the report.

- If you select the **Enable accessibility support** check box.



Format

☑ HTML
Edit options

☑ PDF
Edit options

□ Excel Data

□ CSV

Accessibility

☑ Enable accessibility support

Figure 7. PDF options - part 1

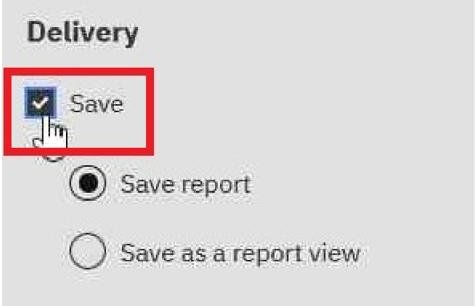
Tip: You can make your report output accessible. Accessible reports contain features, such as alternate text, that allow users with disabilities to access report content using assistive technologies, such as screen readers.

In IBM® Cognos® applications, you can create accessible output for reports, jobs, steps within jobs, and scheduled entries in PDF and HTML.

Accessible reports require more report processing and have a greater file size than non-accessible reports. Consequently, making reports accessible can have a negative impact on performance.

9. You can change the **Delivery** options:

- If you want to save the report in Cognos Analytics, you have two options.



Delivery

☑ Save

● Save report

○ Save as a report view

Figure 8. PDF options - part 1

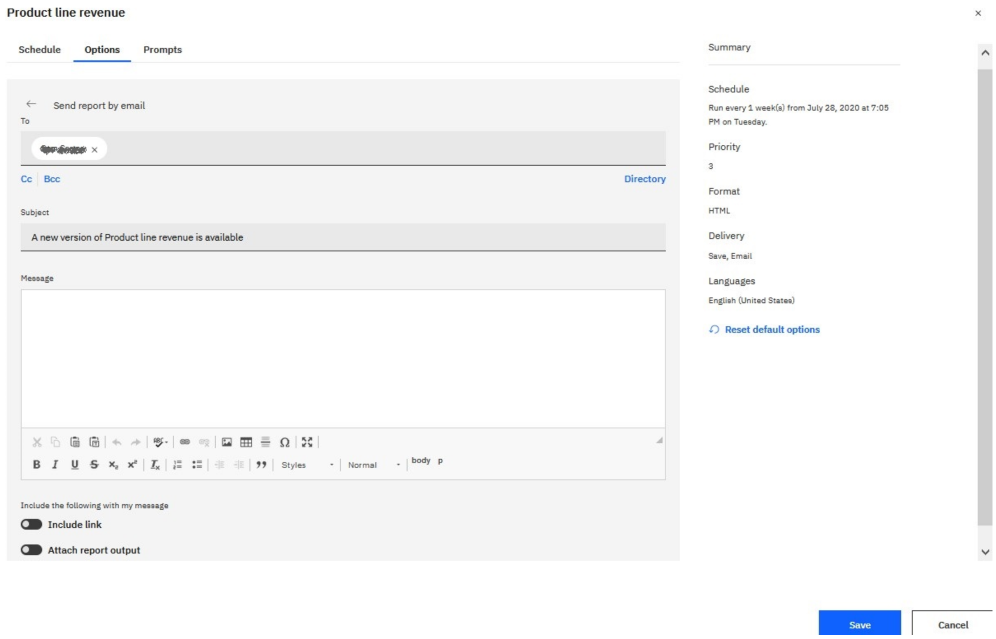
Tip:

– **Save report**. This option is selected by default.

– **Save as a report view**. Unlike saving the report, you can change the name or destination folder of the report view. A report view uses the same report specification as the source report, but has different properties such as prompt values, schedules, delivery methods, run options, languages, and output formats.

  Creating a report view does not change the original report. You can determine the source report for a report view by viewing its properties. The report view properties also provide a link to the properties of the source report.

- If you select **Send report by email** and then click **Edit details**.



Product line revenue

Schedule | Options | Prompts

← Send report by email

To: [redacted] ×

Cc | Bcc | Directory

Subject: A new version of Product line revenue is available

Message:

Include the following with my message

Include link

Attach report output

Summary

Schedule: Run every 1 week(s) from July 28, 2020 at 7:05 PM on Tuesday.

Priority: 3

Format: HTML

Delivery: Save, Email

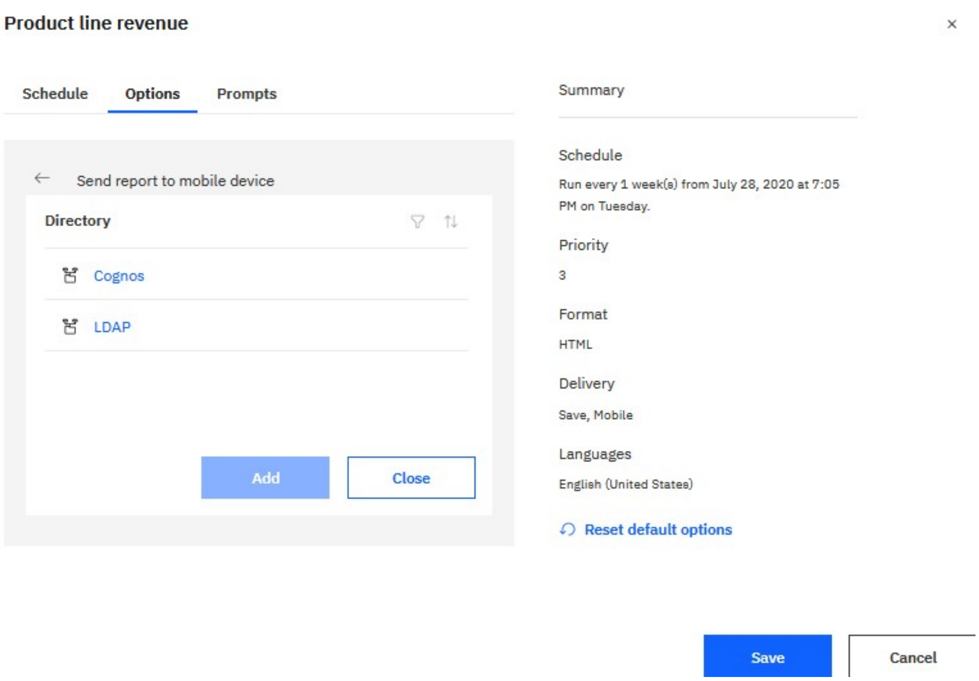
Languages: English (United States)

Tip:

An email window appears, in which you can enter recipients' names, if you have permission. Otherwise, you can choose your email recipients from your local LDAP directory. If your directory is very large, you can use search, filter and sort functions to quickly find your recipients.

After you enter your message, and you have the correct permissions, you can attach the report output to the email. Or you can add a link that your recipient can click to see the report.

- If you select **Send report to mobile device**.


Product line revenue

Schedule | Options | Prompts

← Send report to mobile device

Directory

Cognos

LDAP

Add | Close

Summary

Schedule

Run every 1 week(s) from July 28, 2020 at 7:05 PM on Tuesday.

Priority

3

Format

HTML

Delivery

Save, Mobile

Languages

English (United States)

Reset default options

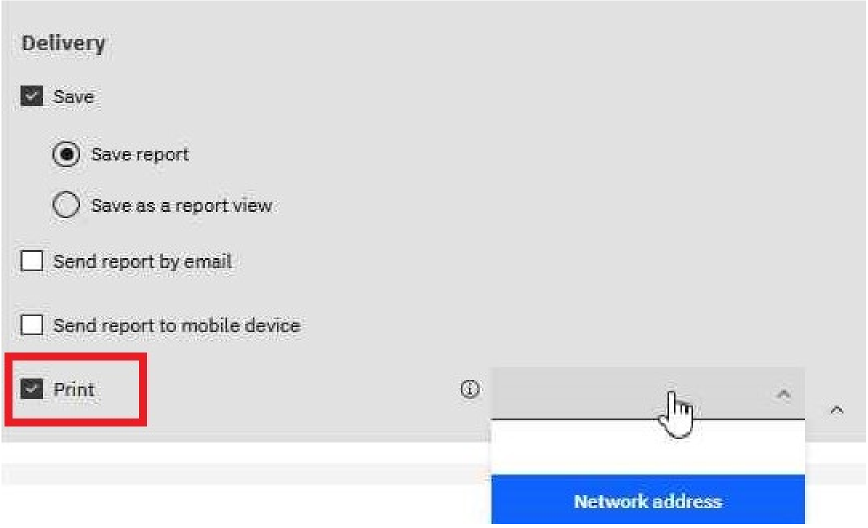
Save | Cancel

Tip:

This option is available only to users of Cognos Analytics on Demand or Cognos Analytics on Cloud Hosted.

Similar to the email option, you can find your recipient in the Directory. When the report is run, it will be sent to the mobile device of the recipient via Cognos Analytics for Mobile.

- If you select **Print**.


Delivery

☑ Save

● Save report

○ Save as a report view

□ Send report by email

□ Send report to mobile device

☑ Print

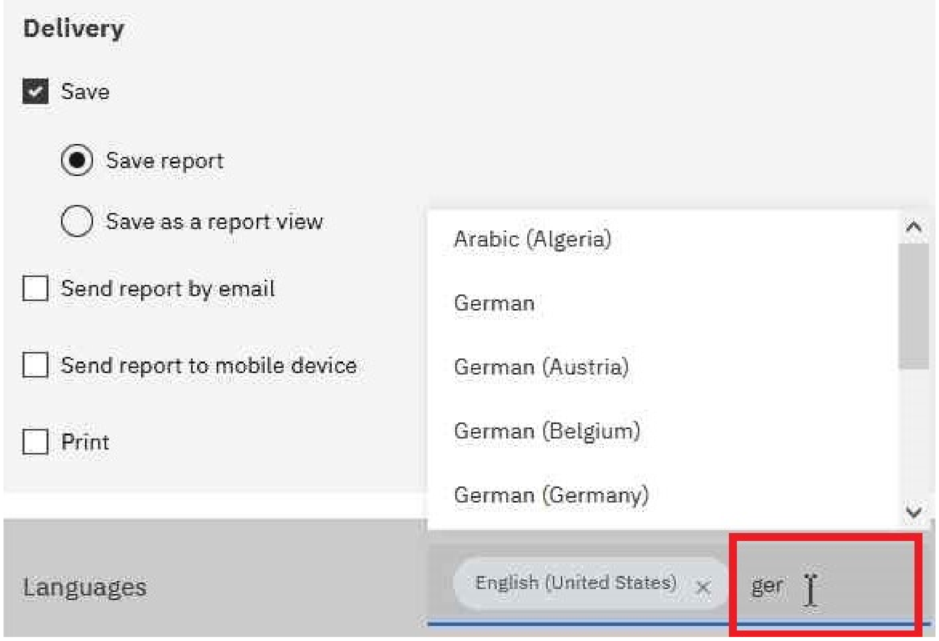
Tip: It may be convenient for you to have a printed copy of a report.

You may need to review a report when your computer is not available, or you may need to take a copy of a report to a meeting.

To print reports, you must have the Generate PDF Output capability.

Select a printer from the list or enter a valid printer name, location, or address and then click **Add**.

- If you want your output in languages other than English (the default).



Delivery

☑ Save

● Save report

○ Save as a report view

□ Send report by email

□ Send report to mobile device

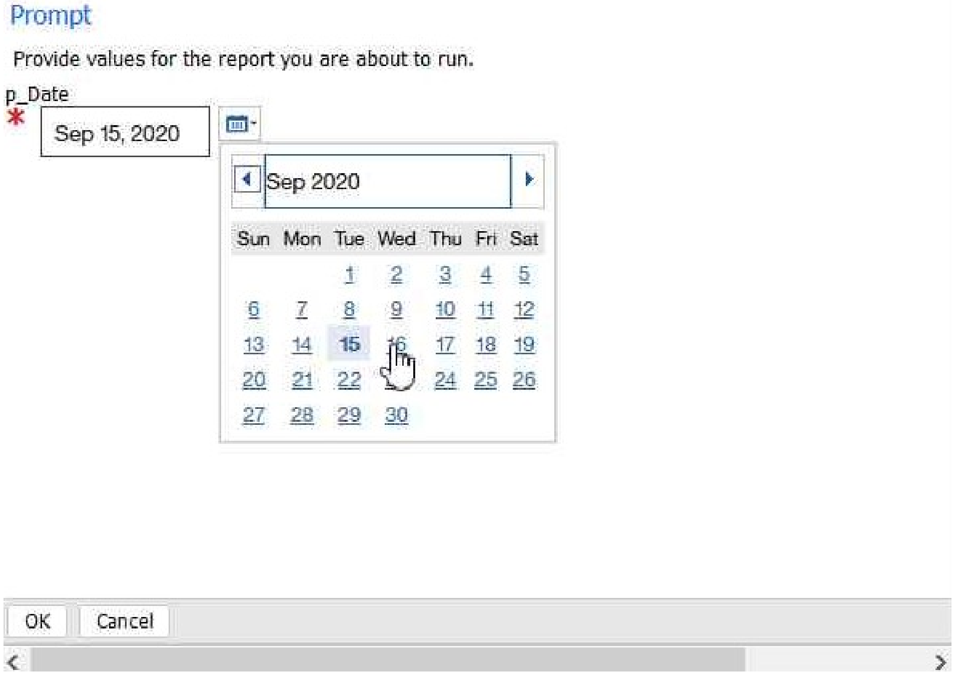
□ Print

Languages: English (United States) × ger

Tip: Start typing the name of the language in the **Languages** field. A dynamic list of languages appears, from which you can select the one you want.

10. If your report has prompts:

    - Click the **Prompts** tab and then click **Set values**.



Prompt

Provide values for the report you are about to run.

p_Date

* Sep 15, 2020

Sep 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Tip: In the example **Prompt** window shown above, the **p_Date** parameter prompts for a date value.

11. Click **Save**.

Results

A schedule is created and the report runs at the next scheduled time.

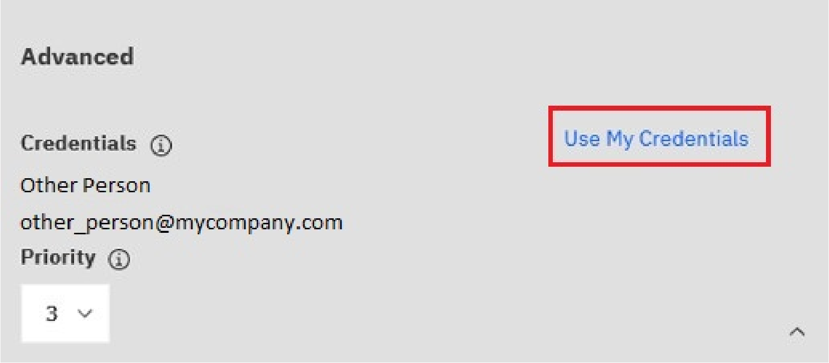
Taking ownership of a schedule

When you edit a schedule owned by someone else, you can take ownership of the schedule during your current Cognos Analytics session.

For example, a schedule owner is on vacation, but you don't have access permissions to change the schedule. You can take temporary ownership of the schedule and change some scheduling options while they are away. However, the schedule's credentials change back to the original owner as soon as you exit the session.

Procedure

1. Click the report's More icon ⋯, and then click **Properties**.
2. Click the **Schedule** tab, and then click **Edit**.
3. On the **Schedule** tab, scroll down and click the **Advanced** section.

   Advanced

   Credentials ⓘ

   Other Person

   other_person@mycompany.com

   Priority ⓘ

   3

   If the schedule is owned by someone else, a **Use My Credentials** link appears.
4. Click **Use My Credentials**.

   Your name appears in the **Credentials** field.
5. Make changes to the schedule.
6. Click **Save** to save the schedule.

Results

The schedule is updated with the changes you made. The schedule's credentials change back to the original owner as soon as you exit the session.

Changing the entry run priority

You can assign a priority of 1 to 5 to scheduled entries.

For example, an entry with priority 1 runs before an entry with priority 5. If there is more than one entry with the same priority, the one that arrived in the queue first runs first. The default priority is 3.

Before you begin

You must have the Scheduling Priority capability to change the entry run priority.

About this task

Interactive entries always run immediately and priority cannot be changed once they are running.

You set the priority for an entry when you schedule it . When an entry is in the current, upcoming, or scheduled queue, you can change the priority.

You may want to set a low priority for entries that take a long time to run so that other entries in the queue are not delayed.

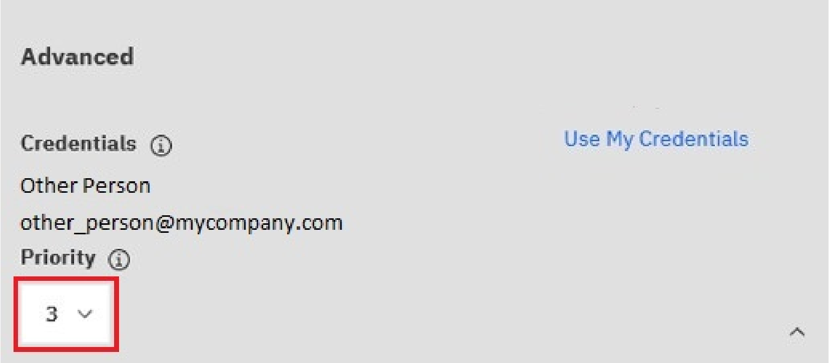
When you schedule a job, you set the priority for the whole job, not for individual entries within the job. You may want to set a low priority for a job with many entries so that other entries in the queue are not delayed.

You schedule priority for the parent job. When the job runs, all the child entries inherit the priority of the parent. When the job is in the queue and is not yet running, you can update the priority. You cannot do this for the individual entries in the job. Changing the priority of the job changes the priority of all its child entries. You can view the run history of a job while it is executing and see which of its entries have completed, are executing, or are pending.

The priority of entries in the queue does not affect an entry that is already running. That entry completes and then the queue priority is checked for the next entry to run.

Procedure

1. Click the report's More icon ⋯, and then click **Properties**.
2. Click the **Schedule** tab, and then click **Edit**.
3. On the **Schedule** tab, scroll down and click the **Advanced** section.



Advanced

Credentials ⓘ

Use My Credentials

Other Person

other_person@mycompany.com

Priority ⓘ

3 ⌄

4. Click the down chevron in the Priority field and then select a number from 1 to 5.
5. Click **Save** to save the schedule.

Managing upcoming activities for a specific day

You can choose to view a list of all upcoming activities that are scheduled for a specific day.

Each entry is listed by name and shows the request time and the priority. A bar chart show the total number of scheduled and canceled entries for each hour of the day. The chart legend shows the total number of scheduled and canceled entries for the day.

You can sort the **Request time**, **Status**, and **Priority** columns. You can choose to view a list of background activities or interactive activities.

Each entry shows the user who scheduled it. You can sort by user.

You can cancel scheduled runs of entries, reschedule entry runs that have been canceled, and set priorities. You can suspend entries indefinitely or suspend them until a specific date. For more information see, "Suspended activities" on page 241

You can click the **Show Details** ▤ icon to see more information. For each entry, this displays **Last Execution Response Time** and **Path**.

You can filter the entries to display only those you want. You can choose the date and time for which you want to view upcoming activities. You can filter by status, priority, type, and scope.

You can also filter by the user that scheduled the entry, and the entry owner.

You can filter to determine how many scheduled entries are currently suspended. For more information, see "Suspended activities" on page 241

You can change the priority of an entry in the queue "Changing the entry run priority" on page 236.

Procedure

1. From the **Manage** menu, click **Administration console**.
2. On the **Status** tab, click **Upcoming Activities**.
3. In the **Filter** section, click the filtering options that you want to use.

   Tip: If you want to use advanced filtering options, click **Advanced options**. To reset all selections to the default settings, click **Reset to default**.
4. Click **Apply**.

   - The list shows the entries that you selected.
   - The filter status line shows the criteria used to generate the list.
   - The bar chart shows the scheduled and canceled entries by hour for the specified day.

   The list of entries, filter status line, and chart are updated whenever you redefine the filter and click **Apply**. The list of entries and filter status line do not change when you browse the chart to a different date.
5. To perform an action on an individual entry, click the **Actions** arrow for the entry and select the action. To perform an action on several entries, select the check box for the entries you want and then click one of the following buttons on the toolbar.

   The following table specifies the actions available for entries and the associated icons:

Table 65. Manage upcoming activities for a specific day actions and icons

Action	Icon
Show Details (top right-hand corner)	☰
Hide Details (top right-hand corner)	☰
Cancel the run (**Actions** menu beside entry)	✱
Suspend entries (**Actions** menu beside entry)	⏸
Run suspended entries (**Actions** menu beside entry)	▶
Re-schedule a run that was canceled (**Actions** menu beside entry)	📅
Set Priority (**Actions** menu beside entry)	▤

Tip: To select all entries in the list, select the check box for the list.

Managing past activities from the Administration console

Past activities are entries that have finished processing in IBM Cognos software.

Each entry is listed by name and shows the request time and the status. You can sort the **Request time** and **Status** columns. The bar chart shows the total number of entries, broken down by status. If an entry has failed, a button appears showing the severity of the error. The user who ran the entry is also listed.

You can filter the entries to display only those you want. You can choose to view a list of activities that occurred over a specified length of time, such as the last four hours or the last day, or you can specify a date or time range. You can filter by status, type, and scope. You can also filter by the user who ran the entry, the user who owns the entry, and the dispatcher where the activity ran.

You can view the run history "Viewing the run history of entries" on page 243.

Procedure

1. From the **Manage** menu, click **Administration console**.
2. On the **Status** tab, click **Past Activities**.

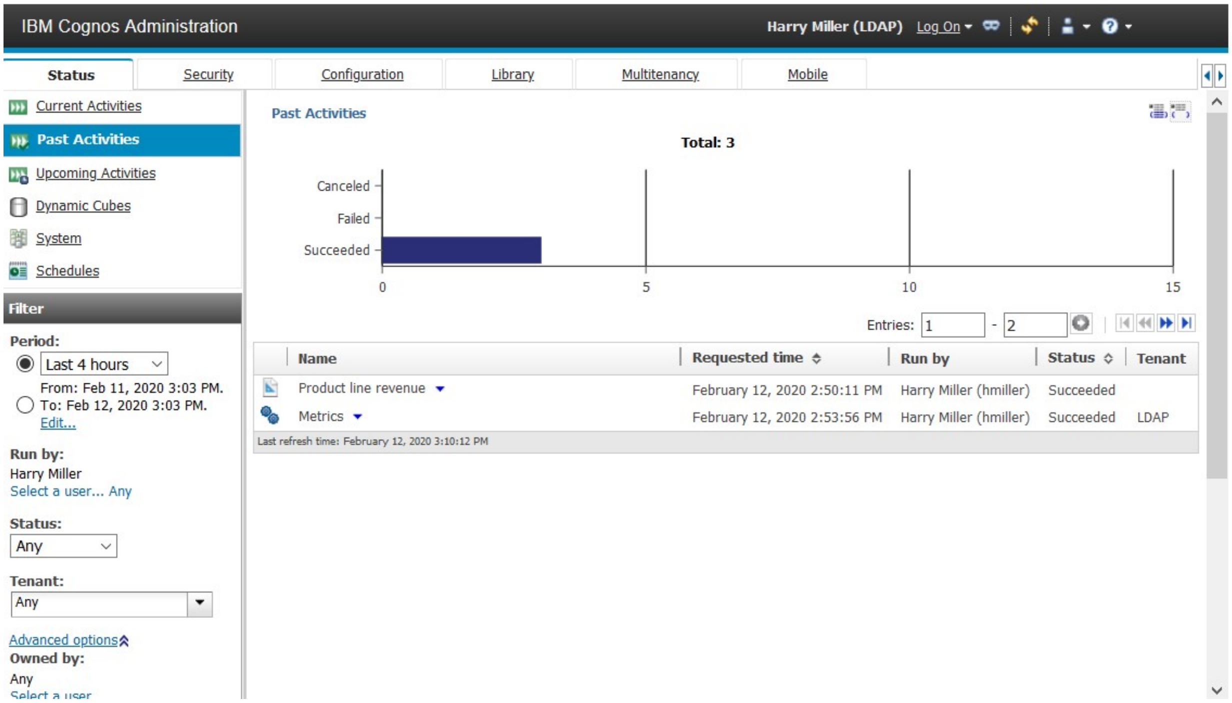
   A chart appears, showing when past activities were run and whether they succeeded, failed, or were canceled. Below the chart, details about the activities are listed.
3. To filter the activities that appear in the chart and the list, go to the **Filter** panel and select the attributes you want.

   Tip: You can filter by the following attributes:

   - the period within which the activities ran
   - the user who performed the activity
   - the activity owner
   - the activity status
   - the activity type
   - the dispatcher that ran the activity
   - the scope of folders in **Team content** where the item resides

   The following diagram shows an example of how past activities are displayed from the Administration console. In this example, note the following:

   - The list is filtered to show only reports run by Harry Miller.
   - The job named Metrics contains two reports that are run as job steps. However, these two report runs do not appear in the list of activities.



Period:
● Last 4 hours
From: Feb 11, 2020 3:03 PM.
○ To: Feb 12, 2020 3:03 PM.
Edit...

Run by:
Harry Miller
Select a user... Any

Status:
Any

Tenant:
Any

Owned by:
Any
Select a user

Entries: 1 - 2

Name	Requested time	Run by	Status	Tenant
Product line revenue	February 12, 2020 2:50:11 PM	Harry Miller (hmiller)	Succeeded	
Metrics	February 12, 2020 2:53:56 PM	Harry Miller (hmiller)	Succeeded	LDAP

Last refresh time: February 12, 2020 3:10:12 PM

4. If an activity failed, you can pause over the error button next to the status to see the severity of the error.
5. To perform an action on an individual entry, click the **Actions** arrow for the entry and select the action.

   To perform an action on several entries, click either the **Show Details** icon or the **Hide Details** icon in the toolbar.

Managing current activities

Current activities are entries that are currently being processed in IBM Cognos software.

Each entry is listed by name and shows the request time, the status, and the priority for background activities. The bar chart shows the total number of entries, broken down by the number of pending, executing, waiting, and suspended entries. When the activity is processing, the process number is displayed.

You can sort the **Request time**, **Status**, and **Priority** columns. You can choose to view a list of background activities or interactive activities. The user who ran the entry is also listed. You can sort by user.

You can suspend background entries and release them later when you want them to run. You can permanently cancel runs for entries that have one of the following statuses:

- pending in the queue
- executing
- suspended
- waiting for a process external to IBM Cognos software to complete

You can filter the entries to display only those you want. You can choose to display only those entries with a specific status or priority, or entries of a specific type or scope.

For interactive current entries, you can filter by status and the dispatcher where the activity is running. For background current entries, you can filter by status, priority, type, scope, user who ran the entry, user who owns the entry, and dispatcher.

When an entry is currently running, the dispatcher, process ID, and start time is displayed. Note that process ID and dispatcher of current background entries might be unavailable when the activity first appears. Refresh the page to see the updated process ID and dispatcher.

If you cancel an entry that contains other entries, such as a job or an agent, steps or tasks that have not yet been completed are canceled. However, steps or tasks that have already completed remain completed.

You can change the priority of entries "Viewing the run history of entries" on page 243"Changing the entry run priority" on page 236 and view the run history .

Procedure

1. From the **Manage** menu, click **Administration console**.
2. On the **Status** tab, click **Current Activities**.
3. In the **Filter** section, click **Background activities** or **Interactive activities**, and specify the filtering options that you want to use.

   Tip: If you want to use advanced filtering options, click **Advanced options**. To reset all selections to the default settings, click **Reset to default**.
4. Click **Apply**.

   The list shows the entries that you selected.
5. To perform an action on an individual entry, click the **Actions** arrow for the entry and select the action. To perform an action on several entries, select the check box for the entries you want and then click one of the following buttons on the toolbar.

   The following table specifies the actions available for entries and the associated icons:

Table 66. Manage current activities actions and icons

Action	**Icon**
Show Details (top right-hand corner)	☰
Hide Details (top right-hand corner)	☰
Cancel the run (**Actions** menu beside entry)	✖
Suspend the run (**Actions** menu beside entry)	⏸
Run suspended entries (**Actions** menu beside entry)	▶
Set Priority (**Actions** menu beside entry)	▦

Tip: To select all entries in the list, select the check box for the list.

Suspended activities

You can suspend entries to respond to system requirements and resume them later.

After suspending entries, you can view a list of entries that are suspended indefinitely.

You can resume suspended entries even after the original execution time has lapsed. For example, if you schedule a report for 9:00 am, then suspend it, you can restart the report at 9:30 am.

The upcoming activities bar chart helps you determine when to reschedule entries. By browsing the upcoming dates in the chart, you can see the number of entries for a specific day. When you pause the pointer over a specific hour in the day, you can find the number of entries for that hour. Use this to find a date when demand is low and reschedule the entry to that date. The chart columns show the total number of scheduled and canceled entries for each hour of the day. The chart legend shows the total number of scheduled, canceled, and suspended entries for the day.

Suspending entries

You can suspend activities.

For example, if your system tends to be overloaded at certain times, you can reduce the workload and avoid bottlenecks during these peak times by suspending entries indefinitely or rescheduling them for a later time.

Procedure

1. From the **Manage** menu, click **Administration console**.
2. On the **Status** tab, click **Upcoming Activities**.
3. In the **Filter** section, for **Day** select a date, and for **Status** click **Scheduled**.
4. Click **Apply**.

   The list shows the scheduled entries for the selected date. Because entries are backlogged on that date, you want to suspend certain entries indefinitely and reschedule others. You want to browse the upcoming dates in the chart and choose another date for the suspended entries.
5. In the chart, click the next and previous icons to browse the upcoming dates. The chart shows both scheduled and canceled entries for each day by hour.

   Important: The list of entries that appears does not change to match the date that you select in the chart. The list of entries matches your specified filter criteria and does not change until you specify and apply a new filter.
6. In the list of scheduled entries, select the check box for the entries that you want to suspend and click the suspend button on the toolbar. In the **Suspend Activity** dialog box,

   - to suspend entries indefinitely, click **Indefinitely**.
   - to reschedule entries to another date, click **Until**, and select a date and time.

   Note that both the chart and the list of entries refresh, and the suspended entries no longer appear in the list of entries.

   Tip: To suspend an individual entry, click the **Actions** menu arrow for the entry, and click **Suspend**.

Viewing suspended entries for a specific day

You can view a list of suspended entries for a specific day.

Procedure

1. From the **Manage** menu, click **Administration console**.
2. On the **Status** tab, click **Upcoming Activities**.
3. In the **Filter** section, under **Day** select a date, and under **Status** click **Suspended**.
4. Click **Apply**.

   The list shows the suspended entries for that day.

   You can run, cancel, or reschedule suspended entries. To perform an action on an individual entry, click the arrow to the right of the entry and select the action that you want. To perform an action on several entries, select the check box for the entries you want, and then click the appropriate button on the toolbar.

   The following table specifies the actions available for entries and the associated icons:

Table 67. View a list of suspended entries for a specific day actions and icons

Action	Icon
Show Details (top right-hand corner)	
Hide Details (top right-hand corner)	
Cancel the run (**Actions** menu beside entry)	
Suspend entries (**Actions** menu beside entry)	
Run suspended entries (**Actions** menu beside entry)	
Re-schedule a run that was canceled (**Actions** menu beside entry)	
Set Priority (**Actions** menu beside entry)	

Tip: To select all entries in the list, select the check box for the list.

Viewing the run history of entries

You can view the run history of entries that are scheduled to run in the background, without waiting to view them.

This includes scheduled entries that are run once and saved, and interactive entries that are saved or mailed. Interactive entries do not have run histories.

IBM Cognos software keeps history information each time an entry runs in the background. The run history for an entry includes information such as the request time, start time, completion time, and whether the report ran successfully.

You can look at a more detailed run history for the entry, which includes general, error, and warning messages related to the entry and any actions you can take. If there is any email associated with the entry, the status of the email delivery is included.

Some types of entries display additional information in the detailed run history page:

- For reports, a report output version is kept each time a report is run according to a schedule. You can view the report output version from the detailed run history.
- For jobs and agents, you can view a list of steps and see a detailed run history for each one. You can also see the parts of the job or agent that have not yet completed. If the entry is part of a parent entry, you can view the parent entry that initiated the run.
- For human tasks contained within an agent, you can view a list of steps and see a detailed run history for each one.
- For deployment export and import entries, you can view the public content in **IBM Cognos Administration**.

  You may see the following message: *Only progress information is currently available. The information will be updated following the completion of the parent activity*.

  This means that the deployment has completed, but the parent activity is still running. Once the final completion information is obtained from Content Manager, the message no longer appears.

You can rerun failed entries “Rerunning a failed entry task” on page 245 from the detailed run history page. You can view a list of related runs that are part of the rerun series and see a detailed run history for each one. You can specify how many run history occurrences to keep or for how long to keep them “Specifying how long to keep run histories” on page 244.

Procedure

1. From the **Manage** menu, click **Administration console**.
2. On the **Status** tab, click **Schedules** or **Past Activities**.
3. Next to the entry, click the arrow and then click **View run history** .
4. If you want, select the **Status** of entries that you want to view.

   A list of selected entries appears.
5. If you want to view the run history details, in the **Actions** column, click the view run history details button next to the entry you want. Then, if you want, from the **Severity** list, select the severity of the entries.

   Under job steps, the complete run history details is shown. If the job run history details level was set to **Limited**, no history details for the jobs steps are recorded.
6. If there is a report output version, in the **Actions** column, click the view outputs button for the entry you want. Then, from the **Versions** list, click the version you want. To delete a version, click **Manage versions** click the check box for the version, and then click **Delete**.
7. If you want to view messages, click an item with a link in the **Messages** column.

   Messages are nested. You can see child messages within child messages. If a message is displayed as a link, you can continue to drill down through the child messages.

Specifying how long to keep run histories

You can keep run histories for a specific number of runs or for a specific number of days or months.

For example, you can keep the run histories for the ten latest runs (occurrences) or for the past two days or six months. You can also choose to keep all run histories.

Before you begin

You must have read and write permissions for the entry and read or traverse permissions for the folder that contains the entry.

Procedure

1. From the **Manage** menu, click **Administration console**.
2. On the **Status** tab, click **Current Activities**, **Upcoming Activities**, or **Schedules**.
3. Next to the entry, click the arrow, and then click **Set properties**

   The entry properties page appears.
4. On the **General** tab, under **Run history**, choose the retention method and type the value:

   - To keep run histories for a specific number of occurrences, click **Number of occurrences** and type the number. To save an unlimited number of run histories, set this value to 0.
   - To keep run histories for a specific length of time, click **Duration** and click either **Days** or **Months**. Type the appropriate value in the box.
5. Click **OK**.

Rerunning a failed entry task

You can resubmit a failed entry.

When an entry, such as a report, agent task, or job, runs according to a schedule or runs in the background and the fails, you can resubmit the failed entry with the same options that were specified in the original run.

For a job that contains steps that ran successfully and steps that did not run successfully, you are not required to rerun the entire job but only the individual job steps. If the job steps are run sequentially, you can rerun the job starting with the failed job step. If you wish, you can select which steps to rerun and skip the failed steps. However, the selected job steps run sequentially and if a step fails, then the steps that occur after the failed step are not run.

When you rerun a job step individually, a new run history that includes only the single job step is created for the parent job. For more information about run histories, see "Viewing the run history of entries" on page 243.

When rerunning an agent entry, associated tasks, such as an email that sends report output to a list of email recipients, are also rerun if they failed initially. If there are two associated tasks running in parallel and one task fails and one succeeds, rerunning the agent only reruns the failed task. However, if tasks are selected to run on failure, they are run again when the rerun fails.

Although the run history shows entries that ran successfully, you cannot rerun an entry that succeeded. The run options are not stored for these entries.

A rerun can fail when a task associated with a failed entry is deleted or updated.

Before you begin

You must have execute permissions to rerun a failed task.

Procedure

1. From the **Manage** menu, click **Administration console**.
2. On the **Status** tab, click **Past Activities**.
3. Next to the entry, click the arrow and then click **View run history details** .

   The **View run history details** page shows run details, such as start time and completion time, run status, and error messages for a failed run. Other information that appears in the page depends on whether the entry is for a single task, a job with multiple steps, or an agent with tasks. For example, if it is a single task, the report options and the report outputs appear. If it is a job with multiple steps, a **Job** section appears with the run details of the job steps.
4. Under **Status**, next to **Failed**, click **Rerun**.

   - If the rerun task is a single task, you receive a message asking you to confirm the rerun.
   - If the rerun task is a job with multiple job steps or an agent with tasks, the **Rerun** page appears. Select the check box next to the entries you want to rerun.

   Tip: You can also rerun failed entries by clicking **Rerun** in the Outstanding to complete section. To rerun a single job step, in the Job section, in the Actions column, click the view run history details button for the failed step.

Chapter 18. Schedule Management

You can schedule IBM Cognos entries to run at a time that is convenient for you. For example, you may want to run reports or agents during off hours when demands on the system are low. Or you may want to run them at a regular weekly or monthly interval.

To use this functionality, you must have the required permissions for the **Scheduling** secured function in **IBM Cognos Administration**.

To schedule reports to run in the delimited text (CSV), PDF, Microsoft Excel spreadsheet (XLS), or XML output formats, you require the generate output capability for the specific format. For more information, see "Report formats" on page 325. You can update an existing schedule that specifies formats that you are restricted from running, but you cannot introduce to the schedule, formats that you are restricted from running.

In **IBM Cognos Administration**, you can control access to scheduling by day, week, month, year, and trigger using the appropriate scheduling capability. You can also restrict intraday scheduling using the **Schedule by minute** and **Schedule by hour** capabilities Chapter 13, "Capabilities," on page 185.

If you have administrator privileges, you can also schedule tasks that:

- maintain your content store "Content store maintenance tasks" on page 54
- schedule query service caching tasks "Creating and scheduling query service administration tasks" on page 144
- import or export entries from a deployment archive Chapter 19, "Deployment," on page 267
- run jobs "Using jobs to schedule multiple entries" on page 260
- run metrics maintenance Chapter 4, "System Performance Metrics," on page 21

You can schedule entries to run at specified intervals. You can schedule entries individually or use jobs to schedule multiple entries at once. Jobs have their own schedules independent from report schedules.

You can schedule entries to run on the last day of each month. You can also schedule entries to be triggered by occurrences, such as database refreshes or emails.

You can run reports to produce outputs based on the options that you define, such as format, language, and accessibility.

Only one schedule can be associated with each entry. If you require multiple schedules for a report or agent entry, you can create report views or agent views and then create a schedule for each view.

After you create a schedule, the entry or job runs at the time and date specified. You can then view the scheduled entries and manage them. For more information, see Chapter 17, "Managing scheduled activities," on page 225.

Credentials for Scheduled Entries

When you open a scheduled entry, the credentials show the current schedule owner. If you are not already the schedule owner, you can name yourself the owner "Example - Change the Credentials for a Schedule" on page 260.

Credentials for a schedule do not change automatically when you modify a schedule. You must explicitly change the credentials.

For information on data source credentials, see "Trusted credentials" on page 181.

Prompts in Scheduled Entries

If an entry that contains prompts is scheduled, you must save the prompt values or specify default values "Specify the Default Prompt Values for a Report" on page 327 to ensure that values exist when the report runs according to the schedule.

In a job, you can specify prompt values for job steps. When an entry runs as part of a job, the prompt values saved in the job definition are used instead of the values saved with the entry. If no values are specified in the job definition, IBM Cognos software uses the values saved in the entry.

Priority for Scheduled Entries

When you schedule an entry, you may be able to select a run priority from 1 to 5. For example, an entry with priority 1 runs before an entry with priority 5. If there is more than one entry with a specific priority, the one that arrived in the queue first runs first. The default is 3. If you do not have permissions for entry priorities, the priority appears but you can not change it.

When you schedule a job, you can set priority for the whole job only, not for individual entries within a job. However, you can change the priority of individual entries when they are pending in the queue.

The priority of entries in the queue does not affect an entry that is already running. The running entry completes and then the queue priority is checked for the next entry to run.

For more information, see "Changing the entry run priority" on page 236.

Run Histories for Scheduled Entries

IBM Cognos software keeps history information each time a scheduled entry runs. You can use the run history for an entry to see the times at which it ran and whether the it ran successfully. For more information, see "Viewing the run history of entries" on page 243.

Scheduling a report

11.1.7 You schedule a report to run it at a later time or at a recurring date and time.

If you no longer need a schedule, you can delete it. You can also disable it without losing any of the scheduling details. You can then enable the schedule at a later time.

If you want, you can change the current schedule owner by changing the credentials for a scheduled entry. For more information, see "Taking ownership of a schedule" in the *Managing User Guide*.

Before you begin

To use this functionality, you must have the required permissions for the **Scheduling** capability. You can see which capabilities are available with your assigned license role in the topic "Default permissions based on licenses" in the *Managing User Guide*.

To schedule a report, you also require the following access permissions for any data sources used by the report:

- dataSource - Execute and Traverse
- dataSourceConnection - Execute and Traverse

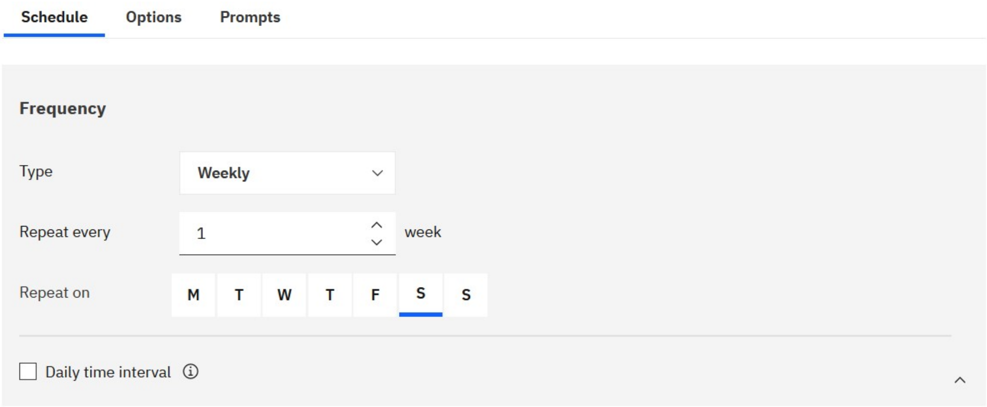
  With only Execute access, you are prompted to log on to the database.
- dataSourceSignon - Execute

To schedule reports to run in the restricted CVS, PDF, XLS, or XML output formats, you require the generate output capability for the specific format. For more information, see *Report formats* in the *Administration and Security Guide*.

To set priority for an entry, you must have the required permissions for the **Scheduling priority** secured feature. For more information, see Capabilities.

Procedure

1. Click the report's More icon ⋯ , and then click **Properties**.
2. In the **Properties** pane, click the **Schedule** tab, and then:
   - Click **Create schedule**.



Frequency

Type: Weekly

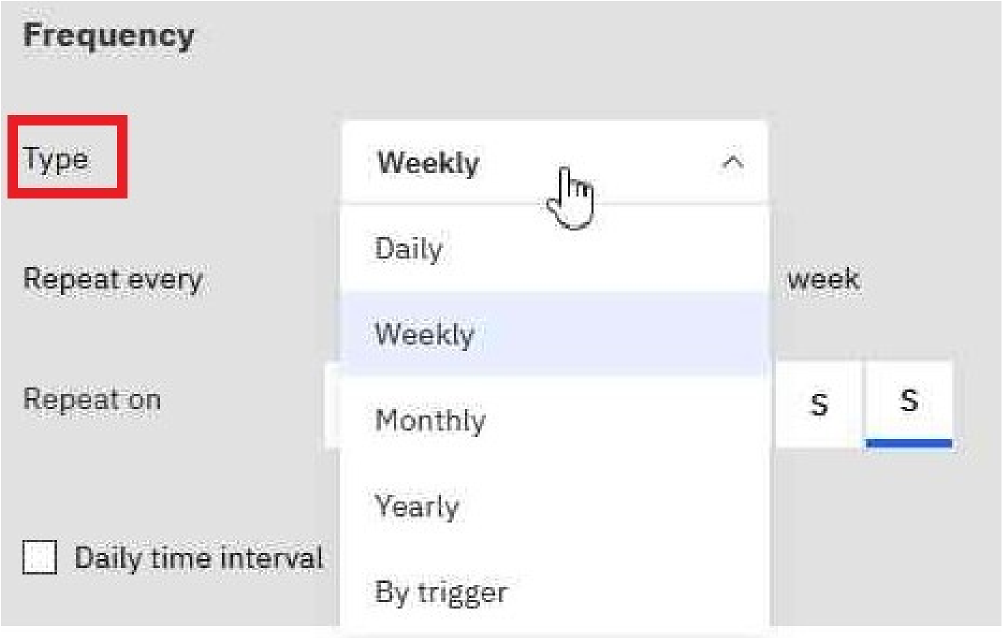
Repeat every: 1 week

Repeat on: M T W T F S S

☐ Daily time interval

Tip: Available options change with each selection. Wait until the pane is updated before you choose additional settings.

3. In the **Frequency** section, specify when and how frequently the report runs:
   - Select the **Type** of time unit to measure the interval between meetings.



Frequency

Type: Weekly

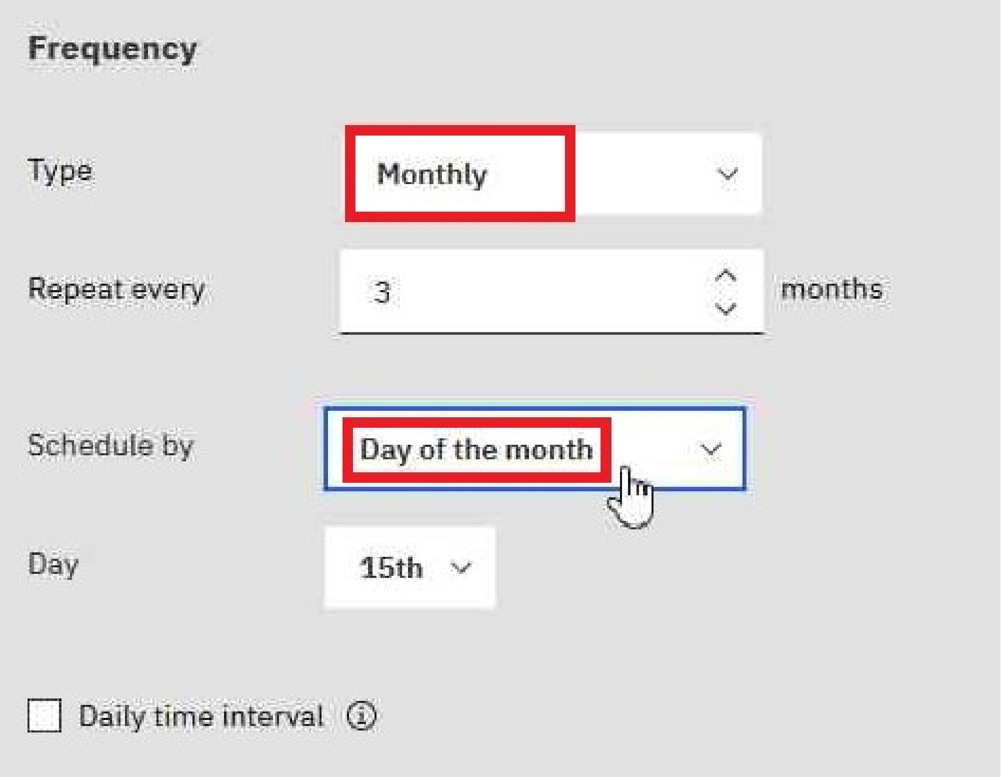
Repeat every: week

Repeat on: S S

☐ Daily time interval

Tip: Try selecting different **Type** values and then watch how the other fields change. For example, selecting **Daily**, **Weekly**, or **Monthly** allows you to select a **Repeat every** *integer*. You can therefore choose an interval which is a multiple of the time unit that you chose, for example, "every 3 weeks".

   - If you are selecting a **Type** value of **Monthly**,

-

Frequency

Type: Monthly

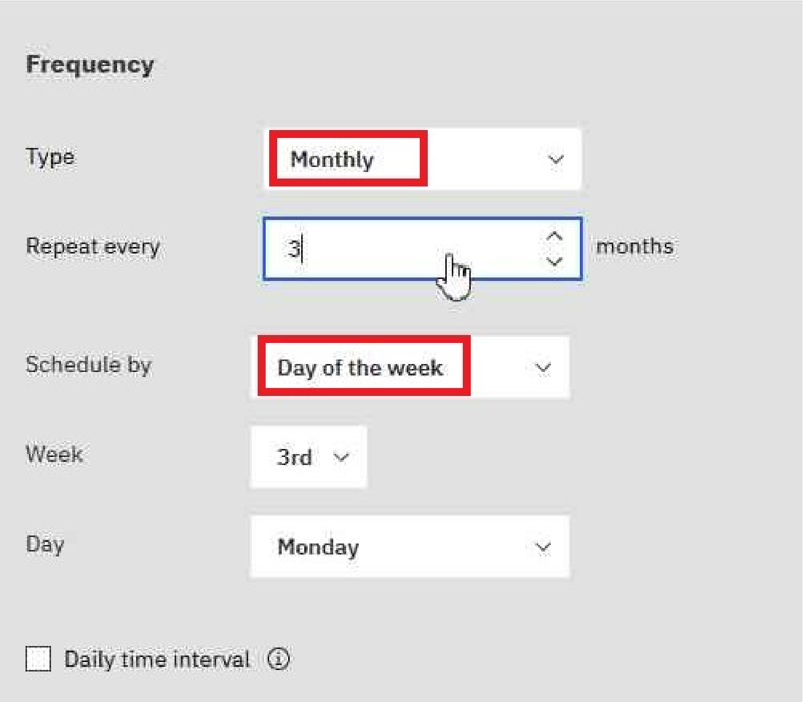
Repeat every: 3 months

Schedule by: Day of the month

Day: 15th

□ Daily time interval

Select **Day of the Month** in the **Schedule by** field so that you can choose, for example, "Repeat every 3 months on the 15th of the month" (see figure above).

-

Frequency

Type: Monthly

Repeat every: 3 months

Schedule by: Day of the week

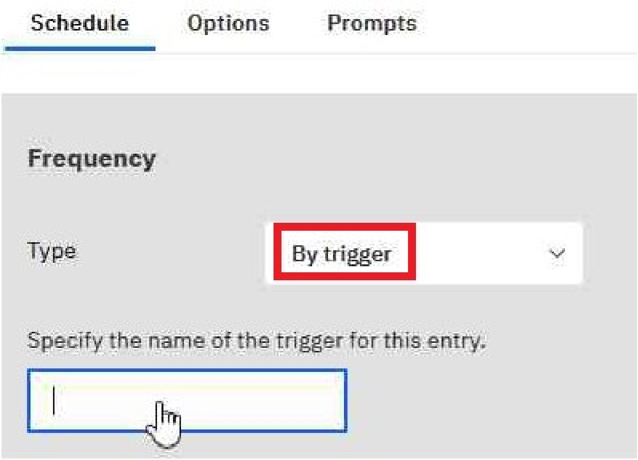
Week: 3rd

Day: Monday

□ Daily time interval

Select **Day of the week** in the **Schedule by** field so that you can choose, for example, "Repeat every 3 months on the 3rd Monday of the month" (see figure above).

- If you are selecting a **Type** value of **By trigger**,



Schedule Options Prompts

Frequency

Type: By trigger

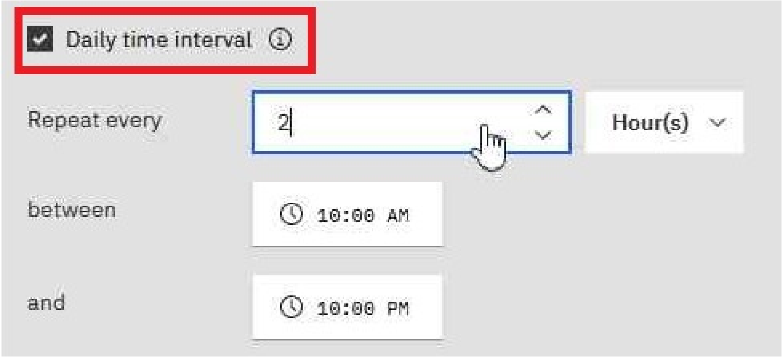
Specify the name of the trigger for this entry.

Tip: If a report is scheduled by a trigger, it can run only if you have already set up a trigger occurrence. For more information, see "Set Up a Trigger Occurrence on a Server" in the *Administration and Security Guide*.

In the field pictured above, enter the name of the trigger occurrence, for example, `trigger.bat`.

4. If you want to select a daily frequency for your scheduled entries:

   - Select the **Daily time interval** check box.



☑ Daily time interval

Repeat every: 2 Hour(s)

between: 10:00 AM

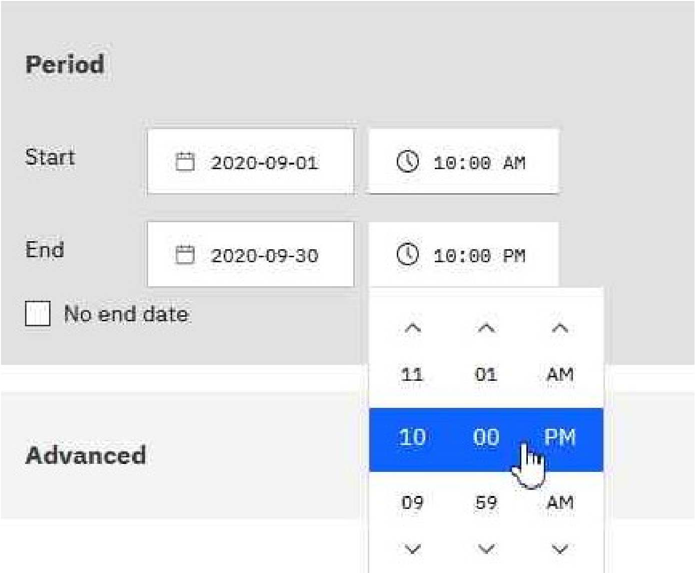
and: 10:00 PM

Tip: Specify the frequency and the period during the day in which the report runs. For example, "every 2 hours between 10:00 AM and 10 PM" (see figure above).

We recommend that you select an hourly frequency that divides evenly into the 24-hour clock. This ensures that your report runs at the same times each day. If you select an hourly frequency that does not divide evenly into the 24-hour clock, your report runs at different times on subsequent days.

5. If you want to set the time period within which the first and last runs of the report will take place:

   - Scroll to the **Period** section.



Period

Start 2020-09-01 10:00 AM

End 2020-09-30 10:00 PM

□ No end date

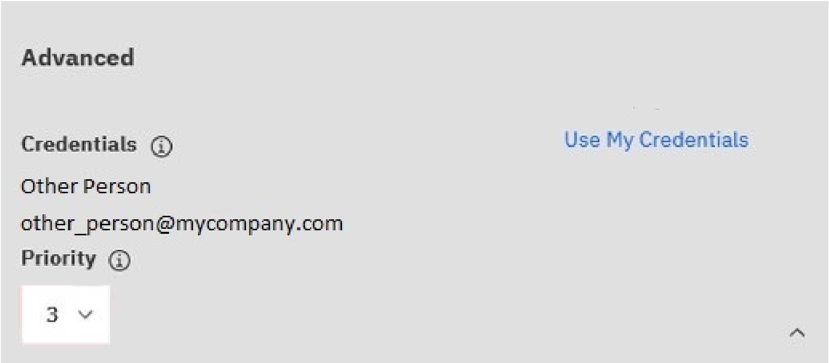
Tip: In the example shown above, the first report run will occur on September 1 at 10:00 AM and the last report run will end on September 30 at 10:00 PM.

Set the date and time for both the start and the end of the period.

If you don't enter anything in the **Period** section, by default the period begins as soon as you save the schedule and there is no end date.

6. If you want to change the credentials or priority of the schedule:

   - Click the **Advanced** section.



Advanced

Credentials ⓘ

Other Person

other_person@mycompany.com

Priority ⓘ

3

Tip:

About the Credentials field

Credentials show the current schedule owner. If you are not already the schedule owner, you can click **Use My Credentials** and make temporary changes to the schedule.

For more information, see " Taking ownership of a schedule" in the *Managing User Guide*.

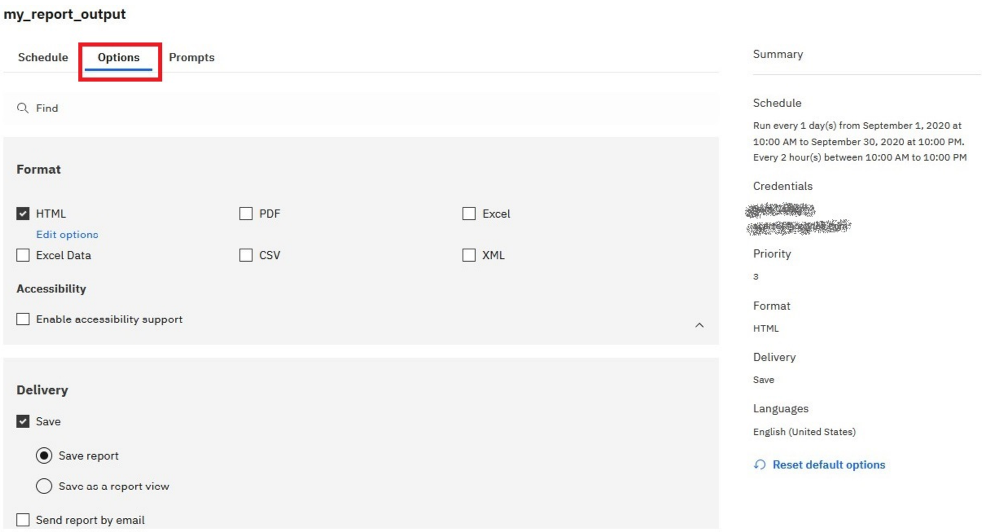
About the Priority field

If you are assigned the Scheduling Priority capability, you can select a priority from 1 to 5 for the scheduled entry to run. Priority 1 runs first.

For more information, see " Changing the entry run priority" in the *Managing User Guide*.

7. To see the default format, delivery method, and language of your report:

   - Click the **Options** tab.



my_report_output

Schedule | Options | Prompts

Find

Format

☑ HTML
Edit options
☐ PDF
☐ Excel
☐ Excel Data
☐ CSV
☐ XML

Accessibility

☐ Enable accessibility support

Delivery

☑ Save

● Save report
○ Save as a report view

☐ Send report by email

Summary

Schedule
Run every 1 day(s) from September 1, 2020 at 10:00 AM to September 30, 2020 at 10:00 PM. Every 2 hour(s) between 10:00 AM to 10:00 PM

Credentials
[redacted]

Priority
3

Format
HTML

Delivery
Save

Languages
English (United States)

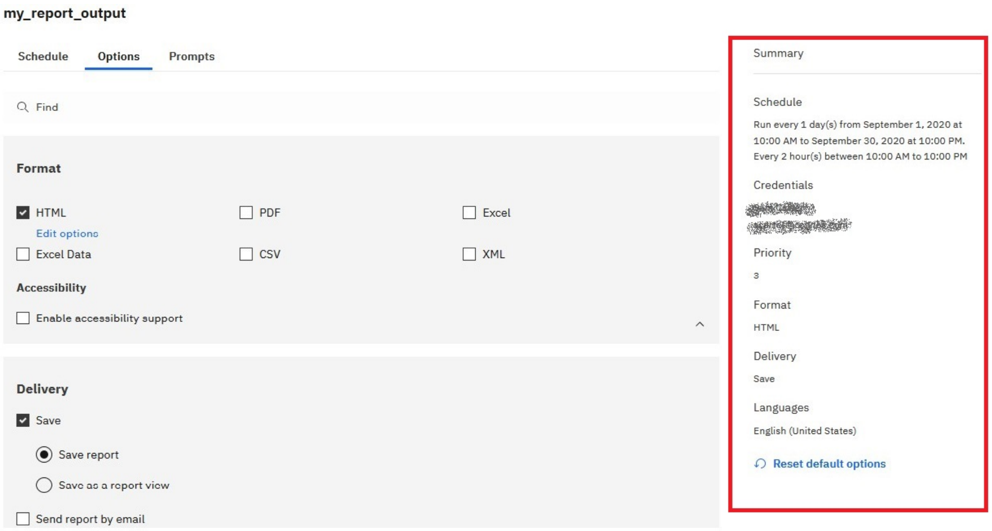
Reset default options

Tip:

The default options are displayed:

- **Format**: HTML only, accessibility support disabled
- **Delivery**: Save report only
- **Languages**: English only

- Did you notice the **Summary** pane?



my_report_output

Schedule | Options | Prompts

Find

Format

☑ HTML
Edit options
☐ PDF
☐ Excel
☐ Excel Data
☐ CSV
☐ XML

Accessibility

☐ Enable accessibility support

Delivery

☑ Save

● Save report
○ Save as a report view

☐ Send report by email

Summary

Schedule
Run every 1 day(s) from September 1, 2020 at 10:00 AM to September 30, 2020 at 10:00 PM. Every 2 hour(s) between 10:00 AM to 10:00 PM

Credentials
[redacted]

Priority
3

Format
HTML

Delivery
Save

Languages
English (United States)

Reset default options

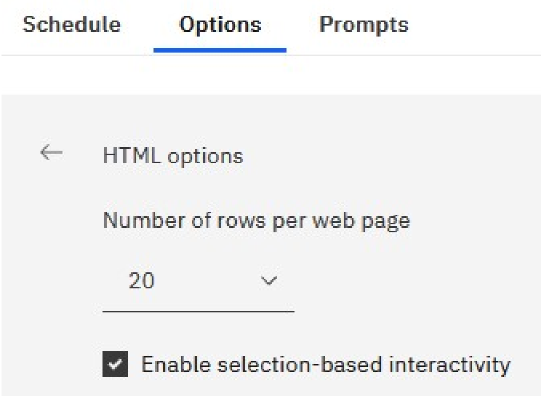
Tip:

As you build your schedule, the **Summary** pane on the right of your window uses natural language to describe all of your selections in real time.

At any time, you can click **Reset default options** to clear the options that you set on every tab.

8. If you want, change the **Format** options:

- If you select HTML format, you can click **Edit options**.



Schedule Options Prompts

HTML options

Number of rows per web page

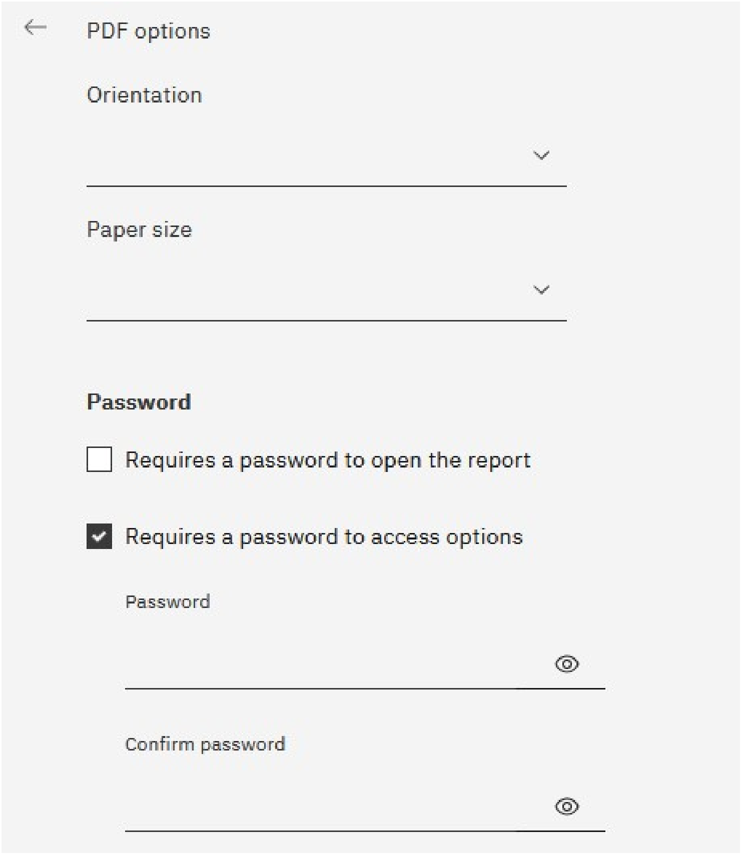
20

☑ Enable selection-based interactivity

Tip:

If you want to drill up and down in a report or drill through to other reports, you must select the **Enable selection-based interactivity** check box. However, if your report is very large, you may want to deselect the check box to shorten the time that it takes the report to run.

- If you select PDF format, you can click **Edit options**.



PDF options

Orientation

Paper size

Password

☐ Requires a password to open the report

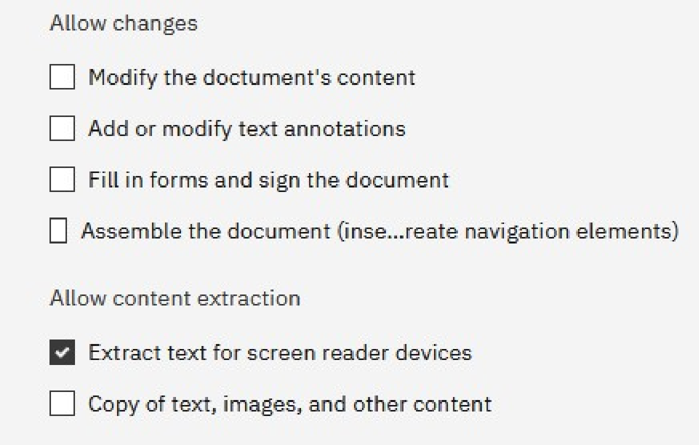
☑ Requires a password to access options

Password

Confirm password

Figure 9. PDF options - part 1

Tip: You can create a password to add extra security to your report. This is in addition to the permissions that users are granted by their capabilities.



Allow changes

☐ Modify the doctument's content

☐ Add or modify text annotations

☐ Fill in forms and sign the document

☐ Assemble the document (inse...reate navigation elements)

Allow content extraction

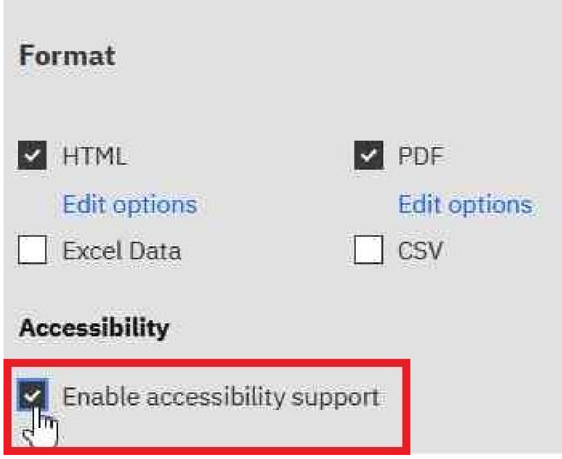
☑ Extract text for screen reader devices

☐ Copy of text, images, and other content

Figure 10. PDF options - part 2

Tip: You can limit the types of changes that other users can make to the report.

- If you select the **Enable accessibility support** check box.



Format

☑ HTML
Edit options

☑ PDF
Edit options

☐ Excel Data

☐ CSV

Accessibility

☑ Enable accessibility support

Figure 11. PDF options - part 1

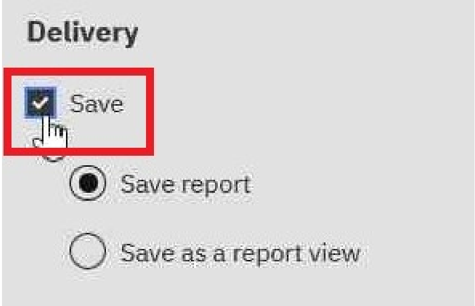
Tip: You can make your report output accessible. Accessible reports contain features, such as alternate text, that allow users with disabilities to access report content using assistive technologies, such as screen readers.

In IBM® Cognos® applications, you can create accessible output for reports, jobs, steps within jobs, and scheduled entries in PDF and HTML.

Accessible reports require more report processing and have a greater file size than non-accessible reports. Consequently, making reports accessible can have a negative impact on performance.

9. You can change the **Delivery** options:

- If you want to save the report in Cognos Analytics, you have two options.



Delivery

☑ Save

● Save report

○ Save as a report view

Figure 12. PDF options - part 1

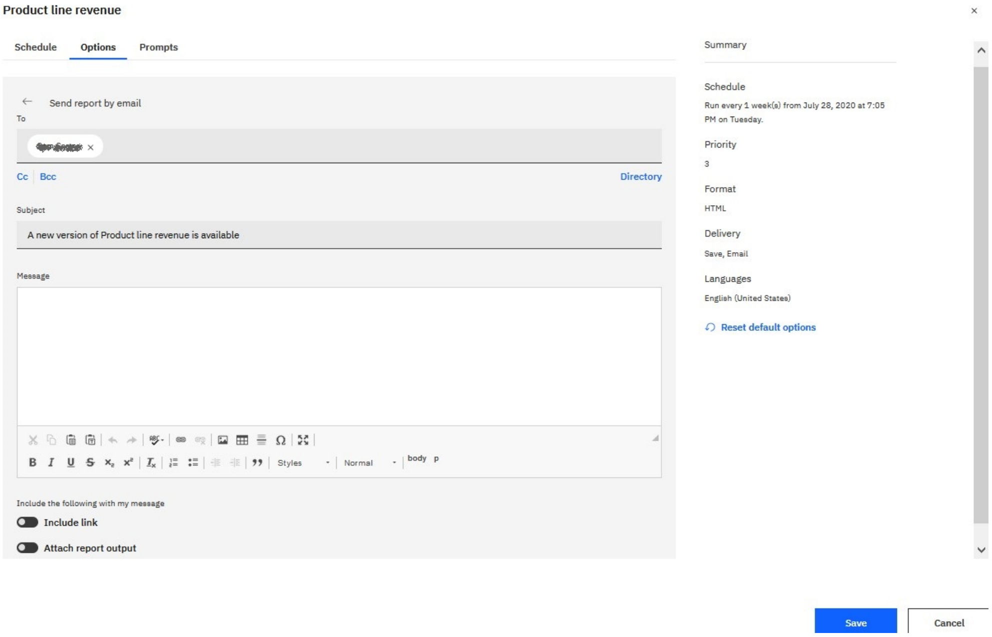
Tip:

– **Save report**. This option is selected by default.

– **Save as a report view**. Unlike saving the report, you can change the name or destination folder of the report view. A report view uses the same report specification as the source report, but has different properties such as prompt values, schedules, delivery methods, run options, languages, and output formats.

  Creating a report view does not change the original report. You can determine the source report for a report view by viewing its properties. The report view properties also provide a link to the properties of the source report.

- If you select **Send report by email** and then click **Edit details**.



Product line revenue

Schedule | Options | Prompts

← Send report by email

To

[redacted] ×

Cc | Bcc | Directory

Subject

A new version of Product line revenue is available

Message

Styles | Normal | body p

Include the following with my message

Include link

Attach report output

Summary

Schedule

Run every 1 week(s) from July 28, 2020 at 7:05 PM on Tuesday.

Priority

3

Format

HTML

Delivery

Save, Email

Languages

English (United States)

Reset default options

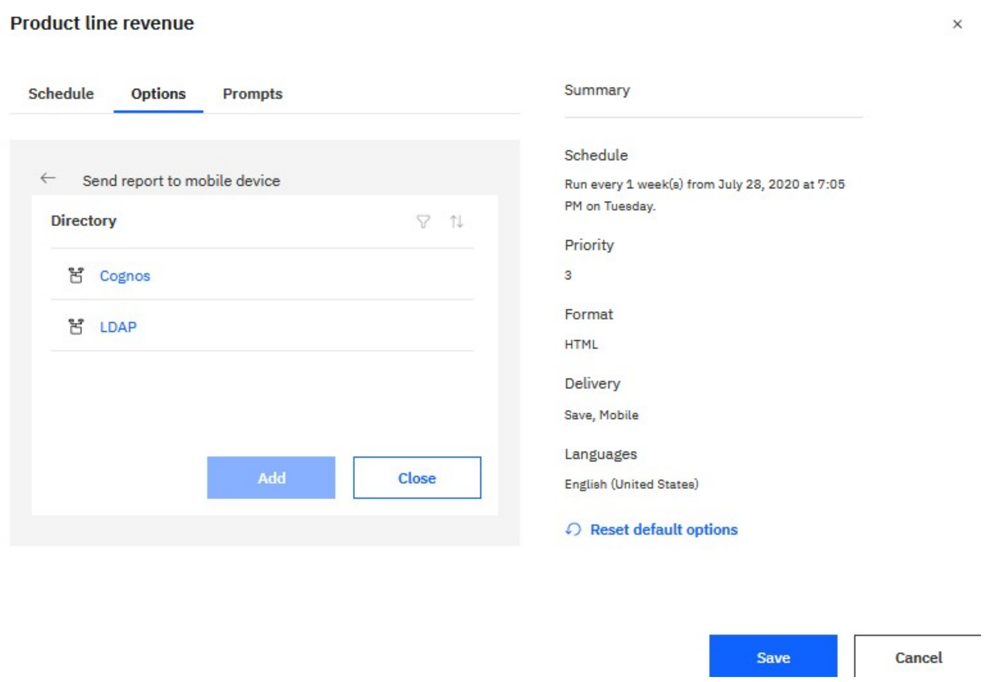
Save | Cancel

Tip:

An email window appears, in which you can enter recipients' names, if you have permission. Otherwise, you can choose your email recipients from your local LDAP directory. If your directory is very large, you can use search, filter and sort functions to quickly find your recipients.

After you enter your message, and you have the correct permissions, you can attach the report output to the email. Or you can add a link that your recipient can click to see the report.

- If you select **Send report to mobile device**.



Product line revenue

Summary

Schedule
Run every 1 week(s) from July 28, 2020 at 7:05 PM on Tuesday.

Priority
3

Format
HTML

Delivery
Save, Mobile

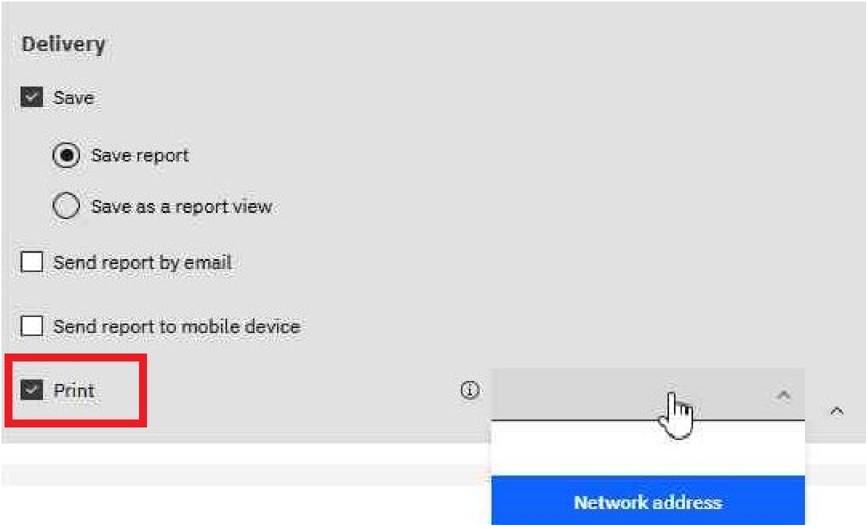
Languages
English (United States)

Tip:

This option is available only to users of Cognos Analytics on Demand or Cognos Analytics on Cloud Hosted.

Similar to the email option, you can find your recipient in the Directory. When the report is run, it will be sent to the mobile device of the recipient via Cognos Analytics for Mobile.

- If you select **Print**.



Delivery

☑ Save

● Save report

○ Save as a report view

□ Send report by email

□ Send report to mobile device

☑ Print

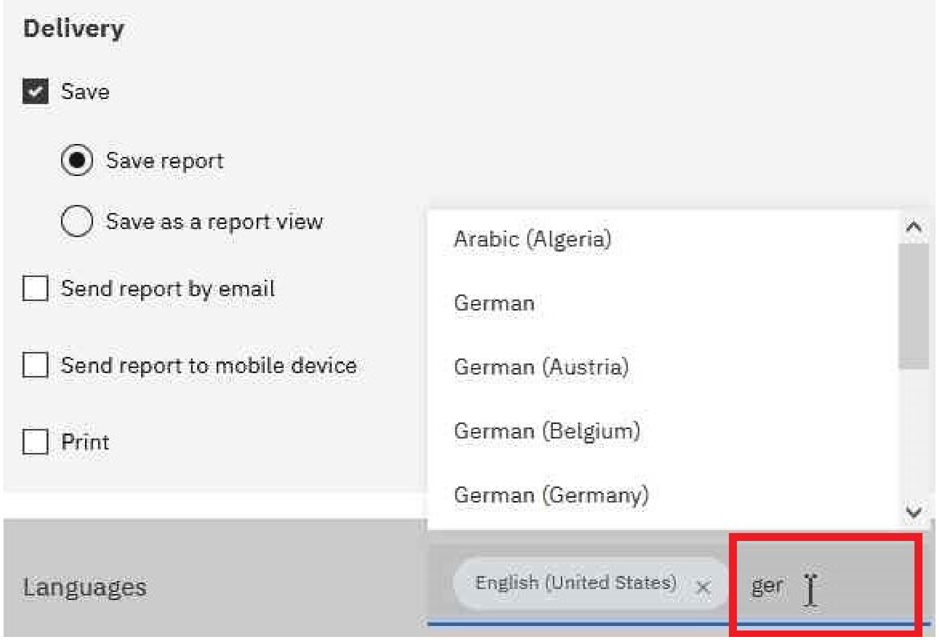
Tip: It may be convenient for you to have a printed copy of a report.

You may need to review a report when your computer is not available, or you may need to take a copy of a report to a meeting.

To print reports, you must have the Generate PDF Output capability.

Select a printer from the list or enter a valid printer name, location, or address and then click **Add**.

- If you want your output in languages other than English (the default).



Delivery

☑ Save

● Save report

○ Save as a report view

□ Send report by email

□ Send report to mobile device

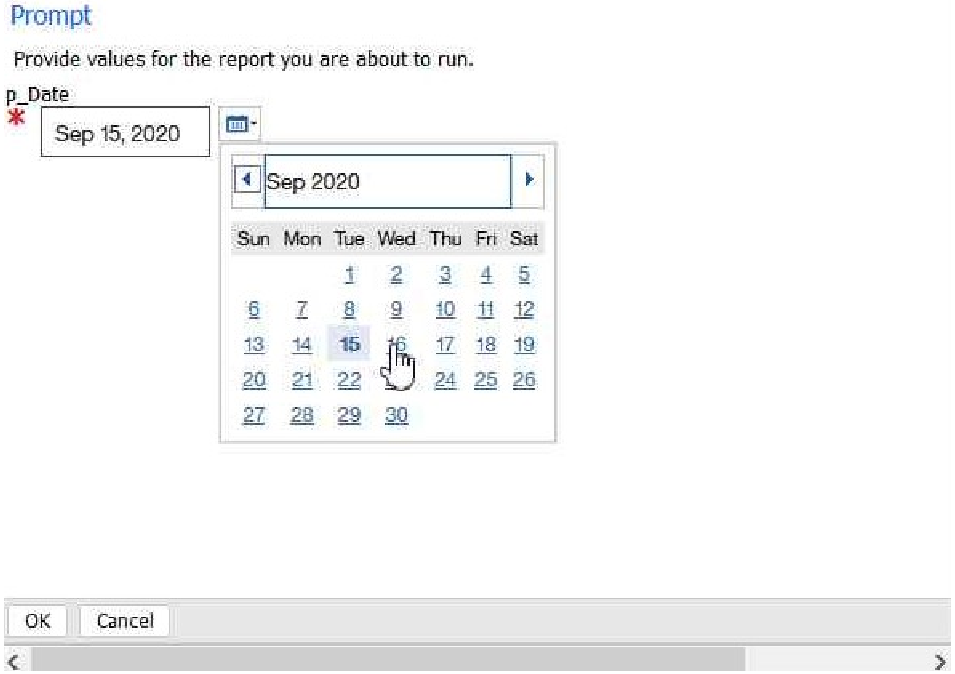
□ Print

Languages: English (United States) × ger

Tip: Start typing the name of the language in the **Languages** field. A dynamic list of languages appears, from which you can select the one you want.

10. If your report has prompts:

    - Click the **Prompts** tab and then click **Set values**.



Prompt

Provide values for the report you are about to run.

p_Date

* Sep 15, 2020

Tip: In the example **Prompt** window shown above, the **p_Date** parameter prompts for a date value.

11. Click **Save**.

Results

A schedule is created and the report runs at the next scheduled time.

Managing scheduled activities

You can view a list of scheduled entries for all users.

Each entry is listed by name, status, and priority. A bar chart shows you an overview of activities broken down by enabled and disabled schedules.

The date and time the schedule was modified and the user who scheduled it are also listed.

You can filter the entries to display only those you want. You can choose to display only the entries with a specific status or priority, or entries of a specific type or scope. You can also filter by the user that scheduled the entry and by the entry owner.

You can set properties, run the schedule once, disable and enable scheduled entries, modify the schedule, remove the schedule, set the priority “Changing the entry run priority” on page 236, and view the run history “Viewing the run history of entries” on page 243. Depending on the entry, you may also be able to perform other functions, such as view outputs or event lists.

For more information on schedules, see Chapter 18, “Schedule Management,” on page 247.

Procedure

1. From the **Manage** menu, click **Activities**.
2. Click the type icon ⌄, and then click **Schedule**.
3. In the **Filter** section, click the filtering options that you want to use.

   Tip: If you want to use advanced filtering options, click **Advanced options**. To reset all selections to the default settings, click **Reset to default**.
4. Click **Apply**.

   The list shows the entries that you selected.
5. To perform an action on an individual entry, click **More** (...) next to the entry and select the action.

   The following table specifies the actions available for entries and the associated icons:

   Table 68. Scheduled activities actions and icons

Action	Icon
Properties	☰
Modify this schedule	📅
View versions	📊
Disable this schedule	⊘
Remove this schedule	⊖
Set priority	≡◂
Use my credentials	👤

   Tip: To select all entries in the list, select the check box for the list.

Example - Change the Credentials for a Schedule

You want to change the credentials for a schedule to identify you as the current schedule owner.

Procedure

1. From the **Manage** menu, click **Activities**.
2. Click the type button , and then click **Schedule**.
3. Click **More** (...) next to the entry and then click **Use my credentials** .
4. Save your changes.

Results

The next time that you open the schedule, your credentials identify you as the owner.

Tip: If you are logged on as an anonymous user, information about the current schedule owner is not available.

Using jobs to schedule multiple entries

You can set the same schedule for multiple entries by creating a job. A job identifies a collection of reports, report views, and other jobs that are scheduled together and share the same schedule settings. When a scheduled job runs, all the entries in the job run.

If a job item is unavailable, you can select a different link by clicking **Link to an entry**.

Jobs contain steps, which are references to individual reports, jobs, and report views. You can specify whether to run the steps all at once or in sequence.

- When steps are run all at once, all the steps are submitted at the same time. The job is successful when all the steps run successfully. If a step fails, the other steps in the job are unaffected and still run, but the job has a **Failed** status.
- When the steps are run in sequence, you can specify the order in which the steps run. A step is submitted only after the preceding step runs successfully. You can choose to have the job stop or have the other steps continue if a step fails.

You can schedule a job to run at a specific time, on a recurring basis, or based on a trigger, such as a database refresh or an email. For more information, see "Trigger-based Entry Scheduling" on page 262.

The individual reports, jobs, and report views in steps can also have individual schedules. Run options for individual step entries override run options set for the job. You can set run options for the job that serve as the default for step entries that do not have their own run options.

You can run reports to produce outputs based on the options that you define, such as format, language, and accessibility.

You can also include content store maintenance and deployment imports and exports in a job. For more information, see "Content store maintenance tasks" on page 54 and Chapter 19, "Deployment," on page 267.

Permissions required to include an entry as part of a job vary depending on the type of entry. The permissions are the same as for scheduling an entry. For more information, see "Scheduling a report" on page 225.

Procedure

1. In the IBM Cognos Analytics portal, click **New** +, and then click **Job**.

   The **Steps** page appears.

2. Click the **Add job step** icon ⊕.
3. Navigate to a report that you want to include in your job step, select it, and then click **Add job steps**.
4. If you want to change the default run options for the step, click the Edit options icon ✎, and then edit the format, delivery, prompts, languages, or accessibility options.
5. Repeat steps “2” on page 261 -“4” on page 261 to include additional steps in your job.
6. To remove a step, hover over the step and then click the Remove job step icon ⊖.
7. If you want to revert to the default run options for any future steps that you add, select **Change default step options**.
8. Under **Run order**, select whether the steps should **Run all at once** or **Run in sequence**.

   If you select **Run in sequence**, the steps are executed in the order they appear in the **Steps** list. If you want the job to continue to run even if one of the steps fails, select the **Continue on error** check box.

   Tip: To change the order of steps, click a step and drag it to the position that you want.
9. In the application bar, click the Save icon 💾.
10. Navigate to a folder in which to save your job, enter a job name in the **Save as** box, and then click **Save**.

    Run now and **Schedule** links appear in the **Run Options** section.
11. To run the report immediately, click **Run now** and click **Finish**. .
12. To schedule at a recurring time, follow these steps:

    a) Click **Schedule**.

    b) Click **New**.

    c) Enter the details of when you want the job to run.

    d) Click **Create**.

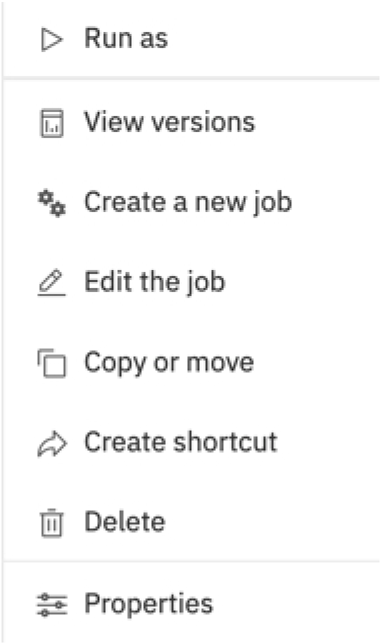
    Tip: If this message appears: "Your credentials are required to complete this operation", click **Renew** and then enter your Cognos Analytics userid and password.

Results

A job, denoted by the job icon ⚙, is created in the folder you selected and will run at the next scheduled time.

What to do next

You can select operations from the following menu after you click the More icon ••• for the job you created:



Cached Prompt Data

For reports that prompt for values each time that the report is run, you may want to use cached prompt data. Reports run faster because data is retrieved from the cache rather than from the database.

The cache is used only when a requested language is the same as one in the cache. For example, the cache contains data for English, English (United States), and German (Germany). When prompted, you request English (United States) for the report. There is an exact match and the cached data is used. The cached data is also used when there is a partial match. If you request English (Canada), the cached data for English is used. If you request German (Austria), there is no match and the cached data is not used.

You can use caches for reports or report views. For report views, the report view cache is used first. If no report view cache is found, the cache for the associated report is used.

You must use a job to create or refresh a cache. You can refresh the cache automatically by scheduling the job to run periodically. If you want to use live data the next time that you run the report, you can clear the cache.

Trigger-based Entry Scheduling

You can schedule entries based on an occurrence, such as a database refresh or an email. The occurrence acts as a trigger, causing the entry to run. For example, you may want to run a report every time a database is refreshed.

Trigger-based scheduling may be used to run entries automatically based on an occurrence. It may also be used to limit when users can run entries. For example, in a warehouse environment where the database is refreshed only once a week, there is no need to run reports more frequently.

You can choose to schedule the report based on the database refresh so that the report runs only once a week.

Trigger-based scheduling applies only to the entry, not to any entry view associated with it. For example, if trigger-based scheduling applies to a report, it does not apply to report views associated with the report. However, you can schedule a report view using a trigger.

In **IBM Cognos Administration**, you can control access to scheduling by trigger using the **Schedule by trigger** capability.

Setting Up Trigger-based Scheduling

To schedule an entry based on an occurrence and confirm trigger-based scheduling, you must have read, write, execute, and traverse permissions.

To schedule reports to run in the delimited text (CSV), PDF, Microsoft Excel spreadsheet (XLS), or XML output formats, you require the generate output capability for the specific format. For more information, see "Report formats" on page 325.

You also require the following access permissions for all data sources used by the entry.

Table 69. Data sources and permissions required for trigger-based scheduling

Data source	Permissions
dataSource	Execute and Traverse
dataSourceConnection	Execute and Traverse With only Execute access, you are prompted to log on to the database.
dataSourceSignon	Execute

Before setting up trigger-based scheduling, ensure that your credentials exist and are up to date.

Tip: Click the my area options button, **My Preferences**, and, on the **Personal** tab, click **Renew the credentials**.

Follow this process to set up trigger-based scheduling:

- "Schedule an Entry Based on an Occurrence" on page 264.
- Set up the trigger occurrence on a server.

Trigger occurrences can also be set up by a Software Development Kit developer using the IBM Cognos Software Development Kit. For more information, see the *Software Development Kit Developer Guide*.

Set Up a Trigger Occurrence on a Server

As part of setting up trigger-based report scheduling, you must set up the trigger occurrence on a server.

You link the external occurrence, such as a database refresh or an e-mail, with a trigger on the server that causes the entry to run. You must also specify the name of the occurrence.

Trigger occurrences can also be set up by a Software Development Kit developer using the IBM Cognos software development kit. For more information, see the *The IBM Cognos Software Development Kit Developer Guide*.

Using the Microsoft Windows script named trigger.bat or the shell script named trigger.sh, you can trigger one or more schedules to run on the server. The script syntax follows where URL is the IBM Cognos server URL, `username` is a valid username in the specified namespace, `password` is the password for the username, `namespace` is the namespace for the username, and `triggerlist` is a comma separated list of trigger names:

```
trigger.bat URL [username password namespace]
triggerlist
```

For example, if users want to schedule a report based on a database refresh and want to schedule a second report based on receipt of an email, your custom trigger command line may look similar to this:

```
trigger.bat http://localhost:9300/p2pd/servlet/dispatch username
password namespace databaserefreshtriggername,emailtriggername
```

Procedure

1. If you are setting up a trigger occurrence on a server other than an IBM Cognos server, complete the following tasks:

   - Ensure that the server has a supported version of either a Java Runtime Environment or a Java Development Kit.
   - Copy the following files from *cognos_analytics_installation_location*/webapps/p2pd/WEB-INF/lib on an IBM Cognos server to the location on the server where you are setting up the trigger occurrence:

     activation.jar

     axis.jar

     axisCrnpClient.jar

     commons-discovery-0.2.jar

     commons-logging-1.1.jar

     commons-logging-adapters-1.1.jar

     commons-logging-api-1.1.jar

     jaxrpc.jar

     saaj.jar

     wsdl4j-1.5.1.jar
   - Copy `mail.jar` from *cognos_analytics_installation_location*/bin64 on an IBM Cognos server to the location on the server where you are setting up the trigger occurrence
   - Copy the following files from *cognos_analytics_installation_location*/webapps/utilities/trigger on an IBM Cognos server, to the location on the server where you are setting up the trigger occurrence:

     trigger.bat

     trigger.sh

     trigger.class (a Java utility that can run on any IBM Cognos-supported platform)
2. Ensure that the command line runs when the external occurrence, such as a database refresh or email, occurs.

   The mechanism that you use to invoke your custom trigger command depends on the application that you are working with, such as a database system or an email application. For information, see the documentation for your application.
3. Inform users that they can now schedule entries based on the trigger occurrence.

   If a user scheduled an entry based on the occurrence, when the user clicks the schedule button for a report view, occurrence information replaces frequency information on the **Schedule** page.

Results

After the script runs, the trigger method returns an integer value representing the number of schedules that were run. The following integers represent errors:

- -1 is a usage error, such as invalid parameter or syntax
- -2 is a communication problem with IBM Cognos server

Schedule an Entry Based on an Occurrence

As part of setting up trigger-based scheduling, you must schedule an entry based on an occurrence.

Trigger-based schedule is activated if the user firing the trigger has:

- read and traverse permissions for the schedule entry
- traverse permissions for all ancestors of the schedule entry

- access to IBM Cognos Administration

To schedule reports to run in the delimited text (CSV), PDF, Microsoft Excel spreadsheet (XLS), or XML output formats, you require the generate output capability for the specific format. For more information, see “Report formats” on page 325.

Before you begin

If it is scheduled by a trigger, a report can run only if you have already set up a trigger occurrence. For more information, see “Set Up a Trigger Occurrence on a Server” on page 263.

Procedure

1. Click the More button ⋯ for the entry that you want to schedule.
2. Click **Properties**.
3. Click the **Schedule** tab.
4. Click ⊕ **New**.
5. In the **Create schedule** panel, click the black triangle in the **Schedule** field, and then click **By trigger**.
6. In the **Trigger name** field, type the name of the trigger occurrence.

   Note: The trigger name that you enter may be provided to you by your administrator or developer. If not, you must inform your administrator or developer of the trigger name that you use.
7. Set the start and end time of the **Period** during which a trigger will cause the schedule to be run.

   Tip: The trigger schedule will run when the trigger is fired (either from trigger.bat or from an Software Development Kit application) anytime between the start and end date.
8. Click **Create**.

Chapter 19. Deployment

Deployment involves moving applications from one installation to another. You can deploy IBM Cognos content from a source environment to a target environment.

You can deploy the entire content store or only specific content, such as packages, folders, namespaces, user accounts, or visualizations.

Typically, deployment transfers entries from a development environment to a test environment and then to a production environment. You can also deploy between operating systems.

It is important to plan your deployment to ensure that you deploy the correct information and that you do not disturb the target environment. It is also important to consider security in the source and target environments.

You can upgrade entries from previous releases by running the deployment import wizard. For more information, "Importing to a Target Environment" on page 283.

You can use an operating system or scripting mechanism to perform deployment from a command line. You can use the IBM Cognos software development kit to automate the deployment process to

- create, update, and delete a deployment specification
- load a deployment specification from a deployment archive
- submit deployment export and import requests
- access deployment history

For more information, see the IBM Cognos Software Development Kit *Developer Guide*.

For information about content deployment in a multitenant IBM Cognos Analytics environment, see "Tenant content deployment" on page 313.

Deployment of human task service is a separate task. For more information, see "Deploy Human Task and Annotation Services" on page 288.

Deployment Specifications

A deployment specification is an entry in the content store that defines the entries to be deployed, the deployment preferences, and the name of the deployment archive.

There are two types of deployment specifications. Export specifications are created in the source environment and control the creation of deployment archives. Import specifications are created in the target environment and control the import of entries from the deployment archive.

You can view the deployment history for each deployment specification to see the date, time, and details of the import or export.

Deployment Archives

A deployment archive is a compressed file that contains actual entries that is created when you export from the source environment.

You move the deployment archive from the source environment to the target environment. Then you import from the deployment archive into the target environment.

To move a deployment archive, you need access to the installation directories on the computer where IBM Cognos software is installed. This location is set in the configuration tool. The default location is *install_location*/deployment. For information about changing the location, see the IBM Cognos *Installation and Configuration Guide*.

If you export to an existing deployment archive, the contents of the archive are overwritten.

Deployment Planning

When you deploy, you must consider how to handle security and which deployment method to select.

To avoid breaking references in the target environment, you must deploy all entries that refer to entries in another package or folder. Entries to consider include:

- jobs and report views
- memberships and entry permissions

Security and Deployment

Before you deploy, you must consider access permissions, security of deployment archives , and references to namespaces other than **Cognos**.

Access Permissions

The entries that you deploy may have security applied to them, such as access permissions Chapter 12, “Access Permissions and Credentials,” on page 173 that specify which users and groups can access them. If you deploy the entire content store “Deploying the Entire Content Store” on page 269, all access permissions are deployed. If you deploy selected packages, public folders and directory content, you can choose whether to deploy access permissions “Deploying Selected Public Folders and Directory Content ” on page 271.

Consider the following:

- Referenced users and groups

  If you deploy access permissions to a target environment, the referenced users and groups must exist in the target environment.

- Access permissions rules

  For access permissions to work after entries are deployed, the source environment and the target environment must use the same authentication provider with the same configuration. Otherwise, the permissions may not work after deployment.

  Use the Cognos namespace to ensure that the permissions from the source environment work in the target environment. For example, in the source environment, create Cognos groups with the group Everyone as a member, and then set access permissions for the groups. After deployment, in the target environment, map the Cognos groups to the appropriate users and groups from the authentication provider, and then remove Everyone from the membership of the group.

For information about deploying Cognos groups and roles, see “Including Cognos Groups and Roles” on page 273.

Securing Deployment Archives

A deployment archive “Deployment Archives” on page 267 can contain sensitive information, such as signons and confidential account or credit card numbers in report outputs. When you export, you can encrypt the deployment archive by setting a password. Later, when you import, you must type the encryption password. The password must contain eight or more characters.

You must encrypt the deployment archive when it contains data source signons or when you deploy the entire content store “Deploying the Entire Content Store” on page 269.

The encryption settings are configured in the configuration tool. For more information, see the IBM Cognos *Installation and Configuration Guide*.

Including References to Other Namespaces

Some entries, such as groups, roles, distribution lists, contacts, data source signons, and some report properties, such as email recipients and report contacts, can refer to entities in namespaces other than the **Cognos** namespace. When you deploy public folders and directory content, you can deploy these entries with or without references to these namespaces.

Consider the following:

- Included references

  If you include the references to other namespaces, the system verifies that each of the referenced entities exists in the applicable namespaces. Therefore, you must ensure that you are logged on to each namespace, and that you have the necessary permissions to access the required entities in the namespaces. If you cannot access the namespaces, you will encounter errors during the deployment.

- No included references

  If you do not include the references to other namespaces, the referenced entities are removed from the membership list. The membership list includes groups, roles, distribution lists, and data source signons and other properties, where they may exist.

When you deploy the entire content store "Deploying the Entire Content Store" on page 269, the references to all namespaces are included.

Maintaining localized object names when importing older archives

New releases of IBM Cognos software introduce support for new locales. Importing older archives into newer versions of can result in missing translations for object names in some locales. To avoid this problem, set the advanced property CM.UpdateInitialContentNamesAfterImport before the import.

About this task

For example, support for Catalan, Croatian, Danish, Greek, Kazakh, Norwegian, Slovak, Slovenian, and Thai locales was added in IBM Cognos Business Intelligence versions 10.1.1 and 10.2. Archives created with earlier versions do not support these locales. When planning to import these types of archives, set the **`CM.UpdateInitialContentNamesAfterImport`** property before the import is started. This will ensure that object names, such as **Public Folders** or **My Folders**, in these additional locales are translated and display properly.

If you notice that object names do not display in the specified language after you import an older archive, see the *IBM Cognos Analytics Troubleshooting Guide*.

Procedure

1. Follow the steps in the section"Configuring advanced settings for specific services" on page 464.
2. For the **ContentManagerService**, type the parameter name **`CM.UpdateInitialContentNamesAfterImport`**.
3. In the **Value** column, type the affected locales and separate each with a comma.

   For example, for Slovenian and Croatian content locales, type the following text string:

   ```
   sl,hr
   ```

Results

Remove this advanced setting when support for the older archive is no longer needed because there is a performance impact associated with having this setting enabled.

Deploying the Entire Content Store

Deploying the entire content store ensures that all packages, folders, and directory content are copied to a new location.

For example, if you are changing the computer where IBM Cognos software is installed, you can move the entire content store from the old environment to the new environment and keep all the reports and other entries created by administrators and users.

Other reasons to deploy the entire content store include:

- moving a whole application into a new, empty environment, such as a new computer, from a development environment
- refreshing a whole application into an existing environment, such as an existing computer, from a development environment
- moving an application from an existing environment that uses a different underlying technology, such as a different database type for the content store, or a different operating system
- upgrading the contents of the content store

When you move a content store from one environment to another, you must use the same namespaces for policies, users, roles, and groups to work correctly.

When you deploy the entire content store, if there are no conflicts, the contents of the target content store are removed and replaced by the contents of the source content store, except for configuration data. The imported entries keep the owners from the source content store. For information about conflict resolution, see "Conflict Resolution Rules" on page 276.

After the deployment is complete, some links for packages associated with reports may not work. You may need to relink packages to reports. For information about linking packages to reports, see the documentation for the studios.

Tip: Instead of deploying the entire content store, you can deploy only specific public folders and directory content "Deploying Selected Public Folders and Directory Content " on page 271.

Content Store

The content store includes all entries in the portal, such as:

- public folders
- packages
- reports
- data sources
- distribution lists and contacts
- printers
- the Cognos namespace
- deployment specifications

It does not include the deployment history "Deployment History" on page 270. Configuration objects "Configuration Information" on page 271 such as dispatchers, are included in exports by default, but excluded in imports.

If you want to deploy users' personal folders and personal pages, you must choose to include the user account information when you export and import.

Deployment History

When you export an entire content store, the export and import deployment specifications that exist in the source content store are exported. Their deployment histories are not exported.

Later, when you import the entire content store, you also import the export and import deployment specifications. You do not see entries in the **View the deployment history** page for the imported specifications.

If any of the imported deployment specifications are used for an encrypted deployment archive, you can delete them. To import an entire content store the first time, you must create a new import deployment specification.

By default, the information saved in deployment records includes the progress and summary reports only. If you want to include more detailed information, change the recording level using the advanced setting

CM.DEPLOYMENTDETAILENTIRECONTENT. Use the steps in "Setting advanced Content Manager parameters" on page 50. More recording levels are available in partial deployment "Recording Deployment Details" on page 274.

Configuration Information

When you import an entire content store, configuration data is included in the export, but excluded from the import by default. We recommend that you do not change this setting. However, if you must import configuration settings, you can change the default in the Advanced Settings "Including configuration objects in import of entire content store " on page 285.

If you import the configuration data, especially in a distributed environment with multiple content managers, the current information about the content manager status may be overwritten by the imported data.

Tip: If you import the configuration, restart the service in the target environment to update status information properly.

For information about including configuration data in the import, see "Including configuration objects in import of entire content store " on page 285.

For information about how specific objects in the content store are imported, see "Conflict Resolution Rules For Deploying the Entire Content Store" on page 277.

Deploying Selected Public Folders and Directory Content

You can choose to do a partial deployment, deploying only selected public folders and directory content, rather than the entire content store.

You can deploy any packages and folders in Public Folders. Browse the Public Folders hierarchy and select a package or folder. This will deploy its entire contents. You cannot select specific entries in the packages or folders. During export, the parent packages and folders are not exported and Content Manager does not create placeholder locations for them in the target environment. During both export and import, you can specify a new target location in the Content Manager hierarchy for each deployed package and folder.

The directory content that you can deploy includes the Cognos namespace, distribution lists and contacts, and data sources and their connections and signons.

When you deploy public folders and directory content, you cannot include objects from the configuration, capability, exportDeploymentFolder, and importDeploymentFolder areas of the content store "Partial Deployment Options" on page 272. For more information, see "Including References to Other Namespaces" on page 268.

For information about how specific objects in the content store are imported, see "Deployment Conflict Resolution Rules When Importing and Exporting" on page 275.

After the deployment is complete, some links for packages associated with reports may not work, even if you included packages and their reports in the deployment. You may need to relink packages to reports. For information about linking packages to reports, see the documentation for the studios.

Tip: If you want to deploy specific entries, you can create a folder at the root level of Public Folders, copy the specific entries to that folder, and select this folder when you deploy.

Deploying Packages

During a partial deployment, you can deploy one or more packages at a time.

A package can reference objects that are outside the package, such as security objects, data sources, and distribution lists. However, referenced objects are not deployed with the package.

While you are importing, you can deselect packages in the deployment archive that you do not want to import.

Renaming Packages and Folders

During a partial deployment, you can rename packages and folders so that they have a new name in the target environment.

This is useful if you do not want to overwrite a package or folder that has the same name in the target environment. The original package or folder remains intact, and the deployed one is renamed.

You might also want to add multilingual names for packages and folders so that users can see names suitable for their locale. A locale specifies linguistic information and cultural conventions for character type, collation, format of date and time, currency unit, and messages.

Disabling Packages and Folders

During a partial deployment, you can disable the packages and folders in the target environment so that users cannot access them.

Disabling packages and folders is useful if you want to test them in the target environment before you make them available to users.

You can disable packages and folders at the time of export or import.

When you disable a package or folder, the entries it contains are not accessible in the target environment after the import. Users cannot run, view, or edit entries. Only users who have write privileges to the disabled entries can access them.

Partial Deployment Options

During a partial deployment, when you export and import, you can choose the following options.

If you do not select an option when you export, it is not available during import.

Including Report Output Versions

You can choose to include the report output versions in your deployment. If you select this option, you can choose what to do if there is a conflict. You can replace the existing report output versions in the target environment with those from the deployment archive or keep target environment versions.

Including Run History

The run history of a report shows statistics about the status and times when the report ran "Viewing the run history of entries" on page 243 in your deployment. You can choose whether to include the run history of reports.

If you select this option, you can choose what to do if there is a conflict. You can replace the existing report run histories in the target environment with those from the deployment archive or keep target environment histories.

Including Schedules

You can choose whether to include schedules Chapter 18, "Schedule Management," on page 247 in your deployment. If you do not deploy schedules, they are removed from the jobs and reports in the target environment.

If you select this option, you can choose what to do if there is a conflict. You can replace the existing schedules in the target environment with those from the deployment archive or keep target environment schedules.

When you choose to import schedules in the deployment, you can change the imported schedule credentials to your credentials. The credential of a schedule is the credential used to run the report in the schedule. This credential determines the permissions on the report as well as the capabilities that apply to the report execution. If the report does not have the **Run as the owner** property set to true, then the credential is also used to access the data source, data connection and signon objects. Changing the credential may affect the operation in the following ways:

- no impact
- report produces different data as a result of selecting a different connection or signon in the data source
- report fails to run because the user does not have the proper capabilities or permissions

To change the imported schedule credentials to the credentials of the person doing the import, do the following:

- Add the advanced setting CM.DeploymentUpdateScheduleCredential and set the value to **True**. See procedure, "Setting advanced Content Manager parameters" on page 50.
- When you import to the target environment using the New Import Wizard "Importing to a Target Environment" on page 283, make sure to click **Include schedules** and select **Replace Existing Entries** under **Conflict Resolution**. Next, under **Entry ownership**, select **The user performing the import**.

Including Cognos Groups and Roles

You can choose whether to include Cognos groups and roles Chapter 11, "Users, Groups, and Roles," on page 167 in your deployment.

When you deploy the Cognos groups and roles, you must deploy them all. However, the following built-in groups are not deployed:

- Anonymous
- All Authenticated Users
- Everyone

When you deploy groups, members of the System Administrators group are merged with the members of this group already in the target environment. This ensures that the target environment is accessible in case the deployed members are not valid. However, you may need to modify the membership list when the deployment is complete.

If you select this option, you can choose what to do if there is a conflict. You can replace groups and roles in the target environment with those from the deployment archive or to keep target environment groups and roles.

Including Distribution Lists and Contacts

You can choose whether to include distribution lists and contacts in your deployment. If you choose to deploy distribution lists and contacts, you must deploy them all.

If you select this option, you can choose what to do if there is a conflict. You can specify whether to replace the distribution lists and contacts in the target environment with those from the deployment archive or to keep the target distribution lists and contacts.

Including Data Sources

You can choose to include data sources and their associated connections Chapter 6, "Data sources and connections," on page 89 in your deployment. If you choose to deploy data sources, you must deploy them all.

You can deploy the data sources with or without their signons. If you do not deploy the signons, you must configure the data sources accordingly in the target environment. If you deploy the signons, you must encrypt the deployment archive.

If you select this option, you can choose what to do if there is a conflict. You can specify whether to replace the data sources in the target environment with those from the deployment archive or to keep the target environment data sources.

If you replace the target data sources, and the data source connections in the source and target environments do not match, you can lose database connections. In this case, you must manually reconnect to the data sources in the target environment after the import, using the database client software.

Including Access Permissions

You can choose to include access permissions "Access Permissions" on page 268 in your deployment.

If you select this option, you can choose what to do if there is a conflict. You can specify whether to replace the access permissions in the target environment with those from the deployment archive or to keep the target environment access permissions.

Recording Deployment Details

You can specify what type of information is saved in the deployment records by setting the **Recording Level** for the deployment. The amount of information kept in the records has an impact on performance.

You can set the following recording levels:

- **Basic**

  Saves the deployment progress and summary information. This is the default option.
- **Minimal**

  Saves only the deployment summary information. This option requires the least memory.
- **Trace**

  Saves all deployment details. This option requires the most memory.

For information about recording deployment details when an entire content store is deployed, see "Deployment History" on page 270.

Ownership Considerations

You can change the ownership of imported entries to the user performing the import. You can select this option at the time of export or import. If you use the owners from the source, the owners are imported along with the entries. You can apply the ownership options to new entries or to new and existing entries.

Advanced Deployment Settings

You can use advanced settings to specify how deployment works in your environment.

Using the advanced settings, you can

- specify if report output is part of deployment
- specify if configuration objects and children are part of deployment

Specifying if report output is part of deployment

You can specify if report output is part of deployment.

There are two advanced settings that you can use:

- CM.DEPLOYMENTSKIPALLREPORTOUTPUT to include or skip all report output from **My content** and **Team content**.
- CM.DEPLOYMENTSKIPUSERREPORTOUTPUT to include or skip user report output from **My content** only.

By default, these are set to False (exclude). To change the default to include, set them to True.

Before you begin

You must have the required permissions to access **IBM Cognos Administration** Chapter 13, “Capabilities,” on page 185.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. From the **Systems** Action menu, click **Set properties**.
3. Click the **Settings** tab.
4. Click **Edit** next to **Advanced Settings**.
5. Select **Override the settings acquired from the parent entry**.
6. In the **Parameter** column, type CM.DEPLOYMENTSKIPALLREPORTOUTPUT or CM.DEPLOYMENTSKIPUSERREPORTOUTPUT.
7. In the **Value** column, type the setting that you want to use.
8. Click **OK**.
9. On the **Set properties** page, click **OK**.

Including configuration objects and their children in deployments

To include configuration objects and their children as part of deployments, set the advanced property CM.DEPLOYMENTINCLUDECONFIGURATION to true. By default, in IBM Cognos Analytics, the value for the property is false.

Before you begin

You must have the required permissions to access **IBM Cognos Administration** Chapter 13, “Capabilities,” on page 185.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. Click the arrow for the Actions menu next to **Systems** and click **Set properties**.
3. Click the **Settings** tab.
4. Click **Edit** next to **Advanced Settings**.
5. Select **Override the settings acquired from the parent entry**.
6. In the **Parameter** column, type CM.DEPLOYMENTINCLUDECONFIGURATION.
7. In the **Value** column, type the setting that you want to use.
8. Click **OK**.
9. On the **Set properties** page, click **OK**.

Deployment Conflict Resolution Rules When Importing and Exporting

Conflict resolution rules apply when you are importing or exporting into a target environment.

The rules are different depending on whether you deploy the entire content store or selected public folders and directory content. The method you choose determines which objects are included in the import and how conflicts are resolved when an object already exists in the target environment.

Objects in the content store represent entries in the portal and the properties of those entries. For example, the object reportView represents a report view entry in the portal and the object runHistory represents the run history of an entry. For more information about objects, see the IBM Cognos Software Development Kit *Developer Guide*.

Objects in **Public Folders** inherit deployment rules by default, depending on whether you are deploying the entire content store, or only selected **Public Folders** and directory content.

Although conflicts can occur only during importing, not during exporting, the same rules are used to process objects in the archive during export. During an export operation, if the rule for an object is KEEP, it is not included in the archive. For any other setting, it is included in the archive.

Conflict Resolution Rules

A conflict can occur when the entry that you want to import from the deployment archive already exists in the target content store.

When this happens, one of the following conflict resolution rules is used, depending on the entry and the advanced settings that you have used.

Table 70. Conflict resolution rules

Rule	**Description**
Replace	Replaces the entry and its children. The entry and all its children are removed from the source content store. The new entry and all its children are added to the source content store.
Keep	Keeps the entry. The properties of the entry and all its children are not updated. Existing children of the entry are kept. New children may be added.
Update	Updates the entry. The properties of the entry and its children are updated. Existing children of the entry are kept. New children may be added.
Merge	Merges the properties of the entries with existing entries.

If an entry has no children, replace and update have the same end result.

Content

All the objects in the content area of the content store are included and replaced when you import the entire content store.

Directory

If you include data sources, connections, and signons, and you keep existing entries, the associated objects from the archive are merged with the objects in the target environment. Even though the objects are merged, the retention rules still apply. A full merge may not occur because some objects may be discarded.

Note that when you want to include Cognos groups and roles, and distribution lists and contacts, these items must be stored in a folder within the namespace in order to be deployed.

The members of distribution lists, groups, and roles in the archive are not merged with the contents in the target environment. Instead, the set of distribution lists, groups, and roles are merged with the set already existing in the target environment. However, the members of the System Administrators group are always merged when this group is imported. For more information, see "Including Cognos Groups and Roles" on page 273.

Conflict Resolution Rules For Deploying the Entire Content Store

The default conflict resolution rule for deploying the entire content store is replace.

Exceptions to the default conflict resolution rule are listed in the following table:

Table 71. Full deployment, exceptions to the default conflict resolution rule

Object name	**Conflict Resolution Rule**
OUTPUT, GRAPHIC, PAGE	Keep if • the advanced setting CM.DEPLOYMENTSKIPALLREPORTOUTPUT is set to True • the object is under user accounts and the advanced setting CM.DEPLOYMENTSKIPUSERREPORTOUTPUT is set to True For more information on the settings, see "Specifying if report output is part of deployment" on page 274.
ACCOUNT	Update if **Include user account information** is selected during deployment, keep if not. For more information about including user account information, see "Deploying the Entire Content Store" on page 269.
SESSION, CACHEOUTPUT, REPORTCACHE, REPORTMETADATACACHE, DEPLOYMENTDETAIL	Keep
FOLDER, MRUFOLDER, SUBSCRIPTIONFOLDER	Replace if directly under Cognos namespace user account object (**My Folders** folder) or directly under 3rd party namespace user account object (**My Folders** folder).
CAPABILITY, SECUREDFUNCTION, CONFIGURATION, CONFIGURATIONFOLDER, DISPATCHER, DIRECTORY, NAMESPACE, NAMESPACEFOLDER, PORTAL, PORTALPACKAGE, PORTALSKINFOLDER, PORTLETFOLDER, PORTLETPRODUCER, PORTLET, PAGELETFOLDER, PAGELET, PAGELETINSTANCE, PORTLETINSTANCE	Update
ROLE, GROUP	Replace (but preserve object ID).
CONTENT, ADMINFOLDER, TRANSIENTSTATEFOLDER	Replace. Note that the deployment option entireContentStoreReplace can be changed to false (update) using a Software Development Kit application only. For more information, see your Software Development Kit documentation.

Table 71. Full deployment, exceptions to the default conflict resolution rule (continued)

Object name	Conflict Resolution Rule
HISTORY, HISTORYDETAIL, HISTORYDETAILREQUEST ARGUMENTS	Keep if under ADMINFOLDER object.

Conflict Resolution Rules For Partial Deployment

When you deploy public folders and directory content rather than the entire content store, you can select the content that you want to deploy.

Some conflict resolution rules depend on the choices you make.

When a parent object is updated, new children from the deployment archive are added and join the existing set of children in the target environment. If a conflict occurs, the conflict resolution rule is to replace the children.

Because all job steps are replaced, no conflict is possible when importing jobStepDefinition objects.

If you include report output versions and run histories and you keep existing entries, the associated objects from the archive are merged with the objects in the target environment. Even though the objects are merged, the retention rules still apply. A full merge may not occur because some objects may be discarded.

The default conflict resolution rule for partial deployments is replace.

Exceptions to the default conflict resolution rule are listed in the following table:

Table 72. Partial deployment, exceptions to the default conflict resolution rule

Object name	Conflict Resolution Rule
REPORTVERSIONSQL	Depends on whether **Include report output versions** is set to replace or keep "Including Report Output Versions" on page 272.
OUTPUT	Keep if advanced setting DEPLOYMENTSKIPREPORTOUTPUT is set to True "Specifying if report output is part of deployment" on page 274. Otherwise, depends on whether **Include report output versions** is set to replace or keep "Including Report Output Versions" on page 272.
GRAPHICPAGE	Keep if advanced setting DEPLOYMENTSKIPREPORTOUTPUT is set to True "Specifying if report output is part of deployment" on page 274. Otherwise, depends on whether **Include report output versions** is set to replace or keep "Including Report Output Versions" on page 272.
HISTORY	Depends on whether **Include run history** is set to replace or keep "Including Run History" on page 272.

Table 72. Partial deployment, exceptions to the default conflict resolution rule (continued)

Object name	**Conflict Resolution Rule**
SCHEDULE	Depends on whether **Include schedules** is set to replace or keep "Including Schedules" on page 272.
JOBSTEPDEFINITION	Replace.
JOBDEFINITION	Update and remove any JOBSTEPDEFINITION children.If PackageHistories is specified and packageHistoriesConflictResolution is set to replace, remove HISTORY objects as well.
DATASOURCE, DATASOURCECONNECTION, DATASOURCENAMEBINDING	Depends on whether **Include data sources and connections** is set to keep or replace"Including Data Sources" on page 273.
DATASOURCESIGNON	Depends on whether **Include data sources and connections** and **Include signons** are set to keep or replace "Including Data Sources" on page 273.
DISTRIBUTIONLIST, CONTACT	Depends on whether **Include distribution lists and contacts** is set to keep or replace "Including Distribution Lists and Contacts" on page 273.
ROLE, GROUP	Depends on whether **Include Cognos groups and roles** is set to keep or replace "Including Cognos Groups and Roles" on page 273. (If it is set to replace, object ID is preserved.)
CACHEOUTPUT, REPORTCACHE, REPORTMETADATACACHE	Keep

Deploying IBM Cognos Entries

To deploy IBM Cognos software, you must export the deployment archive in the source environment, then move the archive to the target environment and import it there.

You can organize your deployment specification in folders in the same way that you organize all your entries.

Deployment and Agents

Deployment can be part of an agent.

Deployment Schedules and Run History

You can schedule deployment to run automatically at a specified time or as part of a job. IBM Cognos software saves the run history for each deployment specification. After you export or import, you can view the date and time and the status of the deployment. You can also view any error messages created by the deployment and the list of entries that were exported or imported. For more information, see Chapter 17, "Managing scheduled activities," on page 225.

Permissions

To deploy IBM Cognos entries, you must have execute permissions for the **Administration tasks** secured feature and traverse permissions for the **Administration** secured function. For more information, see Chapter 13, “Capabilities,” on page 185.

You should also belong to the System Administrators group and have read and write access to the Cognos namespace so that you can deploy the System Administrators group. For more information, see “Set access permissions for an entry” on page 179.

When you do a partial export of public folders and directory content “Deploying Selected Public Folders and Directory Content ” on page 271 rather than exporting the entire content store “Deploying the Entire Content Store” on page 269, you must have read and traverse permissions for the entries that you export. You also need write permissions because you create a deployment specification and deployment history when you export. When you import, you must have write and set policy permissions for the entries that you import.

Prerequisites

IBM Cognos software and other products, must be installed and configured in the source and target environments. For more information, see the IBM Cognos *Installation and Configuration Guide*.

We recommend that you stop the Content Manager service before you export and import. This prevents users from receiving unpredictable results if they are performing operations during the deployment. For example, if users view reports in a package while the package is being imported, users may encounter errors when the report outputs are replaced. For more information, see “Stopping and starting dispatchers and services” on page 40.

Before you start, you must plan the deployment to determine what deployment options to use and what entries to deploy “Deployment Planning” on page 268. You may want to do a back up before deployment Chapter 8, “Back Up Data,” on page 149.

Exporting from a Source Environment

To export the IBM Cognos entries, you create or modify an export deployment specification and then run the export.

You can also use a previously saved deployment specification for export or for redeployment of your entries.

The entries are exported to an export deployment archive “Deployment Archives” on page 267 in the source environment. Later, you import the archive entries into the target environment. You can update the entries in the target environment using the entries from the deployment archive.

For information on conflict resolution during deployments, see “Deployment Conflict Resolution Rules When Importing and Exporting” on page 275.

When you export, you select the entries to deploy, and you set the options that are used as defaults when importing.

Creating a new export deployment specification

An export deployment specification defines the content that must be exported.

For information about exporting content in a multitenant IBM Cognos Analytics environment, see “Tenant content deployment” on page 313.

Before you begin

If you want to preserve data source access accounts when you export a content store, then you must select **Include user account information**. If you want to preserve configuration information when you export, then you can set the CM.DEPLOYMENTINCLUDECONFIGURATION advanced setting to TRUE. For more information, see “Including configuration objects and their children in deployments ” on page 275.

Procedure

1. In the source environment, open **IBM Cognos Administration**.
2. On the **Configuration** tab, click **Content Administration**.
3. On the toolbar, click the **New Export** icon . The **New Export** wizard appears.
4. Type a unique name and an optional description and screen tip for the deployment specification. Select the folder where you want to save it and click **Next**.
5. Choose whether to export the entire content store or to do a partial export of specific content:
   - To export specific content, click **Select public folders, directory and library content**. Click **Next** and proceed to step 7.
   - To export the entire content store, click **Select the entire content store** and select whether to include user account information. Click **Next** and proceed to step 15.
6. In the **Select the Public folders content** page, click **Add**.
7. In the **Select entries** page, in the **Available Entries** box, select one of the following entries or their contents:
   - **Public Folders**

     Contains packages and folders. Select the packages and folders that you want to export.
   - **Directory**

     Contains namespaces, namespace folders, groups and roles, and individual user accounts. When you select a user account, all content associated with the user, including the content of the user's **My Folders**, is included in the export.
   - **Library**

     Contains library resources, such as visualizations.
8. Click the arrow icon to move the selected items to the **Selected entries** box, and click **OK**.
9. For each entry that you are exporting, do one of the following:
   - If you want the entry to have a different name in the target environment, or if you want to change the target location or add multilingual names, click the **Edit** icon , make your changes, and click **OK**.
   - If you do not want users to access the entries and their contents, select the check box in the **Disable after import** column. This is useful, for example, when you want to test the reports before you make them available in the target environment.
10. Under **Options**, select whether you want to include the report output versions, run history, and schedules and what to do with entries in case of a conflict.
11. In the **Select the directory content** page, select whether you want to export Cognos groups and roles, distribution lists and contacts, and data sources and connections and what to do with the entries in case of a conflict.
12. In the **Specify the general options** page, select whether to include access permissions and references to namespaces other than **IBM Cognos**, and who should own the entries after they are imported in the target environment.
13. Specify the **Recording Level** for the deployment history. For more information, see "Recording Deployment Details" on page 274.
14. In the **Specify a deployment archive** page, under **Deployment archive**, select an existing deployment archive from the list, or type a new name to create one.

    If you are typing a new name for the deployment archive, do not use spaces in the name. If the name of the new deployment specification matches the name of an existing deployment archive, the characters _# are added to the end of the name, where # is a number such as 1.
15. Under **Encryption**, click **Set the encryption password**, type a password, and click **OK**.
16. Click **Next**.

The summary information appears.

17. Review the summary information and click **Next**.

    If you want to change the information, click **Back** and follow the instructions.
18. Specify how to run the export deployment specification:

    - To run now or later, click **Save and run once** and click **Finish**. Specify the time and date for the run. Then click **Run**. Review the run time and click **OK**.
    - To schedule at a recurring time, click **Save and schedule** and click **Finish**. Then, select frequency, start and end dates, and click **OK**.

      Tip:

      To temporarily disable the schedule, select the **Disable the schedule** check box. To view the schedule status, see "Managing scheduled activities" on page 259.
    - To save without scheduling or running, click **Save only**, and click **Finish**.

Results

After you run the export, you can move the deployment archive. You can also see the export run history "Viewing the run history of entries" on page 243.

Modifying an existing deployment specification

You can reuse a previously saved deployment specification for export or for redeployment of your entries.

Procedure

1. In the target environment, open **Launch IBM Cognos Administration**.
2. On the **Configuration** tab, click **Content Administration**.
3. In the **Actions** column, click the properties button ▤ for the deployment specification you want to modify, and then click the **Export** tab.
4. Modify the deployment options as required.

   Tip: If you want to change the export target location, click the edit button ✎ next to the export name in the **Target name** column, the **Public Folders content** section, and choose the package or folder you want.
5. Click **OK**.

Results

This saves the options and you can run the export now or at a later time. For more information, see "Running an export" on page 282.

Running an export

After you create a new export deployment archive or modify an existing one, you can run it.

Procedure

1. In the **Actions** column, click the run with options button ▶.
2. Click **Now** to run the export immediately, or click **Later**, and enter the time, that you want the export to run.

   You can also schedule a task to run on a recurring basis, and view a list of scheduled tasks. For more information, see Chapter 18, "Schedule Management," on page 247.

To avoid warning messages when logged into multiple namespaces, before you run the export next time, renew your credentials.

Results

You can now move the deployment archive.

Move the Deployment Archive

Move the deployment archive that you created in the source environment to the target environment.

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

The location where deployment archives are saved is set in the configuration tool. The default location is *install_location*/deployment.

Before you begin

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

Procedure

1. Copy the deployment archive from the source environment to a location on the LAN or to a CD.
2. Copy the deployment archive from the LAN or CD to the target environment in the location set in the configuration tool.

Results

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

Importing to a Target Environment

Create a new import deployment specification or modify an existing one and then run the import.

You can import using an existing deployment specification if you previously saved it without importing, or if you want to redeploy your IBM Cognos entries. You can update the entries in the target environment with entries from the deployment archive.

For information on conflict resolution during deployments, see "Deployment Conflict Resolution Rules When Importing and Exporting" on page 275.

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 cannot select options that were not included in the deployment archive during the export. For information about how specific objects in the content store are imported, see "Deployment Conflict Resolution Rules When Importing and Exporting" on page 275.

You can also use the New Import wizard to upgrade entries from previous releases of the product. You can upgrade report specifications during the import, or choose to upgrade them at a later time using the New Report Upgrade wizard. For more information, see "Upgrading report specifications" on page 286.

When you run an import, content store ids are deleted and new ids assigned. If the store ids must be retained because they are used by certain IBM Cognos functionality, you can choose to preserve store ids. For more information, see "Content ID assignment" on page 287.

To use an existing import deployment specification, see "Modifying an existing import deployment specification" on page 284

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

Creating a new import deployment specification

An import deployment specification defines the content that must be imported.

For information about importing content in a multitenant IBM Cognos Analytics environment, see “Tenant content deployment” on page 313.

Procedure

1. In the target environment, open **IBM Cognos Administration**.
2. On the **Configuration** tab, click **Content Administration**.
3. On the toolbar, click the **New Import** icon . The **New Import** wizard appears.
4. In the **Deployment archive** box, click the deployment archive that you want to import.
5. Type the password that was used to encrypt the content, and click **OK** and then **Next**.
6. Type a unique name and an optional description and a screen tip for the deployment specification, select the folder where you want to save it, and click **Next**.
7. Select the content that you want to include in the import.

   Tip: To ensure that the required target entries exists in the target content store, click the edit button next to the package, and check the location. If you want, you can change the target location now.
8. Select the options that you want, along with your conflict resolution choice for options that you select.
9. In the **Specify the general options** page, select whether to include access permissions and references to namespaces other than **IBM Cognos**, and who should own the entries after they are imported in the target environment.
10. Specify the **Recording Level** for the deployment history. For more information, see “Recording Deployment Details” on page 274.
11. Click **Next**.
12. Review the summary information and click **Next**.
13. Select how to run the import deployment specification:

    - To run now or later, click **Save and run once** and click **Finish**. Specify the time and date for the run. Then click **Run**. Review the run time and click **OK**.
    - To schedule at a recurring time, click **Save and schedule** and click **Finish**. Then, select frequency, start and end dates, and click **OK**.

      Tip: To temporarily disable the schedule, select the **Disable the schedule** check box. To view the schedule status, see “Managing scheduled activities” on page 259.
    - To save without scheduling or running, click **Save only** then click **Finish**.

      When you run the import, you have the option of selecting to upgrade the report specification. If you choose not to upgrade the deployment specification at this time, you can upgrade it later. For more information, see “Upgrading report specifications” on page 286.

Results

After you run the import, you can test the deployment. You can also see the import run history “Viewing the run history of entries” on page 243.

Modifying an existing import deployment specification

You can modify an existing deployment specification.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Content Administration**.
2. In the **Actions** column, click the properties button for the deployment specification you want to modify, and then click the **Import** tab.
3. Modify the deployment options as required.

   Tip: If you want to change the import target location, click the edit button next to the import name in the **Target name** column, the **Public Folders content** section, and choose the package or folder you want.
4. Click **OK**.

Results

This saves the options and you can run the import now or at a later time. For more information, see "Run an Import" on page 285.

Run an Import

After creating or modifying an import deployment specification, run the import.

Procedure

1. In the **Actions** column, click the run with options button .
2. Click **Now** to run the import immediately, or click **Later**, and enter the time, that you want the import to run.
3. If you want to upgrade the report specifications, click **Upgrade all report specifications to the latest version**.

   You can also schedule a task to run on a recurring basis, and view a list of scheduled tasks. For more information, see Chapter 18, "Schedule Management," on page 247.
4. To specify how to assign content ids, under **Content IDs** select
   - **Assign new IDs during import** to replace the existing content ids with new ids
   - **Do not assign new IDs during import** to keep existing content ids on import

Results

You can now test the deployment.

Including configuration objects in import of entire content store

You can include configuration objects when importing an entire content store.

Before you begin

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. For more information, see "Conflict Resolution Rules For Deploying the Entire Content Store" on page 277.

We recommend that you do not import configuration objects. Dispatchers should be configured in your target environment before you import data from a source environment. If you must import configuration objects, you should either stop the source dispatcher services before the import, or restart IBM Cognos software in the target environment after the import. Otherwise, you may get errors with the status of dispatchers. If you want to import configuration objects, you must be prepared for a brief interruption of services.

Procedure

1. Follow the steps in the section "Configuring advanced settings for specific dispatchers" on page 464.
2. For the **ContentManagerService**, type **`CM.DEPLOYMENTINCLUDECONFIGURATION`** as the **Parameter** name.
3. Type **true** as a value for this parameter, and click **OK**.

Testing Deployed Applications

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

You can test your deployment by

- reviewing the run history for a deployment
- ensuring that the correct packages and folders were imported along with their contents
- ensuring that the data sources, distributions lists and contacts, and Cognos groups and roles were imported
- verifying the permissions for the imported entries
- ensuring that the schedules were imported
- ensuring that any references to renamed packages were updated
- running imported reports and report views

Upgrading report specifications

If you did not upgrade report specifications when you ran the import wizard, you can upgrade them using the New Report Upgrade wizard.

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. Log on as an administrator with execute permissions for the **Content Administration** feature.
2. Open **IBM Cognos Administration**.
3. On the **Configuration** tab, click **Content Administration**.
4. Click the arrow on the new content maintenance button on the toolbar, and then click **New Report Upgrade**
5. Type a name for the upgrade task and, if you want, a description and screen tip. Click **Next**.
6. 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.
7. 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.

Content ID assignment

When you run an import deployment, you can choose how to assign content IDs for objects in the content store.

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 archiving report output to an external report repository. If so, you can choose to preserve content IDs when you run the import. For more information about how to assign IDs when importing objects, see "Run an Import" on page 285.

Preserving content IDs can be applied to a partial deployment or a deployment of the entire content store.

Content ID conflicts

When you retain existing content IDs, conflicts can occur on import. Here are the conflict situations that can occur.

Table 73. Conflict with matching content ID

Information	Details
Description	When an imported object exists in the target environment in a different location but with an matching content ID, the ID is not preserved on import but replaced with a newly generated ID. The object that exists in the target environment could be another version of the same object or it could be a completely different object.
Warning	A warning message will describe that the content was not preserved and, if the security privileges allow, will identify which object in the target environment is in conflict. No information is issued about how to resolve the conflict.
Resolution	To resolve any content ID conflicts, you can • Make no changes to content IDs after import and keep IDs as they are. Any links for the imported object would now point to the target environment object which most likely is an older version of the same object. If the content ID for the imported object is not referenced from outside the content store, then there will be no broken external references after the import. The imported object will continue to exist as a separate object. • Delete the imported object and the object in the target environment. If the object is re-imported, the object is added to the same location with its content ID. • Manually update the target object with properties from the imported object. Any links for the object are preserved as the content ID will not have changed. The imported object could then be deleted.

Table 74. Conflict with different content ID

Information	Details
Description	When an imported object exists in the target environment in a same location but with a different content ID, the ID will be preserved on import and will replace the existing ID in the target environment.
Warning	No warning message is issued.
Resolution	Note that all existing external references to the target content ID, if any, are permanently lost when the content ID is replaced.

Deploy Human Task and Annotation Services

Content for the Human Task and Annotation services are stored separately from the main content store. This content may be stored in the same database as the content store as different tables or in a separate database. To deploy this content, scripts are used, rather than the deployment tool.

The procedure in this topic describes using scripts to deploying human task and annotation service content. For information about using scripts to deploy IBM Cognos Workspace comments, see "Deploying IBM Cognos Workspace comments" on page 289.

You deploy them by running a batch file, which retrieves your human tasks or annotations from a source database. Then you run another batch file to install them on a destination server.

Procedure

1. Create task data in your database by creating a selection of tasks pointing to valid reports.

   For instructions on creating user tasks, see the IBM Cognos Event Studio *User Guide*. For more information about annotations (comments), see the *IBM Cognos Workspace User Guide*.
2. On the source server, open a command prompt in *install_location*/bin.
3. Run the file htsDeployTool with the following arguments:

   `htsDeployTool -camUsername` *camUsername* `-camPassword` *camPassword* `-camNamespace` *camNamespace* `-exportFile` *exportFileName* `-password` *exportFilePassword*

   where:

   - *camUsername* is the username for the namespace.
   - *camPassword* is the user password for the namespace.
   - *camNamespace* is the name of the namespace.
   - *exportFileName* is the name of the export file that will be created, for example, HumanTaskExportFile1.
   - *exportFilePassword* is the password for the export file.

   Enclose arguments that contain spaces in quotes. Precede special characters with a backslash. For example:

   ```
   htsDeployTool -exportFile "jan\'s file" -password test2Password -
   camNamespace default -camUsername myId -camPassword myPassword
   ```

   To allow anonymous access, omit the -cam arguments.

   To export annotations, add the argument `-persistenceUnit annotations`. For example:

   ```
   -camPassword <camPassword> -camNameSpace <camNamespace> -exportfile
   AnnotationExportFile1 -password <exportFilePassword> -persistenceUnit
   annotations.
   ```
4. Check to make sure that the file <exportFileName>.xml.gz was created in *install_location*/deployment. For example, HumanTaskExportFile1.xml.gz. Copy it.
5. On the destination server, paste the file <exportFileName>.xml.gz in *install_location*/deployment.
6. On the destination server, open a command prompt in *install_location*/bin and run the file htsDeployTool with the following arguments:

   `htsDeployTool -camUsername` *camUsername camPassword* `-camNamespace` *camNamespace* `-importFile` *importFileName* `-password` *importFilePassword*

   where:

   - *camUsername* is the username for the namespace.
   - *camPassword* is the user password for the namespace.
   - *camNamespace* is the name of the namespace.

- *importFileName* is the name of the file that you created in step 3.
- *importFilePassword* is the password for the file that you created in step 3.

See additional syntax tips in step 3.

Deploying IBM Cognos Workspace comments

You can deploy IBM Cognos Workspace comments using the following procedure.

Procedure

1. On the computer that has the annotations that you want to deploy, export the content store.

   For information about exporting a content store, see "Creating a new export deployment specification" on page 280.
2. On the source server, open a command prompt in the install_location/bin folder.
3. In the bin folder, run the file named htsDeployTool with the following arguments:

   htsDeployTool -persistenceUnit annotations -camUsername *camUsername* -camPassword *camPassword* -camNamespace *camNamespace* -exportFile *exportFileName* -password *exportFilePassword*

   where

   camUsername is the username for the namespace

   camPassword is the user password for the namespace

   camNamespace is the name of the namespace

   exportFileName is the name of the export file that will be created, for example, HumanTaskExportFile1

   Example: htsDeployTool -persistenceUnit annotations -exportFile myFile -password test2Password -camNamespace default -camUsername myId -camPassword myPassword

   To allow anonymous access, omit the -cam arguments.
4. Check to make sure that the file *exportFileName*.xml.gz was created in install_location/deployment. For example, HumanTaskExportFile1.xml.gz. Copy it.
5. On the destination server, import a deployment. For information about deployment and import specifications, see "Deployment Specifications" on page 267.
6. On the destination server, paste the file *exportFileName*.xml.gz in install_location/deployment.
7. On the destination server, open a command prompt in install_location/bin and run the htsDeployTool with the following arguments:

   htsDeployTool -persistenceUnit annotations -camUsername *camUsername* -camPassword *camPassword* -camNamespace *camNamespace* -importFile *importFileName* -password *importFilePassword*

   where

   camUsername is the username for the namespace

   camPassword is the user password for the namespace

   camNamespace is the name of the namespace

   importFileName is the name of the export file that you created in step 3

   importFilePassword is the password for the file that you created in step 3

Storing and reporting on IBM Cognos Workspace comments

This topic provides information about storing and reporting on Cognos Workspace comments.

Storing comments

Comments are stored within their own database tables which can be either in the same database as the content store or in a separate database. The Human Task and Annotation Services property in IBM Cognos Configuration defines the database connection to the database where the annotation tables are stored. If a database connection for Human task service and Annotation service property is not specified, the annotation tables are created in the content store database.

The Human Task and Annotation Services property also defines the database connection for the Human task service tables. However, although the human task service and Annotation service share a database connection, the annotation and human task tables are separate. Annotation tables are prefixed with ANS_ and human task service tables are prefixed with HTS_.

Users are provided scripts to export and import annotation and human task data from the tables to the destination IBM Cognos server. The scripts facilitate activities such as, backing up and restoring comments, and deploying comments between servers.

Reporting on comments

In IBM Cognos Analytics, there is no view or IBM Cognos Framework Manager model representation of Cognos Workspace comments included out of the box. However, you can create a model based on the Annotation service database tables in Framework Manager. The tables, which are simple, can be used to find the comment or annotation text, the person who created the comment, the date that the comment was created, and the report with which the comment is associated. You can also report on the context of a comment by creating a report model or query for the schema where the comments are stored. The dimensions, dimension members, metadata items, and data items would constitute the context of the annotation in the report.

Chapter 20. Packages

You can create packages for Cognos PowerCube and SAP BW data sources from IBM Cognos Administration.

A modeler can create a package while publishing PowerCubes from Transformer. For more information, see the Transformer *User Guide*.

A modeler can also create and publish packages using Framework Manager. For information, see the Framework Manager *User Guide*.

Create a Package for a PowerCube

Before you can use a PowerCube data source in any of the IBM Cognos studios, you must create a package.

When you create a PowerCube data source, you are given the option to create a package using your new data source. You can also create a package for an existing PowerCube data source.

To perform these tasks, you must have execute permissions for the Data Source Connections secured feature.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Data Source Connections**.
2. Select the new data source button.
3. Complete the steps in the **New Data Source wizard**.
   - On the **Specify the connection** page, from the **Type** list, select **IBM Cognos PowerCube**.
   - On the **Finish** page, select **Create a package**.

SAP BW Packages

Before you can use a SAP BW data source in any of the IBM Cognos studios, you must create a package.

When you create a SAP BW data source from IBM Cognos Administration, you are given the option to create a package using your new data source. You can also create a package for an existing SAP BW data source. For more information, see "Data source connections" on page 115.

To edit a SAP BW package after it is created, see "Edit an SAP BW Package" on page 292.

To set the maximum number of objects used in SAP BW packages, see "Setting the maximum number of objects used in SAP BW packages" on page 292

To perform these tasks, you must have execute permissions for the Data Source Connections secured feature, see Chapter 13, "Capabilities," on page 185.

You can set how many objects can be used in a SAP BW package. For information about creating and publishing packages using Framework Manager, see the Framework Manager *User Guide*.

Create an SAP BW Package

The procedure to create a SAP BW Package is as follows.

About this task

For more information, see "SAP Business Information Warehouse (SAP BW) Data Sources" on page 108.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Data Source Connections**.
2. Select the new data source button.
3. Complete the steps in the **New Data Source wizard**.
   - On the **Specify the connection** page, from the **Type** list, select **SAP BW**.
   - On the **Finish** page, select **Create a package**.

Edit an SAP BW Package

The procedure to edit a SAP BW Package is as follows.

Procedure

1. Click **More** beside the package, then click **Edit Package**.
2. Select on of the following options:
   - To modify metadata selections, click **Modify metadata selections**. Return to step 5 in "Create an SAP BW Package" on page 291.
   - To edit the package variables, click **Edit variables**. Click the value you want to edit, then select or type the new variable. Click **OK**.
   - To modify the package settings, click **Modify package settings**, and select **Use Dynamic Query Mode**.

Setting the maximum number of objects used in SAP BW packages

You can set the maximum number of cubes and info queries that can be included when a SAP BW package is created.

The longer a SAP BW import takes, the more time the server spends processing the request, which could have an impact on its performance for other applications. Find a balance between the number of cubes and info queries commonly needed by users and the potential impact on server performance.

The following (case-sensitive) parameters are available:

- **`com.ibm.cognos.metadatauiservice.sap.maxcubes`**

  The maximum number of cubes that can be used in a SAP BW package. Valid settings are zero and greater. The default is 2.

- **`com.ibm.cognos.metadatauiservice.sap.maxInfoQueries`**

  The maximum number of info queries that can be used in a SAP BW package. Valid settings are zero and greater. The default is 5.

For more information about SAP BW data sources and creating SAP BW packages, see Chapter 6, "Data sources and connections," on page 89.

Procedure

1. In **IBM Cognos Administration**, on the **Status** tab, click **System**.
2. In the **Scorecard** pane, from the change view menu of the current view, click **Services** > **Metadata**.

   Tip: The current view is one of **All servers**, **All server groups**, **All dispatchers**, or **Services**.
3. From the **Metadata service Actions** menu, click **Set properties**.
4. Click the **Settings** tab.
5. Next to **Advanced Settings**, click **Edit** .
6. Select **Override the settings acquired from the parent entry**.

7. In the **Parameter** column, type the parameter name.

   For example, type `com.ibm.cognos.metadatauiservice.sap.maxcubes`.
8. In the **Value** column, type the associated value for the setting.
9. Continue typing setting names and values as required.
10. Click **OK**.
11. On the **Set properties** page, click **OK**.

Chapter 21. Managing User Profiles

A user profile defines the portal tabs that the user can access and specifies user preferences, such as the product language, preferred output format of reports, and the style used in the user interface.

A user profile is created when the user logs on to IBM Cognos software for the first time. It can also be created by an administrator. Initially, the profile is based on the default user profile.

Users can view and change the preferences associated with their profile.

To copy, edit, or delete user profiles, an administrator must have write permissions for the namespace that contains the applicable users. The IBM Cognos predefined role, **Directory Administrators**, does not have write permissions for namespaces other than the **Cognos** namespace. **System Administrators** must grant write permissions to **Directory Administrators** so that they can administer user profiles for the namespace.

To manage user profiles, you must have the required access permissions for **IBM Cognos Administration**.

For more information about managing accounts, see Chapter 11, “Users, Groups, and Roles,” on page 167.

Related concepts
Server administration

Edit the Default User Profile

The default user profile is defined in the **Cognos** namespace. It contains settings that apply to all new users. You can edit the default user profile for your users to minimize the number of changes you need to make to individual user profiles.

After you change the default user profile, it applies only to users who log on to IBM Cognos software for the first time. The existing user profiles of other users are not affected.

Procedure

1. In **IBM Cognos Administration**, on the **Security** tab, click **Users, Groups, and Roles**.
2. Click the **Cognos** namespace.
3. On the toolbar, click the edit default user profile button .
4. Set the default user profile and click **OK**.

Results

Each user who logs on to IBM Cognos software for the first time will automatically inherit these settings but can change them later.

View or Change a User Profile

You can view or change user profiles.

You can delete specific items in the user's profile. This may be useful in the following situations:

- The user's content is taking up so much space that performance is affected. You want to delete some or all of the content.
- You want to view a user profile before deleting it to ensure that you do not delete any important content.

If a user was deleted in your authentication provider, the user no longer appears in IBM Cognos software and you cannot change the user profile.

You can only see the profiles of users who logged on at least once. When users log on, a date is displayed in the **Modified** column.

To view a user profile, delete content, or change content, you must have traverse permissions for the user account and any folder containing content owned by the user. You must have write permissions for the entry and the parent of the entry that you want to delete.

You can change the user profile for individual users, but not for groups or roles.

Viewing or changing a user profile

You can view or change a user profile.

Procedure

1. In **IBM Cognos Administration**, on the **Security** tab, click **Users, Groups, and Roles**.
2. Click the namespace that contains the user.
3. Find the user whose preferences you want to view or change.
4. In the **Actions** column, click **More**.
5. Click **Set preferences**.
6. Click the different tabs to view or change the settings.
7. Click **Cancel** to exit without making changes, or make changes and click **OK**.

Delete Content

You can delete specific items in the user's profile, such as the content of My Folders or pages.

Procedure

1. In **IBM Cognos Administration**, on the **Security** tab, click **Users, Groups, and Roles**.
2. Select the namespace that contains the user.
3. Find the user.
4. In the **Name** column, click the user name.

   Tip: If the user name is not a link, it means that the user profile was not created. To create the profile, in the **Actions** column, click the create this user's profile button, and proceed with the rest of the steps.

   A list of the user's folders appears.
5. Click a folder to see its contents.
6. Click the item that you want to delete from the folder, and click the delete button on the toolbar.

   You cannot delete the folders themselves.

Deleting a user profile

You can delete user profiles from the content store.

When deleting a user in your authentication provider, you may first want to delete the user profile from the content store so that it no longer uses storage space.

You should delete the user profile from IBM Cognos software before deleting the user in the associated namespace. After the user is deleted, the user information no longer appears in IBM Cognos software and you cannot manage the user profile in **IBM Cognos Administration**.

If the user account was already deleted from the associated namespace, you can use content store maintenance to find, and optionally remove, all associated user account information from IBM Cognos software.

If a user with a deleted user profile logs on, an account is created using defaults. If a user is logged on while the associated user profile is being deleted, the user's passport expires and the logon page appears.

Before you delete a user profile, you may want to view its contents to ensure that you are not deleting anything important.

You can work only with profiles of users who logged on at least once.

Before you begin

To delete a user profile, you must have write permissions for the parent object.

Procedure

1. In **IBM Cognos Administration**, on the **Security** tab, click **Users, Groups, and Roles**.
2. Click the namespace that contains the user.
3. Find the user whose user profile you want to delete. You can use the Search feature to find a user.
4. In the **Actions** column, click **More**.
5. Click **Delete this user's profile**.
6. Click **OK**.

Copying user profiles

You may want to copy a user profile.

Copying a user profile is useful in the following situations:

- A user changes names and you are setting up an account in the new name.
- A user moves to another namespace or your organization changes namespaces and you must set up new accounts.
- You are creating many new similar user accounts.

If you plan to delete the source user in your authentication provider, copy the user account information before you delete it. After you delete the user, the user no longer appears in IBM Cognos software and you cannot copy the user's account information.

You can only work with profiles of users who have logged in at least once. When users log on, a date is displayed in the **Modified** column and the user name changes into a link.

Before you begin

To copy user profiles, you must have write permissions for the namespaces for both the source and target users.

Tip: When you copy a user profile, trusted credentials are not copied.

Procedure

1. In **IBM Cognos Administration**, on the **Security** tab, click **Users, Groups, and Roles**.
2. Click the namespace that contains the source user (the user you want to copy from).

   Tip: You can select only the namespaces that you have write access to.
3. Find the source user.
4. In the **Actions** column for the source user, click **More**.
5. In the **Perform an action** page, click **Copy this user's profile**.
6. In the **Copy the user profile** page, click **Select the target user** and navigate to find the target user.

7. After you have selected the target user, in the **Copy the user profile** page, select one or more of the following profile settings that you want to copy: **Preferences**, **Portal tabs and personal folders content**, or **Personal folders content**.
8. If required, select the **Delete the source user's profile after the copy completes** check box.
9. Click **Copy**.

Chapter 22. Multitenant environments

Multitenant environments consist of multiple customers or organizations, called tenants. Multitenancy is the capabililty of an application to support multiple tenants from a single deployment. It ensures that within each tenant users can access only the data that they are authorized to use. Multitenancy can reduce the application maintenance costs.

IBM Cognos Analytics provides built-in multitenancy capabilities. Existing deployments can be incrementally migrated to implement multitenant capabilities. The existing deployments that do not use multitenant capabilities are not affected if multitenancy is enabled.

All Content Manager objects can have a single, optional tenant ID. All Cognos users, including administrators, can have an optional tenant ID. Cognos users cannot, regardless of the Cognos Analytics security policies, access a Content Manager object if they do not have a tenant ID that matches the Content Manager object tenant ID. Content Manager objects that do not have a tenant ID are considered public and can be accessed by any user. Users who do not have a tenant ID can access only public objects.

Tip: The tenant ID value is a simple string. There is no restriction on the length of the tenant ID; however, it should not exceed 255 characters, the limit on the tenantID column in the database schema.

The following diagram shows an example how the Cognos Analytics multitenancy capabilities isolate access to objects in your content store. Users can access only the objects that they are authorized to access within each tenant grouping.

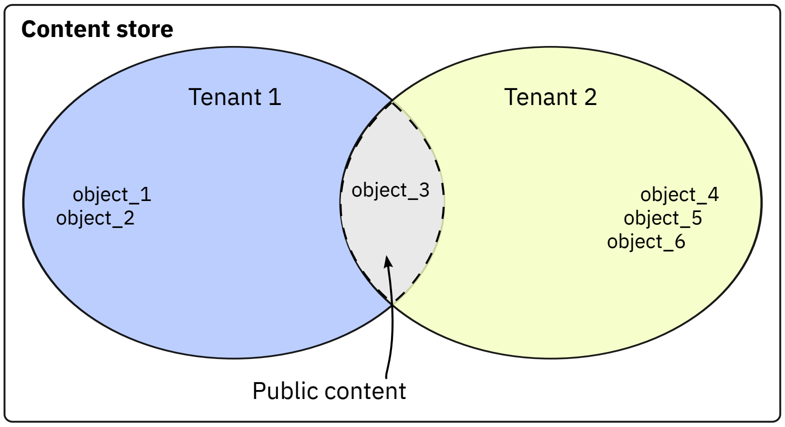


Figure 13. Content store configured to use the Cognos Analytics multitenancy capabilities

In this example, the users have access to the following objects:

- Users that belong to Tenant 1 can access object_1, object_2, and object_3.
- Users that belong to Tenant 2 can access object_3, object_4, object_5, and object_6.

Tip: The system administrator can access all objects in the content store.

When accessing objects, object tenancy is evaluated before object access permissions. Therefore, users in a multitenant application see only the objects that are associated with their tenant and objects that are categorized as public.

After multitenancy is enabled, you can record tenant activities using an audit logging database. IBM Cognos Analytics provides sample audit reports that show how to use the tenancy information to monitor certain user activities. For information about how to use IBM Cognos Configuration to set up a logging database, see the *IBM Cognos Analytics Installation and Configuration Guide*. For information about setting up the sample audit reports, see https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.ig_smples.doc/c_sampleauditreports.html#SampleAuditReports.

Configuring multitenancy

To configure multitenancy in your IBM Cognos Analytics installation, you need to specify the multitenancy properties in IBM Cognos Configuration.

The values for the multitenancy properties are different for each environment and depend on how you map the tenancy information to individual users in your environment.

Important: You should not need to modify anything in your authentication provider to configure multitenancy.

Before you configure multitenancy in IBM Cognos Configuration, you must decide how to map the user account in your authentication provider to the tenant. You can use for this purpose the position of a user within the hierarchy in your authentication provider or the user account properties in your authentication provider. You can also implement a custom tenant provider. For the last option, you must use the IBM Cognos Software Development Kit. Choosing the best implementation method for your environment requires careful planning and knowledge of your authentication provider.

Depending on how you decide to map the user account to the tenant, choose one of the following methods to configure multitenency.

- "Configuring multitenancy that is based on a hierarchy node" on page 300
- "Configuring multitenancy that is based on a user account attribute" on page 301
- "Configuring multitenancy that is based on a custom tenant provider" on page 302

You can configure multitenancy globally, at the **Authentication** level in IBM Cognos Configuration, or for specific namespaces. Multitenancy properties for a specific namespace override any multitenancy properties that are set globally.

Configuring multitenancy that is based on a hierarchy node

You can reuse the node structure information within a hierarchy of your authentication provider when configuring your tenant.

You need to map the hierarchy information to the **Tenant ID Mapping** > **Pattern** property in IBM Cognos Configuration.

Before you begin

You can use the `ancestors` user account attribute for this purpose. The `ancestors` attribute represents the hierarchical path to a user account in the form of an array. The following table shows how you might map the ancestors attribute to a hierarchy to identify the tenancy information:

Table 75. Ancestors attribute mapped to the hierarchy information

Ancestors information	Hierarchy	LDAP example
`ancestors[0]`	Directory node	
`ancestors[1]`	Namespace ID	`base DN`
`ancestors[2]`	Tenant grouping, such as a folder	`organizational units`

For example, if users are stored in an LDAP directory and tenants are directly under the base Distinguished Name (DN) as organizational units, you can set the **Pattern** type to the following value: `~/ancestors[2]/defaultName`.

In addition to `defaultName`, the following `ancestors` qualifiers can return tenancy information:

- `name/locale`

The locale parameter in this example is based on the mapping in the namespace configuration. If no locale is given, the name is the title of the object. For example, you might specify: `~/ancestors[2]/name/EN-ca`

- `searchPath/objectID`

  For example, you might specify: `~/ancestors[2]/searchPath/objectId`

Procedure

1. Open IBM Cognos Configuration.
2. Choose whether to configure multitenancy settings globally for all namespaces, or for a specific namespace.
   - To configure multitenancy for all namespaces, in the Explorer window, for the **Security** category, click **Authentication**.
   - To configure multitenancy for one namespace, in the Explorer window, for the **Security** category, click **Authentication**. Then, click the namespace that you want to configure.
3. In the **Multitenancy** group of properties, click the edit button for the **Tenant ID Mapping** property.
4. In the **Tenant ID Mapping** window that is displayed, specify your mapping in the following way:
   a) For **Type**, select **Pattern**.
   b) For **Value**, type the string that you created based on the instructions earlier in this topic. For example, you could specify the following value: `~/ancestors[2]/defaultName`.
   c) Click **OK**.
5. For an Active Directory namespace only, click in the **Value** column for **Custom properties** and click the edit button. Add the `MultiDomainTree` property and set its value to `true`.
6. Test your multitenancy configuration.
   a) Right-click either **Authentication** or the namespace (depending on your choice in step 2), and click **Test**.
   b) Log on using the credentials of the system administrator, and click **OK**.
   c) Click the **Details** button, and read the information that is displayed.

   If multitenancy is properly configured, your tenant ID is displayed in the details. If the tenant ID is not displayed, update and correct the values and test again.
7. If the testing was successful, from the **File** menu, click **Save**.
8. Restart the IBM Cognos service for the changes to take effect.

Configuring multitenancy that is based on a user account attribute

You can designate a specific user account attribute in your authentication provider to map to the tenant. After you choose the user account attribute that you want to map to the tenant, you must create a custom property and map it to that attribute.

You need to map the user account attribute to the **Tenant ID Mapping** > **Pattern** property in IBM Cognos Configuration.

Before you begin

The user account attribute that you choose to identify the user's tenant should be used only for this purpose.

For example, you can decide that the `businessUnit` attribute of an LDAP user account will identify the user's tenant. In this case, you set the **Pattern** type property as shown in the following example: `~/parameters/parameter_name`. Next, you specify a custom property named `parameter_name` and associate this property with the user account attribute `businessUnit`

Procedure

1. Open IBM Cognos Configuration.
2. Choose whether to configure multitenancy settings globally for all namespaces, or for a specific namespace.
   - To configure multitenancy for all namespaces, in the Explorer window, for the **Security** category, click **Authentication**.
   - To configure multitenancy for one namespace, in the Explorer window, for the **Security** category, click **Authentication**. Then, click the namespace that you want to configure.
3. In the **Multitenancy** group of properties, click the edit button for the **Tenant ID Mapping** property.
4. In the **Tenant ID Mapping** box that is displayed, specify your mapping in the following way:
   a) For **Type**, select **Pattern**.
   b) For **Value**, type the string that you created that is based on the instructions earlier in this topic.

      For example, type `~/parameters/`*`parameter_name`*, where `~/parameters` is a constant part of the syntax and *parameter_name* is the custom property name.

   c) Click **OK**.
5. In the **Account Mappings (Advanced)** group of properties, specify the custom property and map it to the account attribute in the following way:
   a) Click in the **Value** column for **Custom properties**, and click the edit button.
   b) In the **Value - Custom properties** window, click **Add**.
   c) In the **Name** column, type the custom property name. In the **Value** column, type the name of the attribute. For the example that is used in step 4, the custom property should be: `parameter_name` for **Name** and `businessUnit` for **Value**.
   d) Click **OK**.
6. Test your multitenancy configuration.
   a) Right-click either **Authentication** or the namespace (depending on your choice in step 2) and click **Test**.
   b) Log on using the credentials of the system administrator, and click **OK**.
   c) Click the **Details** button, and read the information that is displayed.

   If multitenancy is properly configured, your tenant ID is displayed in the details. If the tenant ID is not displayed, update and correct the values and test again.
7. If the testing was successful, from the **File** menu, click **Save**.
8. Restart the IBM Cognos service for the changes to take effect.

Configuring multitenancy that is based on a custom tenant provider

You can create a custom Java class and reference it when configuring multitenancy. You can use this method when you need to join data from multiple authentication providers, or from an authentication provider and a relational database. You must use the IBM Cognos Software Development Kit for this method.

When using this method, you map the **Tenant ID Mapping** > **Provider Class** property in IBM Cognos Configuration to a custom Java class.

Before you begin

Before you can configure multitenancy by using this method, you must perform the following tasks:

- Compile any required custom Java class files into JAR files and either place the files into the *`install_location`*`/webapps/p2pd/WEB-INF/lib` directory with any associated files, or update the CLASSPATH environment variable to include the path to these files.

- Implement the `ITenantProvider` interface by using the IBM Cognos Custom Authentication Provider and define the custom Java class in that interface. For example, the custom Java class name can be `com.`*`example`*`.`*`class`*. For more information, see the *IBM Cognos Software Development Kit Custom Authentication Provider Developer Guide*.

  Tip: IBM Cognos Custom Authentication Provider includes a sample custom Java class that you can use. You can find the sample files in the *`install_location`*`\sdk\java\AuthenticationProvider\MultiTenancyTenantProviderSample` directory.

Procedure

1. Open IBM Cognos Configuration.
2. Choose whether to configure multitenancy settings globally for all namespaces, or for a specific namespace.
   - To configure multitenancy for all namespaces, in the Explorer window, for the **Security** category, click **Authentication**.
   - To configure multitenancy for one namespace, in the Explorer window, for the **Security** category, click **Authentication**. Then, click the namespace that you want to configure.
3. In the **Multitenancy** group of properties, click the edit button for the **Tenant ID Mapping** property.
4. In the **Tenant ID Mapping** window that is displayed, specify your mapping in the following way:
   a) For **Type**, select **Provider Class**.
   b) For **Value**, type the name of the custom Java class that is defined in the `IBoundingSetProvider` interface that was implemented using the IBM Cognos Custom Authentication Provider. For example, type `com.`*`example`*`.`*`class_name`*.
   c) Click **OK**.
5. If you need to specify any custom property, in the **Account Mappings (Advanced)** group of properties, click the edit button in the **Value** column of the **Custom property**, and add the property name and value as required.
6. Test your multitenancy configuration.
   a) Right-click either **Authentication** or the namespace (depending on your choice in step 2) and click **Test**.
   b) Log on using the credentials of the system administrator, and click **OK**.
   c) Click the **Details** button, and read the information that is displayed.

   If multitenancy is properly configured, your tenant ID is displayed in the details. If the tenant ID is not displayed, update and correct the values and test again.
7. If the testing was successful, from the **File** menu, click **Save**.
8. Restart the IBM Cognos service for the changes to take effect.

Advanced multitenancy features

The advanced multitenancy features can be used to set up delegated tenant administration and content sharing among tenants.

A Cognos user can have a single tenant ID that is associated with the **Tenant ID Mapping** property. If the **Tenant ID Mapping** property is defined, additional tenant IDs can be assigned to a Cognos user by using the **Tenant Bounding Set Mapping** property.

Content Manager objects can have a virtual tenant ID, which can contain multiple tenant IDs, assigned as their tenant ID. This allows users from multiple tenants to access common content, such as folders or reports.

Virtual tenant IDs for Content Manager objects and multiple tenant IDs that are implemented for users by using the **Tenant ID Mapping** and **Tenant Bounding Set Mapping** properties can be used at the same time. These features can be used to allow Tenant Administrators to administer multiple tenants, which is referred to as delegated tenant administration; or Cognos users to access Content Manager objects for multiple tenants, which is referred to as content sharing among tenants.

When delegated tenant administration is implemented, the system administrator can delegate certain tasks, such as administration of security, schedules, activities, and events for some tenants to members of the **Tenant Administrators** role. The tenant administrators can administer a set of tenants, as defined by the tenant administrator's bounding set, in addition to their own tenant. The system administrator retains full control over the permissions of the tenant administrators. For more information, see "Delegated tenant administration" on page 310.

When content sharing among tenants is implemented, users can access content from different tenants, in addition to the users' own tenant content. Content sharing for users can be achieved by using the following multitenancy features:

- The **Tenant Bounding Set Mapping** property.

  A user can access any Content Manager object whose tenant ID is included in the user's tenant bounding set.
- Virtual tenant IDs

  A Content Manager object that has the virtual tenant ID assigned can be accessed by users from any tenant whose tenant ID is included in the object virtual tenant ID.

For more information, see the topic "Setting up virtual tenants to enable content sharing among tenants " on page 311.

Configuring the Tenant Bounding Set Mapping property

The tenant bounding set is a multi-value property that can include multiple tenant IDs.

You configure this property in IBM Cognos Configuration by using one of the following methods:

- "Configuring the tenant bounding set that is based on a user account attribute" on page 304
- "Configuring the tenant bounding set that is based on a custom provider" on page 305

Disabled tenants are present in the bounding set if the user is a system administrator. Deleted tenants are automatically removed from the bounding set.

You can apply this setting globally, to all configured namespaces, or to individual namespaces. Multitenancy properties for a specific namespace override any multitenancy properties that are set globally, at the **Authentication** level in IBM Cognos Configuration.

Tip: The **Tenant ID Mapping** and **Tenant Bounding Set Mapping** properties can have independent implementations. For example, you can use the position of a user within a hierarchy to determine the **Tenant ID Mapping** property and use a custom provider to determine the **Tenant Bounding Set Mapping** property. However, in most implementations both properties should contain tenant IDs of the same type, for example, department number.

Configuring the tenant bounding set that is based on a user account attribute

You can designate a specific user account attribute in your authentication provider to map to the tenant bounding set. Multitenancy must already be enabled.

You need to map the user account attribute to the **Tenant Bounding Set Mapping** > **Pattern** property in IBM Cognos Configuration.

Before you begin

After you choose, in your authentication provider, a user account attribute that you want to map to the tenant bounding set, you must create a custom property and map it to the user account attribute.

You can use the `departmentNumber` attribute of an LDAP user account to identify the user's bounding set. In this case, you can set the **Tenant Bounding Set Mapping**, **Pattern** property as shown in the following example: `~/parameters/bounding_set`. Next, you specify a custom property named `bounding_set` and associate this property with the user account attribute `departmentNumber`

Procedure

1. Open IBM Cognos Configuration.
2. Choose whether to configure this setting globally for all namespaces, or for a specific namespace.
   - To configure this setting for all namespaces, in the Explorer window, for the **Security** category, click **Authentication**.
   - To configure this setting for one namespace, in the Explorer window, for the **Security** category, click **Authentication**. Then, click the namespace that you want to configure.
3. In the **Multitenancy** group of properties, click the edit button for the **Tenant Bounding Set Mapping** property.
4. In the **Tenant Bounding Set Mapping Mapping** box that is displayed, specify your mapping in the following way:
   a) For **Type**, select **Pattern**.
   b) For **Value**, type the string that you created that is based on the instructions earlier in this topic.

      For example, type `~/parameters/`*`boundingSet`*, where `~/parameters` is a constant part of the syntax, and *boundingSet* is the custom property name.
   c) Click **OK**.
5. In the **Account Mappings (Advanced)** group of properties, specify the custom property and map it to the account attribute in the following way:
   a) Click in the **Value** column for **Custom properties**, and click the edit button.
   b) In the **Value - Custom properties** window, click **Add**.
   c) In the **Name** column, type the custom property name. In the **Value** column, type the name of the attribute. For the example that is used in step 4, the custom property should be: `boundingSet` for **Name** and `departmentNumber` for **Value**.
   d) Click **OK**.
6. Test your multitenancy configuration.
   a) Right-click either **Authentication** or the namespace (depending on your choice in step 2) and click **Test**.
   b) Log on using the credentials of the system administrator, and click **OK**.
   c) Click the **Details** button and read the information that is displayed.

   If this setting is properly configured, the **Tenant bounding set** property value is displayed in the details. If this setting is not displayed, ensure that the value is correct and test again.
7. If the testing was successful, from the **File** menu, click **Save**.
8. Restart the IBM Cognos service for the changes to take effect.

Configuring the tenant bounding set that is based on a custom provider

You can create a custom Java class that is started during the user authentication process to determine the tenant bounding set. You must use the IBM Cognos Software Development Kit for this method.

When using this method, you must map the **Tenant Bounding Set Mapping** > **Provider Class** property in IBM Cognos Configuration to a custom Java class.

Before you begin

Before you can configure the tenant bounding set by using this method, you must perform the following tasks:

- Compile any required custom Java class files into JAR files, and either place the files into the `*install_location*/webapps/p2pd/WEB-INF/lib` directory with any associated files, or update the CLASSPATH environment variable to include the path to these files.
- Implement the `IBoundingSetProvider` interface by using the IBM Cognos Custom Authentication Provider. In this interface, define a custom Java class that you can later use when you configure the **Tenant Bounding Set Mapping** > **Provider Class** property. For example, the name can be `com.*example*.*class*`. For more information, see the *IBM Cognos Software Development Kit Custom Authentication Provider Developer Guide*.

Procedure

1. Open IBM Cognos Configuration.
2. Choose whether to configure this setting globally for all namespaces, or for a specific namespace.
   - To configure this setting for all namespaces, in the Explorer window, for the **Security** category, click **Authentication**.
   - To configure this setting for one namespace, in the Explorer window, for the **Security** category, click **Authentication**. Then, click the namespace that you want to configure.
3. In the **Multitenancy** group of properties, click the edit button for the **Tenant ID Mapping** property.
4. In the **Tenant Bounding Set Mapping** box that is displayed, specify your mapping in the following way:
   a) For **Type**, select **Provider Class**.
   b) For **Value**, type the Java class name that you defined in the `IBoundingSetProvider` interface by using the IBM Cognos Custom Authentication Provider.

      For example, type `~/parameters/*boundingSet*`, where `~/parameters` is a constant part of the syntax and *boundingSet* is the custom property name.

   c) Click **OK**.
5. If you need to specify any custom property, in the **Account Mappings (Advanced)** group of properties, perform the following actions:
   a) Click in the **Value** column for **Custom properties**, and click the edit button.
   b) In the **Value - Custom properties** window, click **Add**.
   c) Specify the property **Name** and **Value** as required.
   d) Click **OK**.
6. Test your multitenancy configuration.
   a) Right-click either **Authentication** or the namespace (depending on your choice in step 2) and click **Test**.
   b) Log on using the credentials of the system administrator, and click **OK**.
   c) Click the **Details** button and read the information that is displayed.

   If this setting is properly configured, the **Tenant bounding set** is displayed in the details. If this setting is not displayed, ensure that the value is correct and test again.
7. If the testing was successful, from the **File** menu, click **Save**.
8. Restart the IBM Cognos service for the changes to take effect.

Disabling multitenancy

To disable multitenancy, you must remove the multitenancy authentication properties on all Content Manager computers where they were configured.

All tenant IDs must be removed from all objects in the content store. If all tenant IDs are not removed after disabling multitenancy, the application behavior might be unpredictable.

Procedure

1. Open IBM Cognos Configuration.
2. Choose whether to disable multitenancy settings globally for all namespaces, or for a specific namespace.
   - To disable multitenancy for all namespaces, in the Explorer window, for the **Security** category, click **Authentication**.
   - To disable multitenancy for one namespace, in the Explorer window, for the **Security** category, click **Authentication**. Then, click the namespace that you want to configure.
3. Under **Multitenancy**, click the edit button for the **Tenant ID Mapping** property.

   The **Tenant ID Mapping** box is displayed.
4. Delete the values for the **Pattern** or the **Provider class** property.

   If custom properties were specified for the namespace, you must delete them as well.
5. Test your configuration to verify if multitenancy properties are deleted.

   a) Right-click either **Authentication** or the namespace (depending on your choice in step 2) and click **Test**.

   b) Log on using the credentials of the system administrator, and click **OK**.

   c) Click the **Details** button and read the information that is displayed.

   The tenant ID should not be displayed.
6. From the **File** menu, click **Save**.
7. Restart the IBM Cognos service.

What to do next

After multitenancy is disabled, the system administrator must review and update the policies on objects and then update the tenancy to public.

Tenant administration

Tenant administration tasks are performed by system administrators and delegated tenant administrators.

System administrators must be members of the **System Administrators** role in the **Cognos** namespace. System administrators can view and modify all objects in the content store. They can also delegate tenant administration tasks to other administrators who are members of the **Tenant Administrators** role in the **Cognos** namespace.

Members of the **System Administrators** role can perform the following tasks in a multitenant IBM Cognos Analytics environment:

- Create, change, and delete tenant objects.
- Change tenancy properties on any object in the content store.
- Move tenants.
- Terminate sessions for tenants.

The **Multitenancy** tab in **Manage** is the central area for tenant administration. On this tab, the administrator can add new tenants, and manage all tenants that are registered in the current Cognos Analytics environment. Only members of the **System Administrators** role can access the **Multitenancy** tab.

Tip: The **Multitenancy** tab in IBM Cognos Administration can also be used for tenant administration.

Containment rules for multitenancy

Multiple tenants can co-exist in a single content store. The tenant containment rules ensure security and isolation between tenants. These rules dictate how the content is created and where it can be located.

Every object in the content store has a tenant ID value that indicates which tenant the object belongs to. For information about creating tenant IDs, see “Creating tenants” on page 308.

The tenant ID of an object must be the same as the tenant ID of its parent, unless the parent tenant ID is public. If the parent tenant ID is public, the tenant ID for the child can be changed to any value. For more information, see “Setting a tenant ID for a public object” on page 309.

If the current logged-in user creates an object, the object tenant ID is the same as the user's tenant ID.

Model and modelView objects inherit their tenant ID from the package. For example, models published to a public package are always public.

System administrators can run a content store consistency check to detect instances of violation of the tenant containment rules. For more information, see “Creating and running a content store consistency check ” on page 319.

Creating tenants

System administrators must create and enable the tenant object before the tenant users can access IBM Cognos Analytics.

Before you begin

Multitenancy must already be enabled in IBM Cognos Configuration.

About this task

The system administrator creates the tenant object in the Cognos Analytics **Manage** component, on the **Multitenancy** tab, and assigns a unique tenant ID to the object.

The tenant IDs are defined in the authentication provider, such as LDAP, Active Directory, or a custom authentication provider. For more information, see Configuring multitenancy.

Procedure

1. In **Manage**, select the **Multitenancy** tab.
2. Select the **Add a tenant** ⊕ icon.
3. Specify the **Name** and **Tenant ID** parameters.

   Ensure that you specify a valid tenant ID that was preconfigured in the authentication provider.

   Other parameters on this page are optional.
4. Select **Add**.

Results

The tenant name is displayed on the **Multitenancy** tab. By default, the tenant is disabled ⊘. You can enable the tenant after it is fully configured.

Assigning tenant IDs to existing content

After multitenancy is enabled, the system administrator assigns tenant IDs to the existing content store objects. All objects that belong to a tenant have the same tenant ID.

When a user from a specific tenant logs on to IBM Cognos Analytics, or the system administrator impersonates the tenant,the system looks at the tenant ID and filters the content.

Tenants can be created and tenant IDs can be assigned using the software development kit (SDK).

About this task

In a multitenant environment, all objects in the content store are either public or belong to a single tenant. As a system administrator, you must ensure that the existing objects have a proper tenant ID or are meant to remain public. For example, you can assign tenant IDs to content within a folder, but leave the folder itself public.

If the tenant content is not organized into separate folders, you can create a root folder for each tenant. This helps to preserve the uniqueness of names in the Cognos Analytics environment.

You can also assign tenant IDs for individual objects, such as reports, dashboards, data server connections, user groups and roles, and so on.

Procedure

1. Log on to IBM Cognos Analytics as a system administrator.
2. In **Team Content**, locate the container entries, such as folders or packages, whose descendents should be assigned the same tenant ID.

   When assigning tenant IDs for objects such as data server connections or groups or roles, locate the objects in the appropriate area in the administration interface.
3. Open the **Properties** panel for the object for which you want to assign the tenant ID.
4. On the **General** tab, **Advanced** section, click the link next to **Tenant**.
5. Choose a tenant ID from the list of available IDs, and click **Apply**.

Results

The tenant ID is applied to the entry. If the entry is a container, such as a folder or package, the tenant ID is applied to the entry and its descendents.

The tenant name is displayed on the **General** tab, **Advanced** section, in the object properties page.

Setting a tenant ID for a public object

You can assign a tenant ID for objects whose parent is public.

Procedure

1. Open the **Properties** panel for the object, such as a data server connection, for which you want to specify the tenant ID.
2. On the **General** tab, **Advanced** section, select the link next to **Tenant**.
3. Choose a tenant ID from the list of available IDs.
4. Click **Apply.**

Impersonating a tenant

As a system administrator or a tenant administrator, you can impersonate a single tenant to view and interact with the content from the tenant perspective. When impersonating a tenant, you can perform all tasks that this tenant is allowed to perform and remain logged on to the system.

System administrators can impersonate all tenants that are defined in the content store. Tenant administrators can impersonate only those tenants that they are allowed to administer.

Procedure

1. Log on to IBM Cognos Analytics as a system administrator or a tenant administrator. For more information, see "Tenant administration" on page 307.
2. In the main header, click the **Impersonate Tenant** icon.

   Tip: In **IBM Cognos Administration**, system administrators can also start impersonating tenants from the **Multitenancy** tab. From the **Actions** drop-down menu for any tenant, click **Impersonate**.

   The **Tenant Impersonation** header is displayed.
3. In the tenant selection box, click the drop-down icon, and select the tenant that you want to impersonate.

   The tenant name is displayed in the selection box. If the **Show tenant's content only** check box is selected (default), system administrators or tenant administrators can see only the content associated with the selected tenant. If the **Show tenant's content only** check box is cleared, system administrators can see the content for all tenants in the content store, and tenant administrators can see content for all tenants that they can administer.
4. Perform the tasks that you planned to perform for the selected tenant.

   If you want to modify or create content for another tenant, select that tenant in the selection box.
5. Click the **Close** icon in the **Tenant Impersonation** header to finish the tenant impersonation session.

Delegated tenant administration

System administrators can delegate tenant administration tasks to members of the **Tenant Administrators** role.

If the **Tenant Bounding Set Mapping** property is configured, **Tenant Administrators** can access only tenants that are defined in their bounding set. They are further restricted by the Cognos Analytics security policies assigned to the content by system administrators. In this situation, **Tenant Administrators** are considered bounded tenant administrators.

If the **Tenant Bounding Set Mapping** property is not configured, **Tenant Administrators** bypass tenancy checking and are restricted only by the Cognos Analytics security policies assigned to the content by system administrators. In this situation, **Tenant Administrators** are considered unbounded tenant administrators.

For more information about the **Tenant Bounding Set Mapping** property, see information about advanced multitenancy features in the *IBM Cognos Analytics Administration and Security Guide*.

Tenant Administrators can perform the tenant administration tasks that the system administrator assigns to them.

Tenant Administrators cannot perform the following tasks:

- Access the **Multitenancy** tab in **Manage** and in IBM Cognos Administration.
- Create, delete, deploy, and disable tenants.
- Manage tenant user profilesTerminate user sessions and customize tenants.

- Change tenancy on objects in the content store.
- Perform server administration tasks, such as tuning, and running content store utilization tasks and consistency checks.

Tip: The **Tenant Administrators** role is one of the built-in entries in the " Cognos Namespace" on page 163 .

For information about the role of **System Administrators** in a multitenant environment, see "Tenant administration" on page 307.

Setting up the Tenant Administrators role

In the initial content store, the **Tenant Administrators** role has no members and only **System Administrators** have access permissions for this role. System administrators must add members and modify the initial access permissions for this role to use it for delegated tenant administration.

About this task

When you add members to the **Tenant Administrators** role, choose the users, groups, or roles from the appropriate tenants.

Procedure

Use the following procedure to add or remove members of the **Tenant Administrators** role.

1. Log on to IBM Cognos Analytics as a system administrator who is a member of the **System Administrators** role.
2. In **Manage** > **Accounts** > **Namespaces**, select the **Cognos** namespace.
3. In the list of entries, locate the **Tenant Administrators** role, and from its context menu ⋮, click **View members**.
4. On the **Members** tab, select the add member ⊕ icon, and browse through the hierarchy of your security namespace to select the users, groups or roles that you want to be members of this role.

Results

After you add the appropriate users, groups, or roles to the **Tenant Administrators** role, you can use this role to set up security policies and capabilities for objects in the content store.

For information on setting access permissions, see "Set access permissions for an entry" on page 179. For information on setting capabilities, see Chapter 13, "Capabilities," on page 185.

Setting up virtual tenants to enable content sharing among tenants

When you set up virtual tenants, objects in the content store can be accessed by users who belong to different tenants.

Virtual tenants include real tenants that are already configured in Cognos Analytics.

Before you begin

Multitenancy is enabled for IBM Cognos Analytics and the tenants are created in **Manage** > **Multitenancy**. For more information, see "Creating tenants" on page 308.

About this task

When viewed on the **Multitenancy** tab, the entries for virtual tenants and real tenants look identical. To make it easier to identify virtual tenants, use meaningful names when creating them and specify descriptions.

For example, you want to configure content sharing for tenants named North America, Central America, and South America. You create a virtual tenant named Americas and add the three tenants to this tenant. Users who belong to any of the three tenants can access content of their own tenant, content of the other two tenants, and public content.

If you delete a virtual tenant, all content that is associated with that tenant is also deleted.

For more information, see Advanced multitenancy features (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.ug_cra.doc/c_config_mt_advanced.html).

Procedure

Perform the following steps to create a virtual tenant and a folder for the virtual tenant content.

1. Log on to IBM Cognos Analytics as a member of the **System Administrators** role.
2. In **Manage**, select the **Multitenancy** tab.
3. Select the **Add a tenant** ⊕ icon.
4. Specify the **Name** and **Tenant ID** parameters.

   The virtual tenant ID does not need to be preconfigured. It can be any value.

   For a description, type a string, such as `Virtual tenant`, that will help you to identify the tenant among other tenants in Cognos Analytics.
5. Select **Add**.

   The virtual tenant name is displayed in the list of tenants, and the tenant is disabled by default. You can enable the tenant after you finish configuring it.
6. For the virtual tenant that you created, from its context menu ⋮, select **View members**.
7. On the **Members** tab, select the add member ⊕ icon.
8. Select the tenants that you want to add to the virtual tenant, and click **Add**.

   Tip: You can add disabled tenants. However, users cannot access content of the disabled tenants until the tenants are enabled.
9. Create a new folder. The folder name should be similar to the virtual tenant name for easier identification.
10. In the folder properties page, on the **General** tab, **Advanced** section, change the **Tenant ID** value to the tenant ID of the virtual tenant by selecting the ID from the list of available IDs. For example, if your virtual tenant ID is `Americas`, select this ID from the list and assign it to the folder.

Displaying the tenant name in Cognos Analytics user interface

You can specify whether users without administrative permissions can view the tenant name in the Cognos Analytics user interface.

By default, only system administrators and tenant administrators can see the tenant name associated with objects. If you want to allow the non-administrative users to have the same privilege, change the advanced setting **portal.showTenantInfoForAllUsers** for the presentation service to true.

Procedure

1. Follow the steps in the section "Configuring advanced settings for specific services" on page 464.
2. For the presentation service, specify the **portal.showTenantInfoForAllUsers** property and set its value to true.

Managing tenant user profiles

Each tenant can have its own default user profile that is shared by all tenant users.

About this task

The system administrator creates the tenant user profile. This profile is based on the default user profile that is defined in the **Cognos** namespace. The default user profile can be changed to be relevant to the tenant. For example, the profile can reflect the product language, portal tabs, and the style of the IBM Cognos user interface associated with the tenant.

When a tenant user logs on to IBM Cognos software for the first time, the user profile is automatically created for the user. The profile is based on the tenant user profile, if one exists. If a tenant profile does not exist, the default user profile is applied to the user.

System administrators can modify or delete the tenant user profile. The profile can also be deployed with other tenant objects from the source environment to the target environment. When deploying the tenant, the same conflict resolution rules apply to tenant user profiles as to other tenant objects.

For more information about user profiles in IBM Cognos Analytics, see Chapter 21, “Managing User Profiles,” on page 295.

Procedure

1. In **IBM Cognos Administration**, click the **Multitenancy** tab.
2. Choose the applicable action:
   - To create the user profile for one or more tenants, select the tenant check boxes, and click the **Edit default user profile** icon in the toolbar. If required, make changes on the different tabs.
   - To change an existing user profile for one tenant, from the tenant **Actions** drop-down menu, click **Edit tenant user profile**, and make the required changes on the different tabs.
   - To delete the user profile for one or more tenants, select the tenant check boxes, and click the **Delete tenant user profile** icon in the toolbar. To delete the user profile for one tenant, from the tenant **Actions** drop-down menu, click **Delete tenant user profile**.

Tenant content deployment

You can export and import the tenant content.

Tenant content can be deployed alone or with the public content. Public content can also be deployed by itself.

For general information about deployment in IBM Cognos Analytics, see Chapter 19, “Deployment,” on page 267.

Exporting tenant content to a deployment archive

You can export the tenant content from the source environment to a deployment archive. Later, you can import the archive into the target environment.

Before you begin

Only public content and objects belonging to the selected tenants are exported. Before you start an export, you must complete the assignment of tenancy to objects in the content store.

About this task

You can export the content in the following way:

- Content that belongs to the selected tenants and public content

- Content that belongs to the selected tenants only.
- Public content only

User account information, including public user accounts, can be included or excluded from the export. When exporting tenants with public content included, the public user account information is also included by default. If you want to exclude the public account information from this type of export, use the **`CM.TENANTS_DEPLOYMENT_EXCLUDE_PUBLIC_USER_ACCOUNTS`** advanced setting. For more information, see "Excluding public user account information when deploying public content " on page 316.

When public content is excluded from the tenant export, and a tenant object has public ancestors, the public ancestors are included in the export so that the content references can be preserved in the target system. For example, in a situation where a data source connection belongs to a tenant, but the data source itself is public, the data source is exported.

Procedure

1. In **IBM Cognos Administration**, click the **Multitenancy** tab.
2. Click the **New export** icon in the toolbar.

   The **New Export** wizard opens.
3. Type a unique name and an optional description and screen tip for the deployment specification. Select the folder where you want to save it and click **Next**.
4. In the **Choose a deployment method** page, select **Select tenants**. If applicable, select the **Include user account information** check box as well, and click **Next**.
5. In the **Select the tenants** page, perform the following steps:

   a) Using the arrow icons, move the applicable tenants from the **Available** box to the **Selected** box. Ensure that correct tenant names are in the **Selected** box.

      Important: When you export public content only, the **Selected** box must be empty.

   b) If you want to include public content in the export, select the **Include public content** check box.

   c) Choose one of the **Conflict resolution** options. These options are used when the deployment archive is imported into the target environment. The **Replace existing entries** option replaces objects in the target environment with objects in the deployment archive. The **Keep existing entries** option merges objects from the deployment archive with associated objects in the target environment.

   d) Click **Next**.
6. In the **Specify a deployment archive** page, under **Deployment archive**, select an existing deployment archive from the list, or type a new name to create one.

   If you are typing a new name for the deployment archive, do not use spaces in the name. If the name of the new deployment specification matches the name of an existing deployment archive, the characters _# are added to the end of the name, where # is a number such as 1.
7. Under **Encryption**, click **Set the encryption password**, type the password, and click **OK**.
8. Review the summary information and click **Next**.

   If you want to change the information, click **Back** and follow the instructions.
9. Decide what to do with the deployment specification:

   a) To run it now or later, click **Save and run once** and click **Finish**. Specify the time and date for the run. Then, click **Run**. Review the run time and click **OK**.

   b) To schedule it at a recurring time, click **Save and schedule** and click **Finish**. Then, select frequency and start and end dates. Then click **OK**.

      Tip: To temporarily disable the schedule, select the **Disable the schedule** check box.

   c) To save it without scheduling or running, click **Save only**, and then click **Finish**.

Results

The export deployment specification is saved in IBM Cognos Administration, on the **Configuration** tab, in **Content Administration**. From this location, you can update and run the deployment specification, and move the deployment archive to a different content store.

Importing tenant content to a target environment

The tenant content can be imported from the deployment archive into the target environment.

About this task

When you import from the deployment archive, you select from entries that were exported. If user account information was included with the public content, you can keep this information or exclude it.

When you import content, you can replace the content in the target environment with the content in the deployment archive.

The entire tenant content in the target environment is not replaced, but any content in the target environment that conflicts with the content in the archive is replaced.

Some entries in the target content store might contain references to public content that was excluded from the tenant deployment. If the public content is not already in the target content store, this results in broken references between the entries. Administrators are notified about the broken references through the deployment details. To repair the broken references, you can either deploy the public content separately or re-export the tenant content with the public content included.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Content Administration**.
2. On the toolbar, click the new import icon. The **New Import** wizard appears.
3. In the **Deployment archive** section, select the deployment archive that you want to import.
4. Type the password that was used to encrypt the archive, and click **OK**.
5. Type a unique name, an optional description, and a screen tip for the deployment specification, select the folder where you want to save it, and click **Next**.
6. Verify that the tenant ID is correct.
7. If user account information is included with the public content in the deployment archive, you can decide to include or exclude this information now by selecting or clearing the check box **Include user account information**. This selection is not available when user account information is not included in the archive.
8. Choose one of the **Conflict resolution** options. The **Replace existing entries** option replaces objects in the target environment with objects in the deployment archive. The **Keep existing entries** option merges objects from the deployment archive with associated objects in the target environment.
9. Click **Next**.
10. Review the summary information and click **Next**.
11. Decide what to do with the import deployment specification:

    - To run it now or later, click **Save and run once**, and click **Finish**. Specify the time and date for the run. Then click **Run**. Review the run time and click **OK**.
    - To schedule it at a recurring time, click **Save and schedule** and click **Finish**. Then, select frequency and start and end dates, and click **OK**.

      Tip: To temporarily disable the schedule, select the **Disable the schedule** check box. To view the schedule status, see "Managing scheduled activities" on page 259.
    - To save it without scheduling or running, click **Save only**, and click **Finish**.

When you run the import, you have the option of selecting to upgrade the report specification. If you choose not to upgrade the deployment specification at this time, you can upgrade it later. For more information, see “Upgrading report specifications” on page 286. You also have the option to select Store ID. Choose **Assign new IDs during import**.

12. When you run the import, you have the option of selecting to upgrade the report specification. If you choose not to upgrade the deployment specification at this time, you can upgrade it later. For more information, see “Upgrading report specifications” on page 286. You also have the option to select **Store IDs**. When you run an import, content store IDs are deleted and new IDs are assigned. If the content store IDs must be retained, you can choose to preserve them. For more information, see “Content ID assignment” on page 287.

Results

The import deployment specification is saved in IBM Cognos Administration, on the **Configuration** tab, in **Content Administration**. From this location, you can update and run the deployment specification.

Excluding public user account information when deploying public content

In IBM Cognos software version 10.2.0 there was no option to exclude user account information when public content was deployed. This option exists in the product starting with version 10.2.1.

About this task

When exporting tenants from Content Manager 10.2.0, before upgrading Content Manager to version 10.2.1, you might still have a large number of user accounts without tenant IDs. If you want to exclude those accounts from your deployment, use the **`CM.TENANTS_DEPLOYMENT_EXCLUDE_PUBLIC_USER_ACCOUNTS`** advanced setting.

Procedure

1. Follow the steps in the section “Configuring advanced settings for specific services” on page 464.
2. For the **ContentManagerService**, type the following parameter name: **`CM.TENANTS_DEPLOYMENT_EXCLUDE_PUBLIC_USER_ACCOUNTS`**.
3. Type **true** as value for this parameter, and click **OK**.

Terminating active user sessions for tenants

You must terminate the tenant active user sessions before deleting a tenant or before performing some tenant maintenance operations.

Before you begin

Before terminating its active user sessions, disable the tenant so that new user sessions cannot be started. For more information, see “Disabling and enabling tenants” on page 317.

About this task

Use this action to terminate all active user sessions for the specified tenants. Access for other tenants is not affected.

Procedure

1. In **Manage** > **Multitenancy**, locate the appropriate tenant.
2. From the tenant context menu ⋮, click **Terminate sessions**.

Results

A message that specifies the number of terminated user sessions is displayed.

Disabling and enabling tenants

You can disable a tenant when you want to prevent the tenant users from accessing IBM Cognos Analytics and modifying the tenant content.

About this task

By default, a newly-created tenant is disabled, and you need to enable it after it is configured.

You should disable a tenant before deploying the tenant and its content. For more information, see "Tenant content deployment" on page 313.

As a best practice, you should also disable a tenant before terminating its active user sessions. For more information, see "Terminating active user sessions for tenants " on page 316.

Procedure

1. In **Manage** > **Multitenancy**, locate the required tenant.
2. From the tenant context menu ⋮, click **Disable**.

   An icon that indicates the disabled state is added to the tenant icon .

   You can enable the tenant by selecting **Enable**.

Deleting tenants

You can delete a tenant from IBM Cognos Analytics. This might be needed if the tenant was permanently moved to a different instance of IBM Cognos Analytics.

Before you begin

Before deleting a tenant, you must terminate the tenant active user sessions. Otherwise, you will not be able to delete the tenant. For more information, see "Terminating active user sessions for tenants " on page 316.

About this task

When you delete a tenant, you also delete all content associated with the tenant, such as reports or dashboards.

Procedure

1. In **Manage** > **Multitenancy**, locate the tenant that you want to delete.
2. From the tenant context menu ⋮, click **Delete**.

Creating and running content store utilization tasks

Content store utilization tasks provide insight into the content store usage.

You can determine how many instances of each object type users from your tenants have in the content store and the amount of space that those instances are taking. You can also determine more detailed information, such as the size of every object.

About this task

This information can be used for billing and provisioning purposes. For example, billing decisions can be based on the instance count of particular object types, such as reports. Provisioning decisions can be made by determining which tenants should be moved to a different IBM Cognos instance because of the amount of space that they are using.

After content store utilization tasks are created, you can run them on demand, at a scheduled time, or based on a trigger. The resulting .csv files can be used as data sources to create reports in IBM Cognos Analytics.

Procedure

1. In **IBM Cognos Administration**, click the **Multitenancy** tab.
2. Click the create content utilization icon in the toolbar.
3. Specify the task name, and optionally a description and screen tip.
4. For the **Tenant** property, click **Set** to select the tenant ID that you want to be associated with this task.

   If you do not select the tenant at this point, the task will be created with the current session tenant ID.
5. Select the tenant or tenants that you want to include in this content utilization task by using the arrows icons to move the tenants from the **Available** box to the **Selected** box.
6. In the **Options** section, specify how to save the information to the log files after this task is run:

   - Under **File**, if you select **One for all tenants**, the information for all tenants is saved in a single file. If you select **One per tenant**, the information for each tenant is saved in a separate file.
   - Under **Granularity**, if you select **By object type and tenant**, a high-level summary of information about each tenant is saved. The summary includes an instance count and the total size of each object type in the content store grouped by tenant. If you select **All objects**, a detailed summary of information about each object in the content store is saved. The summary includes the object tenantID, name, storeID, parentStoreID, and size.
7. Choose how to run the task:

   - To run the task now or later, click **Save and run once**. Specify a time and date for the run, and click **Run**.
   - To schedule the task at a recurring time, click **Save and schedule**. Then, select the frequency, start and end dates, and click **OK**.

     Tip: To temporarily disable the schedule, select the **Disable the schedule** check box. To view the schedule status, see “Managing scheduled activities” on page 259.
   - To save the task without scheduling or running, click **Save only**.

Results

The new task appears on the **Configuration** tab, in **Content Administration**. You can modify or run the task later.

The log files that result from running the content store utilization tasks are saved in the `logs` directory that is specified in IBM Cognos Configuration with the following names:

- `cmUtilization_`*`date_stamp`*`.csv` when the **One for all tenants** option was used.
- `cmUtilization_`*`date_stamp_tenant_ID`*`.csv` when the **One per tenant** option was used.

Creating and running a content store consistency check

You can run a consistency check to detect instances of objects that violate the containment rules for multitenancy. Content that does not follow the tenant containment rules might not be accessible to the intended users or might not be deleted when the tenant that it belongs to is deleted.

The tenant containment rules require that the tenant ID of an object must be the same as the tenant ID of its parent, unless the parent tenant ID is public. For more information, see "Containment rules for multitenancy" on page 308.

Before you begin

Back up the content store before running a content store consistency check.

About this task

Instances where an object violates the tenant containment rules are resolved automatically if you use the **Find and fix** option when running the content store consistency check task. The tenant-related inconsistencies are fixed by assigning the parent tenant ID to the child object that is causing the error. You do not need to start the IBM Cognos service for these types of errors to be fixed. However, other types of content store inconsistencies are not fixed until the IBM Cognos service is started. A summary of each repair is created under the task execution history.

If you want to review and manually resolve the instances of tenant containment rules violation you can use the **Find only** option when running the content store consistency check. A summary of each error is created under the task execution history, assuming that the user who runs the task is a system administrator. This option might be safer because it gives you the time to investigate each object individually and assign the correct tenant ID to the object.

Procedure

1. In IBM Cognos Administration, on the **Configuration** tab, click **Content Administration**.
2. Click the new content maintenance icon in the toolbar, and then click **Consistency Check**.
3. Type the task name, and optionally a description and screen tip.
4. Click **Internal references** to check the content store for inconsistencies.
5. Choose how to run the task:
   - To run the task now or later, click **Save and run once**. Specify a time and date for the run. Click **Find only** or **Find and fix**, and then click **Run**. Review the run time and click **OK**.
   - To schedule the task at a recurring time, click **Save and schedule**. Select frequency and start and end dates. Click **Find only** or **Find and fix** and click **OK**.
   - To save the task without scheduling or running, click **Save only**.

Results

The new task appears on the **Configuration** tab, under **Content Administration**. You can modify or run the task later. For more information about using these types of tasks in an IBM Cognos environment, see "Content store maintenance tasks" on page 54.

Access to interactive activities in a multitenant environment

The content of interactive activities in IBM Cognos Analytics is not filtered by the tenant ID. Therefore, additional measures are required to restrict access to interactive activities for users.

The content of background activities is filtered by the tenant ID so all users can view these activities.

Background activities and interactive activities can be accessed in **My Activities and Schedules**. Administrators can see the activities on the **Status** tab in IBM Cognos Administration as well. For more information, see Chapter 17, "Managing scheduled activities," on page 225.

Restricting access to interactive activities for users

To avoid the risk of exposing the tenant content to unintended users, system administrators can restrict access to interactive activities.

About this task

Use the **`COGADMIN.restrictInteractiveActivitiesToSystemAdministrators`** advanced setting to restrict access to interactive activities for users so that only system administrators can view this type of activities.

Procedure

1. Follow the steps in the section "Configuring advanced settings for specific dispatchers" on page 464.
2. For the specified dispatcher, in the **Parameter** column, type the following name:**`COGADMIN.restrictInteractiveActivitiesToSystemAdministrators`**
3. Specify a value of `true` for this parameter, and click **OK**.
4. Restart the IBM Cognos service.

Results

Only system administrators can now view interactive activities in the IBM Cognos environment.

Hiding interactive activities of unknown users

Tenant administrators might not have permissions to view all users in the IBM Cognos environment. However, the administrators can still see interactive activities of all users because these types of activities are not filtered by the tenant ID.

About this task

The system administrator can hide interactive activities of users that the tenant administrator cannot see from his or her view.

Procedure

1. Follow the steps in the section "Configuring advanced settings for specific dispatchers" on page 464.
2. As the **Parameter** name, type the following name:**`COGADMIN.filterInteractiveActivitiesOfUnknownUsers`**
3. Specify a value of `true` for this parameter, and click **OK**.
4. Restart the IBM Cognos service.

Results

Tenant administrators can now view interactive activities of the specific tenant users only.

Chapter 23. Resource library

Administrators import, store, and manage reusable resources such as visualizations and user interface profiles, on the **Library** tab in IBM Cognos Administration.

The **Library** tab provides a central location for administering the resources.

To access and manage content on the **Library** tab, you must be a member of the **Library Administrators** role. For more information, see "Predefined roles" on page 202.

Administrators must import resources and set access permissions for the resources in the library. Users with the appropriate permissions can then use resources in IBM Cognos reports.

Administrators can also delete resources from the library.

Visualizations

Visualizations help report consumers to spot patterns and outliers and to understand data. Use IBM Cognos Analytics visualization tools to incorporate diverse types of visualizations and greater interactivity into the IBM Cognos reports.

Administrators must import visualizations from local systems and file shares into IBM Cognos Analytics.

A variety of ready-to-use, customizable visualizations is available from Custom visualizations used in the samples (https://community.ibm.com/community/user/businessanalytics/blogs/steven-macko/2016/10/06/ibm-cognos-analytics-custom-visualizations-used-in-the-samples). You can choose the visualizations that match your data and answer your business question, and download them to your file system or network shares. Then, use the **Library** tab to import the visualizations into the library and make them available to the report authors.

Visualizations are included in a full content store deployment. When performing a partial content store deployment, administrators have the option of including visualizations. For more information, see *Deployment* in the *Administration and Security Guide*.

Importing visualizations into the library

Administrators import visualizations from local systems and file shares into the IBM Cognos Analytics environment. The imported visualizations are then listed on the **Library** tab and are available for use in IBM Cognos reports.

About this task

Existing visualizations can be re-imported if they were changed. Because changes to visualizations cannot be reverted, you must understand their impact on the associated reports before replacing the visualizations. Otherwise, this action can result in unintended changes to the reports or prevent the reports from running.

When re-importing visualizations, report authors must update the reports that contain the visualizations in IBM Cognos Analytics - Reporting for the changes to take effect. For most changes, it is sufficient to re-open the reports in a new window in Reporting. In some cases, however, modifications in the report are needed. For example, if the new visualization changed or renamed items in the data set structure of the report, the report must be modified in Reporting.

Procedure

1. In **IBM Cognos Administration**, on the **Library** tab, click **Visualizations**.
2. In the toolbar, click the **Import** icon .

   The **Select Visualizations - New Visualization Import Page** opens.

3. Click **Browse** to navigate to the visualization file that you want to select. Browse again if you want to select additional visualization files.

   Tip: To remove a visualization file from the list of selected visualizations, click the **Remove selection** ✖ icon.

4. To replace an existing visualization, select the **Replace existing entries** check box.

   If you clear this check box while trying to import an existing visualization, the import will fail. This is to ensure that an existing visualization is not accidently overwritten, which could result in breaking the reports that use that visualization. If you decide to replace a specific visualization, import the visualization selecting the **Replace existing entries** check box. Then, in Reporting, update the reports that contain that visualization.

5. To import selected visualizations click **Import**.

Results

The imported visualizations are now listed on the **Visualizations** page. The visualizations have default access permissions that administrators can change.

Managing visualizations

After you import visualizations into IBM Cognos Administration, you can manage them on the **Library** tab.

About this task

You can perform the following actions to manage the visualization resources:

- **Set properties**

  Visualizations are assigned default properties, including access permissions, when they are imported. Library administrators can change the default settings, including access permissions, for a visualization resource.

  For more information see, Chapter 16, “Entry Properties,” on page 219 and “Set access permissions for an entry” on page 179.

  Important: The Set properties icon in the toolbar is used to set properties, including access permissions, for the **Visualizations** page in the **Library**.

- **View my permissions**

  Administrators can view their own permissions for each visualization.

- **Delete**

  You can delete individual or multiple visualizations from the content store database.

- **Download**

  You can download an existing visualization to your hard drive or network share to modify the visualization.

Procedure

1. In IBM Cognos Administration, on the **Library** tab, click the **Visualizations** page.
2. In the visualizations list you can perform the following tasks:
   - To manage one visualization, click its drop-down action menu, and click the chosen action.
   - To delete multiple visualizations, select the check boxes that are associated with the chosen visualizations, and in the toolbar, click the **Delete** ✖ icon.

Chapter 24. Reports and Cubes

You can use reports, cubes, and documents to analyze data and help you make informed and timely decisions.

In IBM Cognos Analytics, reports and cubes can be published to the portal to ensure that everyone in your organization has accurate and relevant information when they need it.

Working with Reports and Cubes

A report can refer to the specification that defines the information to include in a report, or the results themselves. Report specifications can have saved results or you can run a report to produce new results.

After a report is published to the portal, you can view, run, or open it or view report output versions. You can also view the report in various formats.

You can distribute reports by saving them, sending them by email, sending them to IBM Cognos Analytics Mobile Reports, printing them, or bursting them. You can also set run options for the current run, and set advanced run options for the current run.

You can schedule a report to run at a later time or on a recurring basis. You can schedule a report as part of a job or based on a trigger. You can view the run history for a report. You can also include a report in an agent.

You can add yourself to the alert list for a report so that you are alerted when new versions of the report are created. You can also specify watch rules in saved HTML report output so that you are alerted whenever the events specified by the watch rules are satisfied.

You can disable selection-based features, such as drilling up and down and drill-through.

Mixed Currencies

Mixed currency values occur when you calculate values with different currencies. When using an OLAP data source, mixed currency values use the asterisk character (*) as the unit of measure.

IBM Cognos Active Reports

You can use IBM Cognos Analytics - Reporting to create active reports. IBM Cognos Active Report is a report output type that provides a highly interactive and easy-to-use managed report. Active reports are built for business users, allowing them to explore their data and derive additional insight.

Report authors build reports targeted at their users' needs, keeping the user experience simple and engaging. Active reports can be consumed by users who are offline, making them an ideal solution for remote users such as the sales force.

Active reports are an extension of the traditional IBM Cognos report. You can leverage existing reports and convert them to active reports by adding interactive behavior, providing end users with an easy-to-consume interface.

Report Views

A report view uses the same report specification as the source report, but has different properties such as prompt values, schedules, delivery methods, run options, languages, and output formats.

About this task

Creating a report view does not change the original report. You can determine the source report for a report view by viewing its properties. The report view properties also provide a link to the properties of the source report.

If the source report is moved to another location, the report view link is not broken. If the source report is deleted, the report view link is broken and the properties link to the source report is removed.

If you want to use a generic report as the underlying structure for additional reports, make a copy of the report.

The report view has the same run options and properties as the original entry.

View Lineage Information for a Data Item

Lineage information traces the metadata of a data item in an HTML report or a report view back through the package and the data sources used by the package.

Lineage also displays any data item filters that were added by the report author, or that were defined in the data model. For example, you can click a cell in a crosstab to see how the cell value was calculated.

You cannot view lineage information when running a report from a mobile device.

IBM Cognos Analytics can be configured to use the default lineage solution that comes with the product, or a custom lineage solution. IBM InfoSphere Information Governance Catalog is also supported.

To access lineage information in a report, an administrator must configure the lineage solution, enable the **Lineage** capability, and grant read permissions for you on the report.

For more information, see "Configuring the lineage solution" on page 81, Chapter 13, "Capabilities," on page 185, and Chapter 14, "Object Capabilities," on page 197.

The IBM Cognos lineage solution shows lineage on reports at their highest level. The lineage does not change after drilling down on a report. Because the selection context used to launch lineage can be affected by drill-down actions, we recommend that you always launch lineage at the highest report level before drilling down on the report. Otherwise, the lineage may not launch properly.

Procedure

1. Open an HTML report or report view.
2. Right-click the data item you want, and click **Lineage**.

   The lineage views appear.

Access the InfoSphere Business Glossary

If your organization uses IBM InfoSphere Business Glossary, you can also access the Glossary in the Cognos software, from the IBM Cognos Analytics viewer and from the metadata tree in Reporting, Query Studio, and Analysis Studio.

Before you begin

Before you can access the InfoSphere Business Glossary, you must have permissions for the **Glossary** capability, and the Glossary URI must be configured by the administrator.

For more information, see Chapter 13, "Capabilities," on page 185, Chapter 14, "Object Capabilities," on page 197, and "Configure the InfoSphere Business Glossary URI" on page 82.

Procedure

1. Open an HTML report or report view in Cognos Analytics viewer.
2. Right-click the data item you want, and click **Glossary**.

Results

By default, the Glossary search results in Cognos software return only terms that contain the keyword specified in the search. Other types of assets are not returned.

Report formats

In IBM Cognos Analytics, you can view reports in a browser, or depending on your permissions, you can generate reports in formats that can be imported into other applications. Administrators can restrict access to the capabilities that are required to run reports in delimited text (CSV), PDF, Microsoft Excel spreadsheet (XLS), or XML formats.

By default, all users have permissions for the following capabilities:

- Generate CSV Output
- Generate PDF Output
- Generate XLS Output
- Generate XML Output

These separately secured functions support the management of system resources. To control the formats options that users can see and run in the user interface, set access permissions for these capabilities.

If your access to a format is restricted, you can view content in the restricted format, and specify the restricted format in the properties of a report.

To perform the following actions, you must have execute and traverse permissions for the appropriate capability:

- Run reports in a restricted format.
- Set schedules or jobs for reports that run in a restricted format.
- Drill to targets that run in a restricted format.
- Print a PDF report in a Cognos Workspace widget.

When you run a report, you see only the format options for which you have the generate output capability. The HTML format is not a secured function.

The generate output capabilities do not apply to PowerPlay or active reports.

To specify the report format, you must also have read and write permissions for the report and traverse permissions for the folder that contains the report.

You can specify the default format to be used when a report is run.

You can specify the report format in the run options page, in the report properties, or in your preferences.

HTML Formats

In IBM Cognos Analytics, you can choose HTML output format for a report.

PDF Format

Use the PDF format to view and distribute reports in an online book format. In IBM Cognos Analytics, to generate report output in the PDF format, you must have execute and traverse permissions for the **Generate PDF Output** capability.

You must have administrator privileges to specify the advanced PDF options.

Microsoft Excel Formats

You can export your report output to several different Microsoft Excel spreadsheet software formats.

In IBM Cognos Analytics, to generate report output in Microsoft Excel formats, you must have execute and traverse permissions for the **Generate XLS Output** capability.

The Excel formats render report output in native Excel XML format, also known as XLSX.

The **Excel** format provides fully formatted reports. The output is similar to other Excel formats, with the following exceptions:

- Charts are rendered as static images.
- Row height can change in the rendered report to achieve greater fidelity.
- Column widths that are explicitly specified in reports are ignored in Microsoft Excel 2007.
- Merged cells are used to improve the appearance of reports.
- The default size of worksheets is 65 536 rows by 256 columns.

  Your IBM Cognos administrator can enable larger worksheets and change the maximum number of rows in a worksheet, up to a maximum of 16,384 columns by 1,048,576 rows, by using advanced server properties.

Excel Data provides data with minimal formatting. Default data formatting is applied to the data based on the data type and assumes that each column has a single data type.

The output is similar to other Excel formats, with the following exceptions:

- The generated output includes only the first list query in the report. If a report contains multiple queries and the first query is a multi-dimensional query for a crosstab or for a chart, an error message is displayed when the report runs.
- Nested frames and master-detail links are not supported.
- Cells in the Microsoft Excel file have a default width and height. You must adjust the column width and height if the data is larger than the default size.
- Style specifications are not rendered, including color, background color, and fonts.
- Borders are not rendered.
- User-specified data formatting in the report specification are not applied, including exception highlighting and color rules for negative numbers.

CSV Format

Reports saved in delimited text (CSV) format open in the application associated with the .csv file type.

You must have execute and traverse permissions for the **Generate CSV Output** capability to generate report output in the CSV format.

Reports saved in CSV format

- are designed to support Unicode data across many client operating systems
- are UTF-16 Little Endian data-encoded
- include a BOM (Byte Order Mark) at the beginning of the file
- are tab-delimited
- do not enclose strings in quotation marks
- use a new line character to delimit rows
- show only the results of a report query. Page layout items, such as titles, images, and paramDisplay values do not appear in the CSV output.

Report Languages

You can choose the language for a report.

You can specify the report language in the report properties or in your preferences. When you run a report, the language specified in the report properties is used. When it is not specified in the report properties, the language in your preferences is used.

Selecting a language for your report does not change the language used in the portal. You can change the language used in the portal interface in your preferences.

When a report runs, the report server connects to the underlying data source to obtain data. When using an SAP BW data source, if the SAP BW server does not support the language associated with your content locale, IBM Cognos Analytics checks a locale map for a corresponding locale. If the SAP BW server supports the language for the corresponding locale, this language is used. Otherwise, the report runs using the default language installed on the SAP BW server.

To specify the report language, you must have read and write permissions for the report and traverse permissions for the folder that contains the report.

The package used to create the report must contain multilingual data before the report outputs are shown in the selected languages.

Specify the Language for a Report

To specify the language for a report, change the report properties.

Specify the Default Prompt Values for a Report

By default, if a report contains prompts, you must select values each time the report runs. You can change the prompt behavior in the report properties.

About this task

To set default prompt values, you must have read and write permissions for the report and read or traverse permissions for the folder that contains the report.

If you are the report author, you can create default prompt values for a report. When the report is run, the data is automatically filtered based on the prompt values that you specify. The user does not have to specify prompt values when the report is run. You may find this useful if most users use the same prompt values each time they run a report.

If you have write access to a report and change the prompt values, those values are saved for everyone running the report after you. If you consistently use prompt values that differ from the majority of users, create a report view of the report.

Saving report output

You select how to save report copies as a delivery option.

All report output is stored automatically in IBM Cognos Analytics. You may also be able to save copies of reports in other file locations:

- in IBM Cognos Analytics so that it can be used again and for archive purposes
- outside of IBM Cognos Analytics for use in external applications such as web sites and for use by people who don't have access to IBM Cognos Analytics

You can also choose how to save a report when you schedule it .

Before you begin

Before you can save report output to file locations, your administrator must set up the locations.

For more information about setting up file locations, see “Saved report output” on page 77.

Procedure

1. In a folder or subscription list, for the report that you want to run, click the More button ⋯ and then click ▶**Run as** or ▶**Run once**.
2. Select an output format.
3. If required, select **Run in background**, click **Advanced**, and then follow these steps:
   a) Select **Now** or select **Later** and specify when you want the report to run.
   b) In the **Languages** field, select one or more output languages.

c) In the **Delivery** field, choose whether the report will be:

- sent as an attachment or link in an email
- sent to a printer
- saved as a local file
- saved as an external file

Tip: The **Save report as an external file** option is available only if you have configured a File systems location for external files. For more information, see "Saving report output files outside of IBM Cognos software" on page 78.

d) You can also change how file conflict is resolved. Click **Keep existing** to not overwrite existing files or **Replace** to overwrite existing files. Click **Time stamp** or **Version number** to avoid overwriting existing files by making new files with unique timestamps or sequence numbers.

e) If more than one file location is defined, select the location where you want to save from the **Location** list.

4. Click **Done**.

Specifying how long to keep report output versions

From the report properties, you can specify the number of report output versions to keep and the number of days or months they should be kept.

Specify How Long to Keep Report Output Histories

You can keep report output for a specific number of runs or for a specific number of days or months.

For example, you can keep the report output for the ten latest occurrences or you can keep the report output for the 2 days or 6 months.

About this task

You must have read and write permissions for the entry and read or traverse permissions for the folder that contains the entry.

Data Sources With Named Sets May Produce Unpredictable Results

If your dimensional data sources include named sets, which are sets of members or set expressions that are created for reuse, the data results are unpredictable in Query Studio when combined with filtering and level nesting.

Additionally, if your data sources include multilevel named sets, the data results are unpredictable in Analysis Studio when aggregated.

We therefore recommend that you avoid exposing named sets or multilevel named sets to Query Studio and Analysis Studio users.

Working with named sets may also cause unpredictable results in Reporting. For more information, see the IBM Cognos Analytics - Reporting *User Guide*.

Series 7 Reports in IBM Cognos Analytics

PowerPlay 7.3 or later can be configured to use IBM Cognos Analytics rather than Upfront as a portal. However, if you are accessing content from other IBM Cognos applications or versions previous to PowerPlay 7.3, the administrator may still depend on the Upfront portal.

Series 7 PowerPlay Reports and Cubes

After Series 7 PowerPlay reports and cubes are published to IBM Cognos Analytics, you can use PowerPlay authoring tools to create and edit Series 7 PowerPlay reports.

For more information about PowerPlay authoring tools, see the PowerPlay Web *User's Guide*.

You can change the default run options of Series 7 PowerPlay reports and cubes and select multilingual properties.

Series 7 PowerPlay reports and cubes function differently from other reports. The following actions do not apply to Series 7 PowerPlay reports and cubes:

- Viewing the run history and report output versions.
- Specifying how long to keep report outputs and histories.
- Canceling and suspending reports.
- Specifying prompt values for report formats other than PDF.
- Specifying language for the content of reports.
- Running a report as the owner.
- Scheduling reports.
- Distributing reports.

Single Signon

Single signon ensures that users who are logged on to one IBM Cognos application are not prompted for authentication when they run another IBM Cognos application.

You can ensure that your users benefit from single signon by ensuring that both IBM Cognos Analytics and PowerPlay use the same Series 7 namespace as their authentication source. Alternatively, you can ensure that the authentication namespaces used for both IBM Cognos Analytics and PowerPlay are configured to use an external single signon mechanism for authentication, such as operating system signons for Series 7 PowerPlay or LDAP provider with External Identity Mapping in IBM Cognos Analytics.

For instructions about setting up Series 7 single signon, see the Access Manager *Administrator Guide*.

For instructions about setting up single signon for the IBM Cognos reporting product, see the *Installation and Configuration Guide*.

Change the Defaults for a Series 7 PowerPlay Report

You can change the defaults for Series 7 PowerPlay reports.

You can select one of the following default actions when a report is run:

- Run the report in PDF format (default).
- Open the report with PowerPlay Web Explorer.

For HTML format reports, you can choose to open the report in design mode (without data). Opening a report in design mode is useful to quickly view the structure of the report.

For PDF format reports, you can choose to be prompted for values that filter the range of data included in a report. For example, you can specify a date range that is a subset of the dates available in the report. If the Series 7 PowerPlay report was created with prompt values, you are prompted to enter values when the report runs.

Multilingual Properties for Series 7 Reports and Cubes

In IBM Cognos Analytics, you can select the multilingual properties of a Series 7 report or cube.

The settings in IBM Cognos Analytics do not affect content, data, category labels, and other labels. The language for these items is set by the PowerPlay administrator who creates the report or cube.

Chapter 25. Managing Human Tasks

There are three types of human tasks you can see in **My Inbox**: approval requests, ad-hoc tasks, and notification requests.

You open **My Inbox** from your **Personal menu** on the Welcome page.

Tasks can be created from

- Event Studio (notification requests and approval requests)

  For more information, see the Event Studio *User Guide*.
- **My Inbox** (notification requests and ad-hoc tasks).
- a watch rule set up for a report (notification requests only).

Approval Requests and Ad-hoc Tasks

You can create approval requests using Event Studio.

For more information, see the Event Studio *User Guide*.

You can create ad-hoc tasks from your task inbox. For more information, see "Create an Ad-hoc Task" on page 332.

An approval request or ad-hoc task can have various recipients:

- a task owner - one specific user
- potential owners - multiple users, groups, roles, or distribution lists
- stakeholders - one or more interested parties, who are not potential owners

If a task only has one potential owner, that user automatically becomes the task owner. If a task has multiple owners, the user who claims the task becomes the task owner.

It is possible to create a task with one or more stakeholders, but no owner or potential owners. In this case, stakeholders can assign potential owners after it has been created.

Task Status

The status of an approval request or ad-hoc task can be one of the following:

- Not Started - the task is waiting to be started.
- Started - the task has an owner and is in progress.
- Completed - the owner has complete the task.
- Canceled - the task has been canceled by a recipient.

View Comments

You can view comments added by other recipients, as well as audit history comments, recorded by the system.

You can also add your own comments to a task. For more information, see "Add Comments to a Task" on page 336.

Procedure

1. View your task inbox.
2. Select the task for which you want to view comments, and then click the **Discussion** tab in the reading pane.

By default, only user comments are shown.

3. Select the type of comments you want to view from the comments drop-down list.

   You can view all user and audit comments, or you can filter the display by comment type.

Subscribe to E-mail Notifications

The default notification options are set up when the task is created. You can change your subscriptions for any task with a status of Not Started or Started.

You can choose to receive, or stop receiving, notifications when

- a task is not started by the start date
- a task is not completed by the due date
- the status of a task changes (started, completed or canceled)
- the owner of a task changes
- a user comment is added to a task

Note:

- Notifications are sent to the task owner and copied to all stakeholders.
- The recipient who changes the status or owner of a task, or adds a user comment, does not receive the associated notification.

Procedure

1. View your task inbox.
2. Select the task for which you want to change your notification subscriptions, and then click the **Notification Options** tab in the reading pane.
3. Select the appropriate check boxes for the notifications you want to receive, and clear the boxes for those you do not require.
4. Click **Save**.

Create an Ad-hoc Task

Create an ad-hoc task to send a task to the task inbox of the recipients you specify.

You can add deadlines to an ad-hoc task when you create it. Alternatively, potential owners or stakeholders can add deadlines at a later date, by updating the task from their task inbox.

You can set up notification options for the task owner to receive e-mails when

- an ad-hoc task is not completed by the due date
- an ad-hoc task is not started by the start date

Note: Stakeholders are also copied on these e-mails.

In addition, you can set up notification options for the task owner and all stakeholders to receive e-mails when

- the status of an ad-hoc task changes (started, completed or canceled)
- the owner of an ad-hoc task changes
- a comment is added to an ad-hoc task

Note: Potential owners and stakeholders can unsubscribe from receiving specific notifications by updating the task from their task inbox.

Procedure

1. View your task inbox.

2. From the task drop-down list, select **New Task** .
3. In the reading pane, click **Add/Remove recipients**.

   The **Select recipients** page appears.
4. Select the required users, groups, roles, and distribution lists to add as potential owners and stakeholders.

   - To choose from listed entries, click the appropriate namespace, and then select the check boxes next to the users, groups, roles or distribution lists.

     Tip: To make the user entries visible, click **Show users** in the list.
   - To search for entries, click **Search** and, in the **Search string** box, type the phrase you want to search for. For search options, click **Edit**. Find and click the entry you want.
   - To type the name of entries you want to add, click **Type** and type the names of groups, roles, or users using the following format, where a semicolon (;) separates each entry:*namespace/group_name*;*namespace/role_name*;*namespace/user_name*;

     Here is an example:

     Cognos/Authors;LDAP/scarter;
5. Click the **Potential Owner** or **Stakeholder** arrow button to update the **Selected entries** list, and click **OK**.

   Tip: To remove entries from the **Selected entries** list, select them and click **Remove**. To select all entries in the list, select the check box for the list.
6. Click **OK**.
7. In the **Subject** box, type the subject of the task.
8. If required, add a completion deadline for the task in the **Due Date** box.
9. If required, add a start by deadline for the task in the **Start By** box.
10. Select the priority from the **Priority** list.
11. In the **Message** box, type text directly.
12. To add links, click **Add links**, select the entries you want, click the arrow button to update the **Selected entries** list, and click **OK**.

    Tip: To remove links, select them and click **Remove links**.
13. If you want to set up notification options, click **Advanced**, otherwise move on to step 16.
14. Select the task creation and deadline notification options as required:

    - **Send notification if not started by the start date**
    - **Send notification if not completed by due date**
15. Select the approval request change notification options as required:

    - **Started**
    - **Comment**
    - **Owner changed**
    - **Completed**
    - **Canceled**
16. Click **Save**.

Actions That You can Perform on Approval Requests and Ad-hoc Tasks

The actions you can perform on an approval request or ad-hoc task differ depending on your recipient type.

The following table summarizes the actions that can be performed by each type of recipient.

Table 76. Approval request and ad-hoc actions by recipient type

Action	Potential owner	Owner	Stakeholder
Claim ownership of a task	X		
Change the recipients for a task	X	X	X
Revoke ownership of a task		X	
Set deadlines for a task	X	X	X
Change the priority of a task	X	X	X
Add comments to a task	X	X	X
Start or stop a task		X	
Complete a task		X	
Cancel a task		X	X

Claim a Task

If you are a potential owner of a task that is Unclaimed, you can claim the task. The task is then owned by you.

If you are the only potential owner of a task, the task is automatically owned by you. In this case, it is not necessary to claim the task.

Procedure

1. View your task inbox.
2. Select the task you want to claim, and then click **Make me the owner** in the reading pane.

Change the Recipients for a Task

Any task recipient can change the current owner of a task.

In addition, they can add or remove potential owners and stakeholders for a task. The status of the task must be Not Started or Started.

Note: If you are the owner of a task, you can revoke ownership of the task "Revoke Ownership of a Task" on page 335.

Change the Current Owner

You can change the current owner.

Procedure

1. View your task inbox.

2. Select the task for which you want to change the current owner, and then click **Change Owner** in the reading pane.

   The **Select the user** page appears.
3. Select the user.
   - To choose from listed entries, click the appropriate namespace, and then select the required user.
   - To search for an entry, click **Search** and, in the **Search string** box, type the phrase you want to search for. For search options, click **Edit**. Find and click the entry you want.
4. Click **OK**.
5. Click **Save**.

Change the Potential Owners and Stakeholders

You can change the potential owners and stakeholders.

Procedure

1. View your task inbox.
2. Select the task for which you want to change potential owners and stakeholders, and then click **Add/ Remove recipients** in the reading pane.

   The **Select recipients** page appears.
3. Select the required users, groups, roles, and distribution lists.
   - To choose from listed entries, click the appropriate namespace, and then select the check boxes next to the users, groups, roles or distribution lists.

     Tip: To make the user entries visible, click **Show users** in the list.
   - To search for entries, click **Search** and in the **Search string** box, type the phrase you want to search for. For search options, click **Edit**. Find and click the entry you want.
   - To type the name of entries you want to add, click **Type** and type the names of groups, roles, or users using the following format, where a semicolon (;) separates each entry:

     namespace/group_name;*namespace/role_name*;*namespace/user_name*;

     Here is an example:

     Cognos/Authors;LDAP/scarter;
4. Click the **Potential Owner** or **Stakeholder** arrow button to update the **Selected entries** list, and click **OK**.

   Tip: To remove entries from the **Selected entries** list, select them and click **Remove**. To select all entries in the list, select the check box for the list.
5. Click **OK**.
6. Click **Save**.

Revoke Ownership of a Task

If you are the owner of a task, you can remove yourself as the task owner.

This changes the owner to Unclaimed and the status of the task to Not Started.

Procedure

1. View your task inbox.
2. Select the task you want to revoke, and then click **Remove me as owner** in the reading pane.

Set Deadlines for a Task

Any task recipient can add a start date or due date for an approval request or ad-hoc task with a status of Not Started or Started. They can also amend existing deadlines.

Where notifications are set up, if a task is not started or completed by the required time, e-mail notifications are sent all subscribing potential owners and stakeholders. For more information on notifications, see "Subscribe to E-mail Notifications" on page 332.

Procedure

1. View your task inbox.
2. Select the task for which you want to update the deadlines.
3. If required, add a completion deadline for the task in the **Due Date** box.
4. If required, add a start by deadline for the task in the **Start By** box.
5. Click **Save**.

Change the Priority of a Task

The priority of a task is set when the task is created. Any task recipient can change the priority of a task with a status of Not Started or Started.

Procedure

1. View your task inbox.
2. Select the task for which you want to change the priority, and then select the priority from the **Priority** list in the reading pane.
3. Click **Save**.

Add Comments to a Task

Any task recipient can add comments to a task.

For information on viewing comments added to a task, see "View Comments" on page 331.

Procedure

1. View your task inbox.
2. Select the task for which you want to add a comment, and then click the **Discussion** tab in the reading pane.
3. Click **Add Comment** , type your comments in the window that appears, and then click **OK**.
4. Click **Save**.

Start or Stop a Task

If you are the owner of a task that has not been started, you can start the task.

This changes the status to Started so that other task recipients can view the progress of your task.

A potential owner can also start an unclaimed task. The user then becomes the owner of that task.

If you own a task that has already been started, you can stop the task. This changes the status to Not Started.

Procedure

1. View your task inbox.

2. Select the task you want to start, and then select **Start task** from the **Status** drop-down list in the reading pane.

   Tip: To stop a task that has been started, select **Not Started** from the **Status** drop-down list.
3. Click **Save**.

Completing a Task

If you are the owner of a task with a status of Not Started or Started, you can complete the task by performing the required action.

The action required differs depending on the task type. For ad-hoc tasks, you must mark the task as complete.

For approval request tasks, the action depends on how the task creator set up the task. You must perform one of the following actions:

- approve or reject the request

  For this type of approval request, you must approve or reject the request from your task inbox to complete the task.

  Depending on how the task was set up, completion of the task may result in another action being performed. For example, if you approve a request to distribute a report, when the task is complete, the report may be automatically distributed. If the request is rejected, no further actions will occur.
- Specify the remaining tasks to approve and run

  This type of approval request contains one or more tasks that are scheduled to run after the task is complete. You must select which tasks you approve to run.

Complete an Ad-Hoc Task

The procedure to complete an ad-hoc task is as follows.

Procedure

1. View your task inbox.
2. Select the task you want to complete and then click **Mark as complete**.

   The status of the task changes to Completed.

Approve or Reject a Request

The procedure to approve or reject a request is as follows.

Procedure

1. View your task inbox.
2. Select the task you want to complete and view the details in the reading pane.
3. If required, add a comment to explain your decision in the **Comment** box.
4. Click **Approve** or **Reject** to complete the task.

   Note: Approve and **Reject** are the default button names. The user who created the task may have used custom button names, which differ from the default.

   The status of the task changes to Completed.

Specify the Remaining Tasks to Approve and Execute

You can specify the remaining tasks to approve and execute.

Procedure

1. View your task inbox.
2. Select the task you want to complete and view the details in the reading pane.
3. Select the remaining tasks to approve, and then click **Submit**.

   Note: Submit is the default button name. The user who created the task may have used a custom button name, which differs from the default.

   The status of the task changes to Completed.

Cancel a Task

A task owner or stakeholder can cancel an approval request or ad-hoc task with a status of Not Started or Started.

Procedure

1. View your task inbox.
2. Select the task you want to cancel, and then click **Mark as canceled** in the reading pane.

   The status of the task changes to Canceled.

Notification Requests

You can create a notification request with an option for recipients to acknowledge the request. You can also specify deadlines for acknowledgements.

A notification request can have various recipients:

- users, groups, roles, and distribution lists to whom the request is sent (To list recipients)
- stakeholders to whom the request is copied (CC list recipients)

The status of a notification request can be

- Unread - the request has not been opened by a recipient
- Read - the request has been opened by a recipient
- Acknowledged - the request has been confirmed by a recipient included on the To list.

Notifications can also be created in IBM Cognos Event Studio. For more information, see the Event Studio *User Guide*.

Acknowledgements

When a notification request is created, you can request an acknowledgement from each recipient included on the To list.

Note: Stakeholders (CC list recipients) do not have the option to acknowledge notification requests.

Deadlines

When a notification request is created, you can include an acknowledgement deadline. You can also specify that an e-mail is sent to each recipient on the To list who does not acknowledge a notification request by the deadline date. On the deadline date, a separate e-mail is sent to stakeholders on the CC list informing them that some recipients on the To list have not acknowledged the notification request.

Tip: A stakeholder can verify who has acknowledged a notification request by checking e-mails or the audit tables.

When all the To list recipients have acknowledged the request, the deadline is canceled.

Create a Notification Request

Add a notification request to an agent to send a secure notification about an event to the inbox of recipients you specify.

You can request an acknowledgement, and add an acknowledgement deadline.

Procedure

1. View your task inbox.
2. Select **New Notification** from the task drop-down list.
3. Click **Add/Remove recipients** in the reading pane.

   The **Select recipients** page appears.
4. Select the required users, groups, roles, and distribution lists to add as recipients.
   - To choose from listed entries, click the appropriate namespace, and then select the check boxes next to the users, groups, roles or distribution lists.

     Tip: To make the user entries visible, click **Show users** in the list.
   - To search for entries, click **Search** and, in the **Search string** box, type the phrase you want to search for. For search options, click **Edit**. Find and click the entry you want.
   - To type the name of entries you want to add, click **Type** and type the names of groups, roles, or users using the following format, where a semicolon (;) separates each entry:

     `*namespace/group_name*;*namespace/role_name*;*namespace/user_name*;`

     Here is an example:

     Cognos/Authors;LDAP/scarter;
5. Click the **To** or **Cc** arrow button to update the **Selected entries** list, and click **OK**.

   Tip: To remove entries from the **Selected entries** list, select them and click **Remove**. To select all entries in the list, select the check box for the list.
6. Click **OK**.
7. In the **Subject** box, type the subject of the notification request.
8. In the **Message** box, type text directly.
9. To add links, click **Add links**, select the entries you want, click the arrow button to update the **Selected entries** list, and click **OK**.

   Tip: To remove links, select them and click **Remove links**.
10. If you want to set up notification options, click **Advanced**, otherwise move on to step 13.
11. To request an acknowledgement from each recipient on the To list, select the **Request Acknowledgement** box.
12. To send an e-mail notification to recipients who do not acknowledge the request by a deadline date, select the **Send notification if not acknowledged by the date** box, and then select the required date.
13. Click **Save**.

Read and Acknowledge a Notification Request

New notification requests in your task inbox have the status Unread.

You can read the notification request, and acknowledge it, if this option is available to you.

Procedure

1. View your task inbox.
2. Select the unread notification request you want to read, and view the details in the reading pane.

The status of the notification request changes to Read.

3. If your username appears in the **To** list, and an acknowledgement is required, click **Acknowledge**.

   The status of the notification request changes to Acknowledged.

   Note: If your username appears in the **To** list, you are a recipient of the notification request. If it appears in the **CC** list, you are a stakeholder copied on the request. If there is a deadline set up for the notification request, it is shown in the **Deadline** box.

Archive Tasks

Archiving is a method of removing unwanted tasks from your inbox.

When you archive a task, it remains active in IBM Cognos Analytics, and other task recipients can continue to work with it. Any notifications associated with an archived task also remain active.

Tasks that are deleted from your archive also remain active, but you can no longer view them.

Procedure

1. View your task inbox.
2. Select the tasks you want to archive, and then click **Archive** from the **Move to** drop down list.

View the Task Archive

You can view a list of tasks that you have archived.

Procedure

View your task inbox, and then click the **Archive** tab.

What to do next

You can view the details of a task, by selecting it. The task details are shown in the reading pane. If the task contains an attachment, such as a report, you can double-click to view it.

Tip:

- To view the due date for tasks instead of the date received, select **Display Due Date** from the **Display Date Received** drop-down list.
- To return to your task inbox, click the **Inbox** tab.
- To delete unwanted tasks, select them, and then click **Delete** .

Chapter 26. Drill-through Access

Drill-through applications are a network of linked reports that users can navigate, retaining their context and focus, to explore and analyze information.

Drill-through access helps you to build applications that are bigger than a single report.

For example, you have an Analysis Studio report that shows revenue and you want to be able to drill through to a Reporting report that shows details of planned and actual revenue.

Another example is an Analysis Studio report that lists the top 10 promotions by retailer and you want to be able to drill through to a Reporting report that shows promotion plan revenue.

Drill-through access works by passing information from the source to the target object, usually a report. You define what is passed from the source report by having the system match information from the selection context of the source report to the content of the target (dynamic drill through) or by defining parameters in the target (parameterized drill through). You define drill-through access for the source, either at the package level or at the report level. Within a package, you control the scope of the data for which drill-through access is available in the drill through definition. Within a report, you define the drill-through access on a report item.

What You Should Know

For a drill-through link to work, it is necessary to know:

- what the source report is or is going to be
- what the target report is or is going to be
- whether the users of the drill through link in the source report have the appropriate permissions to view or run the target report
- how the data in the two reports is related

  Depending on the underlying data, you may create a drill through definition (dynamic drill through) or map the source metadata to parameters defined in the target report or package (parameterized drill through)
- whether to run the target report or to open it

  The target of drill-through access is usually a saved report definition. The report can be created in Reporting, PowerPlay Studio, Query Studio, or Analysis Studio. The target of drill-through access can also be a package that contains a PowerCube, in which case a default view of the PowerCube is created.
- if the target is being run, in what format to run it and what filters to run it with

  If you don't want to run the target report on demand, you may link instead to a bookmark in the saved output.

Sources and Targets

There are many different combinations of source and target. For example, you can drill through

- between reports created in different packages against different data source types, such as from an analysis against a cube to a detailed report against a relational data source. For more information on creating drill through access in packages, see "Setting up drill-through access in packages" on page 347.
- from one existing report to another report using Reporting. For more information on creating drill through access in a report, see "Set Up Drill-through Access in a Report" on page 353
- between IBM Cognos Viewer reports authored in Reporting, Query Studio, PowerPlay Studio, and Analysis Studio

- from Series 7 PowerPlay Web cubes to IBM Cognos Analytics reports.

Understanding drill-through concepts

Before you set up drill-through access, you must understand the key concepts about drilling through. Knowing these concepts will help you to avoid errors so that report consumers drill through as efficiently as possible.

Drill through paths

You can create a drill through path in a source report, or using drill through definitions. A drill through path is the definition of the path that is taken when moving from one report to another, including how the data values are passed between the reports.

Using **Drill Through Definitions**, you can create a drill through path from any report in the source package to any target report in any other package. This type of drill through definition is stored in the source package.

For any target report that contains parameters, you should map the target parameters to the correct metadata in the drill through path. This ensures that the values from the source report are passed to the correct parameter values, and that the target report is filtered correctly. If you do not map parameters, then the users may be prompted for values when the target report is run.

A report-based drill through path refers to a path created and stored in a source report. This type of drill through path is also called authored drill through. The path is associated with a specific data column, chart, or cross tab in the source report, and is available only when users select that area of the report. If an authored drill through definition is available, a hyperlink appears in the source report when it is run.

Report-based drill through is limited to reporting source reports and any target reports. Use this type of drill through access when you want to pass data item values or parameter results from within a source report to the target report, pass the results of a report expression to a target report, or a use URL link as a part of the drill through definition.

Selection contexts

The selection context represents the structure of the values selected by the user in the source.

In IBM Cognos Analysis Studio, this includes the context area. When a package drill through definition is used, the selection context is used to give values for mapped parameters (parameterized drill through) or also to map the appropriate data items and values.

Drill through links can also be defined to open the target object at a bookmark. The content of this bookmark may also specified by the selection context.

Drill through access is possible between most combinations of the IBM Cognos Analytics studios. Each studio is optimized for the goals and skills of the audience that uses it, and in some cases for the type of data source it is designed for. Therefore, you may need to consider how the various studios manage the selection context when you drill through between objects created in different studios, and how the data sources are conformed. During testing or debugging, you can see how source values are being mapped in different contexts using the drill through assistant.

Drilling through to different report formats

The settings in the drill through definition determine the format in which users see the report results.

For example, the users may see the reports in IBM Cognos Viewer as an HTML Web page, or the reports may open in IBM Cognos Query Studio, IBM Cognos PowerPlay Studio, or IBM Cognos Analysis Studio. If your users have PowerPlay Studio, then they may also see the default view of a PowerCube.

Reports can be opened as HTML pages, or as PDF, XML, CSV, or Microsoft Excel spreadsheet software formats. When you define a drill through path, you can choose the output format. This can be useful if the expected use of the target report is something other than online viewing. If the report will be printed, output it as PDF; if it will be exported to Excel for further processing, output it as Excel or CSV, and so on.

To run reports, or drill to targets that run reports in the delimited text (CSV), PDF, Microsoft Excel spreadsheet (XLS), or XML output formats, users require the generate output capability for the specific format.

Note: PDF drill through is supported only in Internet Explorer using the Adobe PDF plug-in.

If you define a drill through path to a report that is created in Analysis Studio, PowerPlay Studio, or Query Studio, consumers can open the report in its studio instead of in IBM Cognos Viewer. This can be useful if you expect a consumer to use the drill through target report as the start of an analysis or query session to find more information.

For example, if an application contains a dashboard style report of high-level data, you can define a drill through link to Analysis Studio to investigate items of interest. The Analysis Studio view can then be drilled through to a PDF report for printing.

Note: IBM Cognos Analytics - Reporting does not display data results.

Related concepts

Report formats

Drilling through between packages

You can set up drill through access between packages.

The two packages can be based on different types of data source, but there are some limits. The following table shows the data source mappings that support drill through access.

Table 77. Data source mappings that support drill through access

Source data source	Target data source
OLAP	OLAP **Note:** OLAP to OLAP drill through is supported only if the data source type is the same, for example, SSAS to SSAS.
OLAP	Dimensionally modeled relational
OLAP	Relational data **Note:** For more information, see "Business keys" on page 345.
Dimensionally modeled relational	Dimensionally modeled relational
Dimensionally modeled relational	Relational
Relational	Relational

Bookmark References

When you drill through, the values that you pass are usually, but not always, used to filter the report.

IBM Cognos Analytics supports bookmarks within saved PDF and HTML reports so that a user can scroll a report to view the relevant part based on a URL parameter.

For example, you have a large inventory report scheduled to run daily or weekly during off hours because of resource considerations. Your users may want to view this report as a target because it contains detailed information, but you want them to view the saved output rather than run this large report. Using this Action option and bookmark settings, users can drill through from another source location based on products to open the saved report to the page that shows the product they want to focus on.

When a bookmark in the source report is used in a drill-through definition, it provides the value for the URL parameter. When report consumers drill through using this definition, they see the relevant section of the target report.

Note: PDF drill-through is supported only in Internet Explorer using the Adobe PDF plug-in.

Bookmark references are limited to previously run reports that are output as PDF or HTML and contain bookmark objects.

Members and values

Dimensionally modeled data, whether stored in cubes or stored as dimensionally modeled relational (DMR) data, organizes data into dimensions. These dimensions contain hierarchies. The hierarchies contain levels. And the levels contain members.

An example of a dimension is Locations. A Locations dimension may contain two hierarchies: Locations by Organization Structure and Locations by Geography. Either of these hierarchies may contain levels like Country or Region and City.

Members are the instances in a level. For example, New York and London are members in the City level. A member may have multiple properties, such as Population, Latitude, and Longitude. Internally, a member is identified by a Member Unique Name (MUN). The method by which a MUN is derived depends on the cube vendor.

Relational data models are made up of data subjects, such as Employees, which are made up of data items, such as Name or Extension. These data items have values, such as Peter Smith.

In IBM Cognos Analytics, the methods of drilling through available are

- Dimensional (member) to Dimensional (member)
- Dimensional (member) to Relational (data item value)
- Relational (data item value) to Relational (data item value)

If the target parameter is a member, the source must be a member. The source and target should usually be from a conformed dimension. However, if the data supports it, you may also choose to define a mapping using different properties of the source metadata item.

If the target parameter is a value, the source can be either a value or a member. If the source is a dimensional member, you must ensure that the level or dimension is mapped to the target data item correctly in the drill through definition. The business key from which the member is sourced should usually match the relational target value, which is most often the business key. However, if the data supports it, you may also choose to define a mapping from the caption of the source metadata item.

Conformed dimensions

If you work with more than one dimensional data source, you may notice that some dimensions are structured the same, and some are not.

The reason that dimensions can be structured differently is that the data sources may serve different purposes.

For example, a Customer dimension appears in a Revenue data store, but not in an Inventory data store. However, the Products dimension and the Time dimension appear in both data stores.

Dimensions that appear in multiple data stores are conformed if their structure is identical for all of the following:

- hierarchy names
- level names
- level order

- internal keys

Drilling through is possible between different dimensional data stores only if the dimensions are conformed, and if the dimension data store is of the same vendor type, such as IBM Cognos PowerCube as the source and the target. For example, in two data stores for Revenue and Inventory that contain Products and Time dimensions, it is possible to define the Products and Time dimensions differently for each data store. However, for drill-through between the Products and Time dimensions to work, their structures must be identical in each data store.

If you are not sure whether your dimensions are conformed, then you should check with the data modeler to ensure that the drilling through will produce meaningful results.

IBM Cognos Analytics does not support conformed dimensions generated by IBM Cognos Framework Manager for SAP BW data sources.

Dimensionally modeled Relational Data Sources

Ensure that each level contains a business key that has values that match your PowerCube or other DMR models. Also, you must also ensure that the **Root Business Key** property is set and uses the business key of the first level in the hierarchy. This helps to ensure that you have a conformed member unique name when attempting to drill through using members from this dimension.

Business keys

When drill-through access is defined from a member to a relational value, the business key of the member is passed by default.

This means that your relational target parameter must be set up using the data item with a matching value, which is most often the business key data item. You can also choose to pass the caption of the source metadata item.

For example, employees are usually uniquely identified by an employee number, not by their name, because their name is not necessarily unique. When you drill through from a dimensional member to a relational data item, the value provided is the business key. Therefore, the parameter in the target report must be defined to accept a business key value. The exact logic used to define the business key value supplied depends on the cube vendor. For IBM Cognos PowerCubes, the business key value is the **Source** property defined for the level in IBM Cognos Transformer. IBM Cognos Series 7 Transformer PowerCubes pass the source value if the drill-through flag was enabled before the cube was built. Otherwise, the category code is used.

In IBM Cognos Analytics - Reporting, you can determine what the member business key is using an expression such as `roleValue('_businessKey',[Camping Equipment])`. This expression is case-sensitive.

SSAS 2005 multipart business keys are not supported in drill-through operations.

Tip: When other users run your drill-through report, you may not want them to be prompted for a business key. In Reporting, you can build a prompt page with a text that is familiar to the users, but filters on the business key. Your IBM Cognos Framework Manager modeler can also set the **Display Item Reference** option for the **Prompt Info** property to use the business key when the data item is used in a prompt.

Scope

Scope is specific to drill-through definitions created using drill-through definitions (package drill-through definitions). The scope you set defines when the target report is shown to the users, based on the items they have in the source report.

Usually, you define the scope of a drill-through path to match a parameter that it passes. For example, if a target report contains a list of employees, typically you want to display the report as an available drill-through choice only when a user is viewing employee names in a source report. If employee names are not in the source report and the scope was set on the employee name in the drill-through definition, the employee report does not appear on the list of available drill-through target reports in the **Go To** page. You can set the scope to a measure or to an item in the report.

In report-based drill-through access, where the drill-through path is associated with a specific report column, the column serves as the scope.

Mapped parameters

Drill-through targets may contain existing parameters or you can add parameters to the target for greater control over the drill-through link.

You usually map all parameters in a drill-through target to items from the source.

When you map source items that are OLAP or DMR members to target parameters, you can select from a set of related member properties to satisfy the requirements of the target parameter. For a dimensional target, a dimensional source item uses the member unique name by default. For a relational target, a dimensional source item uses the business key by default.

For example, you could change the source member property that is used for a mapping to the member caption instead of the business key to match the parameter in a relational target. For a dimensional target, you could define a parameter that accepts a particular property (such as business key or parent unique name), then pass the appropriate source property to satisfy that target.

Note: If you define drill through between non-conformed dimensions, you should test carefully to ensure that the results behave as expected.

If you do not specify parameter mappings, then by default, you will be prompted for any parameters required in the target when you use the drill-through link. To customize this behavior, use the display prompt pages setting.

When the action is set to **Run the report using dynamic filtering**, then additional filtering is applied if names from the context in the source report match names of items in the target. Use this action as well when there are no parameters defined in the target.

If parameters are not mapped correctly, then you may receive an empty report, the wrong results, or an error message.

The source and target cannot contain identical parameter names when they are from different packages, even if the data structure is conformed. If the source and target are from the same package, there is no restriction.

If you have the necessary permissions, you can use the drill-through assistant to look at what source parameters are passed, and what target parameters are mapped for a given drill-through link.

You can change the dynamic drill-through filter behavior if you want drill-through to generate a filter using the Member Business Key instead of the default Member Caption. For more information, see Changing Drill-Through Filter Behavior in the *IBM Cognos Administration and Security Guide*.

Drilling through on dates between PowerCubes and relational packages

The usual method of drilling through from OLAP to relational packages requires that the target report parameter is set using the business key in the relational data, which does not work well for dates.

OLAP data sources typically view dates as members, such as Quarter 1 2012, while relational data sources view dates as ranges, such as 1/Jan/2012 to 31/March/2012.

A special feature exists for drilling through between PowerCubes and relational packages. Ensure that the target report parameter is set up using `in_range`. The parameter must be of type date-time, and not integer.

An example follows:

```
[gosales_goretailers].[Orders].[Order date] in_range ?Date?
```

Also ensure that the drill-through definition maps the parameter at the dimension level and that the PowerCube date level is not set to suppress blank categories. Enabling the option to suppress blank categories in the Transformer model before you build the cube may cause the drill-through on dates to be unsuccessful. This happens because there are missing values in the range.

Setting up drill-through access in packages

A drill-through definition specifies a target for drill-through access, the conditions under which the target is available (such as the scope), and how to run or open, and filter the target.

In IBM Cognos Analytics, a drill-through definition is associated with a source package. The drill-through path defined in the drill-through definition is available to any report based on the source package it is associated with. The target can be based on any target package and can be stored anywhere. For example, all reports authored in the GO Data Warehouse (analysis) sample package or in a folder linked to this package can access any drill-through definition created in this package.

Note: You can define drill-through access in specific reports by setting up the drill-through definition in the report instead of in the package, or restrict drill-through access by changing report settings so that the report is unavailable as a drill-through target.

You can define drill-through definitions between reports created in the different studios, and reports based on different packages and data sources.

The target report must exist before you start creating the drill-through definition. Drill-through targets can be reports, analyses, report views, PowerCube packages, and queries.

Drill-through definitions support both dimensional and relational packages.

Before you begin

To run reports, or drill to targets that run reports in the delimited text (CSV), PDF, Microsoft Excel spreadsheet (XLS), or XML output formats, you require the generate output capability for the specific format.

Procedure

1. Check the drill-through target:

   - Confirm that the drill-through users have access to the target.
   - Hide the target from direct access if you want.
   - If necessary, check what parameters exist in the target.

     When a drill-through definition links objects in different packages, you must consider the data types used in both the source and the target object. Review the structure and values of data that you intend to pass in the drill-through, and ensure that the created parameters are appropriate for your scenario, if you have defined parameters, or that dynamic drill-through will work successfully.
2. Launch **Drill-through Definitions**.
3. Navigate to the package for which you want to create the drill-through definition.
4. Click the **New Drill-through Definition** icon on the toolbar.

   Tip: If the **New Drill-through Definition** icon does not appear, confirm that you are at the package level, and not in a folder in the package. Drill-through definitions must be stored at the package level.
5. Type a name for the drill-through definition.
6. If you want, type a description and screen tip, and then click **Next**.
7. Follow the instructions on the screen:

   - If you want, restrict the scope to a query item or a measure in the source.

     If the target contains parameters, you should set the scope to the parameters that are mapped to the target report

- Select the target from any package.

  If PowerPlay targets are available, then you must choose whether to set the target as a report or a PowerCube.
- Click **Next**.

8. In the **Action** section, specify how to open the target object when the drill-through link is run and if you chose to run the report, in the **Format** section, specify the format to run the report in.

   Note: Users may be able to change the **Action** settings when they use the drill-through link. If you are using bookmarks in the target, then you must select the action **View most recent report**.
9. In the **Parameter values** table, specify how to map the source metadata to any parameters that exist in the target report or object.

   For example, if you drill through between OLAP data sources, then members are mapped to each other. If you drill through from an OLAP to a relational data source, then the source value (member) is mapped to the query item name (value).

   Usually, every parameter that exists in the target should be mapped to the source metadata. If not, then the report user may be prompted for any missing values when the drill-through link is used.
10. Click **Map to metadata**, or click the edit button ✎.
    - In the screen that appears, select the metadata from the source to map to the target parameter.
    - If the source package is dimensional, you can select what property of the source metadata item to use in the mapping. By default, the business key is used for a relational target, and the member unique name is used for a dimensional target.
    - Repeat for each parameter in the list.
11. In the **Display prompt pages** section, specify when the prompt pages will appear.
    - In the screen that appears, select the metadata from the source to map to the target parameter.
    - If the source package is dimensional, you can select what property of the source metadata item to use in the mapping. By default, the business key is used for a relational target, and the member unique name is used for a dimensional target.
    - Repeat for each parameter in the list.

    You can set this action only when there are parameters in the target report and the target report will be run. If you change the action to **View most recent report**, for example, for bookmark references, the **Display prompt pages** property is disabled because you will use a previously run report. If you choose to open the report directly in Analysis Studio, then the **Display prompt pages** property is also disabled.

    You specify prompt settings in **Report Properties**, **Prompt for Values**.
12. Click **Finish**.
13. Run a report from the source package, and test the drill-through link.

    Note: The drill-through definition is associated and stored with the source. Errors related to the target are only generated when you run the drill-through links, not when you save the drill-through definition.

Related concepts

Report formats

Editing existing drill-through definitions

You can edit existing drill-through definitions.

Procedure

1. On the IBM Cognos Analytics Welcome page, click **New** > **Other** > **Drill-through Definitions**.
2. Click a package name to view its drill-through definitions.

3. For the drill-through definition that you want to modify, in the **Actions** column, click the **Set Properties** ▤ icon.

   Tip: If you do not see the drill-through definitions, check that you are not in a folder in the package. Drill-through definitions are all stored at the root level of the package. If you do not see a specific drill-through definition, confirm that you have the correct permissions.
4. Click the **Target** tab.
5. Make the necessary modifications, and click **OK**.
6. Run a report from the source package, and test the drill-through link.

   Note: The drill-through definition is associated and stored with the source. Errors related to the target are only generated when you run the drill-through links, not when you save the drill-through definition.

Setting Up Parameters for a Drill-Through Report

For greater control over drill-through access, you can define parameters in the target report.

Set up parameters for a drill-through report

For greater control over drill-through access, you can define parameters in the target report.

Procedure

1. Open the target report.
2. Ensure that the report is available for drill-through access:
   - From the **Data** menu, select **Drill Behavior**.
   - In the **Basic** tab, select **Accept dynamic filters when this report is a drill-through target** and then click OK.
3. Create a parameter that will serve as the drill-through column, or that will be used to filter the report. (**Data** menu, **Filters**).

   For example, to drill through or filter on Product line, create a parameter that looks like this:

   ```
   [Product line]=?prodline_p?
   ```

   Tip: Use the operators `in` or `in_range` if you want the target report to accept multiple values, or a range of values.
4. In the **Usage** box, specify what to do when a value for the target parameter is not passed as part of a drill-through:
   - To specify that users must click a value in the source report, click **Required**.

     If a value for the target parameter is not passed, users are prompted to choose a value.
   - To specify that users do not need to click a value in the source report, click **Optional**.

     Users are not prompted to choose a value and so the value is unfiltered.
   - To specify not to use the parameter, click **Disabled**.

     The parameter is not used in the report, and therefore not available for drill-through definitions. For more information about defining report parameters, see the Reporting *User Guide*.

     Tip: If the parameter is needed in the report for other reasons, then you can also specify not to use it in the drill-through definition (**Parameters** table, **Method**, **Do not use parameter**).

Results

The drill-through definition controls when prompt pages or parameters are displayed.

Set up parameters for a drill-through report in Query Studio

For greater control over drill-through access, you can define parameters in the target report in Query Studio.

Procedure

1. Open the target report in Query Studio.
2. Confirm that the report is available for drill-through access:
   - From the menu, select **Run Report**, **Advanced Options**.
   - Select **Enable drill through from a package in the report output** and then click OK.
3. Create a filter that will serve as the drill-through parameter, or that will be used to filter the report.
   - Select the column that you want to filter on, and click the filter button.
   - Change the settings as needed, and click OK.

Set Up Parameters for a Drill-through Target in Analysis Studio

You can create a drill-through target analysis and add target parameters in the analysis by setting a dimension as the Go To parameter.

When you create a drill-through definition for the analysis, this parameter appears in the target parameter list.

To support drilling down within the dimension and then drilling through, map the dimension in the source metadata to the target dimension. The member or members which are currently in your view are passed to the target analysis as filter values. This applies to any query, report, or analysis used in drill-through actions. To support drilling through directly from a particular level, map that level in the source metadata to the target dimension.

You can set multiple parameters in an analysis target. However, you cannot pass members within a selection set in Analysis Studio.

Procedure

1. In Analysis Studio, create a cross-tab analysis using the package that was set up for drill-through analysis.
2. If you want, add as a row or column the data item that you want to be the prompt.
3. Move or add the dimension or level that you want to be a target parameter to the **Context** area.

   Note: You cannot pass members within a selection set in Analysis Studio.
4. View the list for the item in the **Context** area and click **Use as "Go To" Parameter**.
5. Save this analysis as your target report.

   You can now create the drill-through definition under a source package.

Results

When you create the drill-through definition and use the cross-tab analysis as a target, the **Go To** parameter item in the analysis appears as a drill-through parameter.

Debugging a Drill-through Definition

IBM Cognos Analytics includes a debugging functionality that you can use to find problems with your drill-through definitions, and to correct any drill-through errors.

It can also help you understand how the drill-through functionality works, especially across different types of data sources. This functionality is also referred to as the drill-through assistant. You can also debug drill-through definitions that were created in a PowerCube and migrated to IBM Cognos Analytics.

If your target report is not receiving any parameters, check the mapping in your drill-through definition, and ensure that your parameters were created against the correct data type for your drill-through scenario. For example, if you want to create a drill-through definition from an OLAP package to a target report based on a relational package, your target parameters need to be set up to a query item that has the same value as the OLAP business key or the member caption. For more information, see "Members and values" on page 344.

If your target report is being filtered with the wrong values, check the values that are being mapped from the source to the target.

You must have the necessary permissions to use the drill-through assistant. The information that the drill-through assistant provides is available from the **Go To** page, when you run the drill-through. The drill-through assistant provides the following information.

Passed Source Values

The source values are the values from the selection context that are available for passing to the target report when the user chooses to drill through to the target report or object. For example, if you drill through from a source in Analysis Studio, you see the values at the intersection you selected before the drill-through action, and any values in the context area.

The values in the debug list are the values in the source report that were transformed by any drill-through operation.

- Display Value

  Shows the value that users see when using this data item or this member. For OLAP members, this is the member caption or label. For example: `Telephone` is a member from the `Order Method` dimension.

- Use Value

  Shows the value that IBM Cognos reports and analyses use when retrieving the data item or the member. For OLAP members, this is the member unique name (MUN). For example: `[great_outdoors_company].[Order Method].[Order Method].[Order Method1]->:[PC].[@MEMBER].[2]` is the MUN for the `Telephone` member in the `Order Method` dimension.

Target Mapping

If you chose to use parameters in the target, then the target mapping shows the name of each parameter that was mapped in the drill-through definition, and the values that the source is attempting to pass to that parameter.

- Parameter Name

  Shows a list of valid target parameters mapped in the drill-through definition to receive information from the query item, level, or hierarchy on which you performed the drill-through action.

  You can see only parameters for which there is a valid mapping and only the names of the parameters. For example, if the target report contains a parameter for `Product Type` and the drill-through definition maps that target parameter to the source `Product Type` level metadata, you see this target parameter only if you attempt to drill through on the `Product Type` level in the source report. Drilling through on the `Product Line` level does not display this parameter target.

  You must ensure that the target parameters in your drill-through definitions are mapped correctly. Incorrectly mapped parameters can receive information from the wrong source metadata, especially where you have data values that are not unique. If you cannot see any target parameters or the parameters you expected to see in the **View Target Mapping** list, check the parameter mapping in the drill-through definition.

- Display Value

  Shows the value that users see when using a data item or member. For OLAP members, this is the member caption or label. For example: `Telephone` is a member from the `Order Method` dimension

- Use Value

  Shows the transformed value that the drill-through definition uses when passing a data item value or member to the target parameter.

  OLAP members passed to relational target parameters obtain the business key from the members MUN and pass only the business key. Using the example of the `Telephone` member in `Order Methods`, the business key is 2. If you are unsure of what the business key is for a member, you can write an expression such as `roleValue('_businessKey',[member])`. This value is passed to the target parameter.

  OLAP members passed to a target parameter based on another OLAP package of the same OLAP type show a transformed MUN. Using the `Order Methods` example, the MUN is now transformed and the drill-through definition uses the value of `[great_outdoors_company].[Order Method].[Order Method].[Order Method1]-> [Order Method1]. [2]:[PC].[@MEMBER].[2]`. The middle portion of `[Order Method1][2]` is where the drill-through definition finds the correct member in the target when the OLAP data sources are different. To see the MUN for a specific member, you can look at the properties of the member in Reporting and look at the `Member Unique Name` property.

Access the Drill-through Assistant

You can use the drill-through assistant for debugging purposes when you work with drill-through definitions.

Before you begin

To use this functionality, you must have the required permissions for the **Drill-Through Assistant** secured function in IBM Cognos Administration.

Procedure

1. Select a link in your source report, right-click the link, and select **Go To**, or from PowerPlay Studio, click the drill-through button.

   The **Related links** page appears, showing the list of available target reports. If your target report is not shown, review the scope settings in your drill-through definition.

   Tip: If only one target is available, then when you select **Related links**, the target is opened without showing the **Go To** page.
2. Click **View passed source values** to see the values that are available for passing by the source report.
3. Next to the target report, click the down arrow and choose **View Target Mapping**.

   A list of the valid mapped data appears, showing the available source values, and the use and display values.
4. For either set of values, click **More information** to see the XML for the selection context (passed source) or the drill-through specification (target mapping.

Example - Debugging a Drill-through Definition

Here is an example of debugging a drill-through definition.

Your OLAP source has a Products dimension with the levels Line, Type, and Name. You have defined a parameter in your relational target to match each level of that OLAP source dimension. You can have a situation where you see all target parameters from a single dimension displayed in the View Mapped Target list. This is likely because the individual target parameters are mapped to a single dimension in the drill-through definition, in this case the Products dimension. In your OLAP data source, you have a business key value, or the source value used to create the members, that is duplicated in all three levels, as shown in the following table.

Table 78. Example of problematic parameter mapping for drill-through definition

Parameter Name	**Display Value**	**Use Value**
Prod Line Param	Camping Equipment	1
Product Type Param	Cooking Gear	1
Product Name Param	Trail Chef Water Bag	1

Having all three parameters mapped to the Products dimension is correct if the use values are not duplicated in the dimension. In the preceding table, the members from all three levels have the same use value. In this case the drill-through operation cannot determine which level is the correct one because the scenario indicates that all levels are valid. In this situation, the first level encountered with a valid business key or use value is fulfilled by the drill-through definition. This can result in unexpected behavior.

This example shows why it is important to always ensure that your data warehouses and OLAP sources are designed with unique business keys or source values. To correct this situation, the drill-through definition should have each individual target parameter mapped to each associated level in the source metadata rather than in the dimension.

Set Up Drill-through Access in a Report

Use Reporting to create a source drill-through report to link two reports containing related information. You can then access related or more detailed information in one report by selecting a value or multiple values in the source report. You can also drill through within the same report by creating bookmarks.

Before you begin

Tip: To use a report as a source in a drill-through definition, the option **Allow package based drill-through** must be selected (**Data** menu, **Drill Behavior**). This option is selected by default.

Procedure

1. Open the target report.
2. Create a parameter that will serve as the drill-through column or that will filter the report.

   For example, to drill through or filter Product line, create the following parameter:

   [Product line]=?prodline_p?

   Tip: Use the operators `in`or `in_range`to enable the target report to accept multiple values or a range of values.
3. In the **Usage** box, specify what to do when a value for the target parameter is not passed as part of a drill through:
   - To specify that users must select a value, click **Required**.

     If a value for the target parameter is not passed, users are prompted to choose a value.
   - To specify that users do not need to select a value, click **Optional**.

     Users are not prompted to choose a value and so the value is unfiltered.
   - To specify not to use the parameter, click **Disabled**.

     The parameter is not used during the drill-through. It will also not be used in the report for any other purposes.

     Tip: If the parameter is needed in the report for other reasons, then you can also specify not to use it in the drill-through definition (**Parameters** table, **Method**, **Do not use parameter**).

Results

The drill-through text appears as a blue hyperlink in text items in the non-chart areas of the report. Report consumers can also start the drill-through action by clicking the **Go To** button or by right-clicking the item and clicking **Go To**, **Related links**. If you have the necessary permissions, you can view which parameters were passed from the source and how they are mapped in the target object from the **Go To** page using the drill-through assistant.

Specify the drill through text

You can specify the drill through text that appears when users can drill through to more than one target.

For example, if users from different regions view the report, you can show text in a different language for each region.

Procedure

1. Click the drill through object and then, from the **Properties** pane, click **Drill-through definitions**.
2. If more than one drill through definition exists for the object, in the **Drill-through definitions** box, click a drill through definition.
3. Click the **Label** tab.
4. To link the label to a condition, in the **Condition** box, do the following:
   - Click **Variable** and click an existing variable or create a new one.
   - Click **Value** and click one of the possible values for the variable.
5. In the **Source type** box, click the source type to use.
6. If the source type is **Text**, click the ellipsis button that corresponds to the **Text** box and type text.
7. If the source type is **Data item value** or **Data item label**, click **Data Item** and click a data item.
8. If the source type is **Report expression**, click the ellipsis button that corresponds to the **Report expression** box and define the expression.
9. If the label is linked to a condition, repeat steps 5 to 8 for the remaining possible values.

Results

When users run the source report and click a drill through link, the **Go to** page appears. The drill through text you specified appears for each target. If you did not specify the drill through text for a target, the drill through name is used.

Chapter 27. IBM Cognos Workspace

IBM Cognos Workspace is a Web-based tool allows you to use IBM Cognos content and external data sources to build sophisticated, interactive workspaces. For more information about IBM Cognos Workspace, see the IBM Cognos Workspace *User Guide*.

To start Cognos Workspace, from the **Welcome** page, click **New** > **Other** > **Workspace**.

Removing HTML markup from RSS feed details

In IBM Cognos Workspace, a user can insert an RSS widget from the toolbox. After configuring the RSS feed, the RSS feed widget displays HTML markup when the feed details are enabled.

You can hide the HTML markup when the **Show feed details** option is enabled by specifying the advanced setting, **`CPSRssAllowUnsafeCharacters`** on the dispatcher. You must set the parameter for each dispatcher. For multiple dispatchers, you can set the parameter globally.

Procedure

1. In IBM Cognos Administration, click **Configuration** > **Dispatchers and Services**.
2. To specify the **`CPSRssAllowUnsafeCharacters`** setting for a single dispatcher, do the following:
   a) In the **Name** column, click a dispatcher, and click **Set properties**.

   b) Go to the **PresentationService**, and click **Set properties**.

   c) Click the **Settings** tab, and for **Environment**, **Advanced settings**, click **Edit**.

   d) Click **Override the settings acquired from the parent entry**. Now, go to step 4.
3. To specify the **`CPSRssAllowUnsafeCharacters`** parameter globally, for multiple dispatchers, do the following:
   a) On the **Configuration** toolbar, click **Set properties - Configuration**.

   b) Click the **Settings** tab, and for **Environment**, **Advanced settings**, click **Edit**.
4. In the **Parameter** field, type **`CPSRssAllowUnsafeCharacters`**, and in the **Value** field, type **`true`**.
5. Click **OK**.

Results

HTML markup is not displayed in the RSS feed details.

Chapter 28. Cognos Analytics Mobile Reports administration

IBM Cognos Analytics Mobile Reports extends the functionality of your existing IBM Cognos Analytics installation to mobile devices so that users can view and interact with the Cognos Analytics content on their tablets or smartphones.

With the Cognos Analytics Mobile Reports rich client, users can view on their mobile devices the active reports from Cognos Analytics - Reporting and the workspaces from Cognos Workspace. The active reports must exist on the server as saved outputs, or be delivered to the Cognos Analytics Mobile Reports user. Active reports need to be run on the server, not on the client.

The Cognos Analytics prompt functionality and scheduling mechanism are used to deliver customized reports in a timely fashion. Cognos Analytics security and various, vendor-specific security mechanisms, including device-based and server-based security, are used to protect the report and workspace content.

Many of the device-specific management servers and administration tools that are used by Cognos Analytics Mobile Reports offer the ability to remotely remove content from a device or to disable the device completely. For example, if a device is lost or stolen, the Cognos Analytics administrator can use this functionality to protect sensitive content on the device. The Cognos Analytics administrator can also set an expiry date for a report after which the report becomes inaccessible until the user re-authenticates.

Cognos Analytics Mobile Reports supports requests between the mobile device and the server environment for the following product functions:

- Search
- Browse
- Run

The **Mobile** tab in IBM Cognos Administration provides centralized administration capabilities for Cognos Analytics Mobile Reports. To access this tab, the administrator must have the required access permissions for the **Mobile Administration** capability. **Mobile Administrators**, one of the predefined roles in the **Cognos** namespace, can be used to specify access permissions for this capability.

Cognos Analytics Mobile Reports uses the same set of users as Cognos Analytics. For information about administering Cognos Analytics, see other sections in the *IBM Cognos Analytics Administration and Security Guide*.

Pre-configuring the Cognos Analytics Mobile Reports native apps for users

Configure the IBM Cognos Analytics Mobile Reports application to streamline the setup for users and control how the application works on iOS and Android devices.

About this task

You can encode and generate configuration settings in a URL to distribute to Cognos Analytics Mobile Reportse application users in an email message, a chat, or by other methods. With this URL, the users can automatically configure the application on their mobile devices.

The Cognos server URL is included in the configuration so that users do not need to type the URL on their mobile devices when configuring the application.

As an additional security measure, a password can also be included in the configuration. The mobile configuration password provides a tamper-evident seal to ensure integrity of the configuration URL and confirms that the source of the URL is valid. The configuration URL and password should never be transmitted together using the same medium, such as email or chat, at the same time. Users need to enter this password only once when they open the configuration URL.

Procedure

1. In **IBM Cognos Administration**, click the **Mobile** tab.
2. Click **Remote Configuration**.
3. For **IBM Cognos Server URL**, type your IBM Cognos Analytics server URL: `http://`*`server_name`*`:`*`port_number`*`/bi/v1/disp`
4. Enable or disable the following settings:

   Pass-Through Authentication

   Enable this setting so that users can navigate to the Cognos Analytics server through the different intervening web pages that are displayed to them.

   By default, Cognos Analytics Mobile Reports requires direct connectivity with the IBM Cognos Analytics server. If direct connectivity is not possible because of intervening security products, this setting must be enabled. The intervening products could include CA SiteMinder, Tivoli® Access Manager, Microsoft ISA Server, or landing pages in public WiFi networks.

   Automatic Downloads

   Enable this setting for the Cognos Analytics Mobile Reports apps to automatically download new report outputs from the user's inbox and from reports pushed to the user. This setting should be enabled, unless bandwidth is a concern.

   Display Sample Server

   Enable this setting for the Cognos Analytics Mobile Reports apps to access the Cognos Analytics Mobile Reports sample server. The sample server contains sample IBM Cognos reports that illustrate the capabilities of IBM Cognos software. The sample reports are optimized for use in Cognos Analytics Mobile Reports.

   Maintain Application State

   Enable this setting so that the application can restore its latest content space after the application is restarted. For example, if the application is closed while viewing a report in the content space "My Reports", the application reopens the content space "My Reports" after a restart. If this setting is disabled, the application displays the main panel after a restart.

   Default: **Off**
5. Optional: Select the **Mobile Configuration Password** check box and type a password of your choice.

   The password can contain a maximum of 20 alphanumeric characters, and cannot contain spaces.

   If you decide to specify this password, ensure that you provide it to the users separately from the configuration URL.
6. Optional: Select the **SSL/TLS Certificate Pinning** check box and paste the SHA-1 fingerprint of the SSL or TLS certificate that secures the entry point to your Cognos Analytics server. An example of the Cognos Analytics server entry point is a web server, a proxy server, or a load balancer.

   Enable this setting to ensure that the client communicates only with the servers that are configured with the X.509v3 certificate and that have the same SHA-1 fingerprint.

   The value for this setting is a sequence of 40 hexadecimal characters (a-f and 0-9) without any punctuation marks. Remove the punctuation marks from the value before pasting it in this field. You can specify multiple SHA-1 fingerprint values separating them with a colon (:).

   Tip: In Firefox, you can obtain the SHA-1 fingerprint by clicking on the padlock icon in the browser URL bar and then clicking **More Information** > **View Certificate**.
7. Click **Generate Mobile Configuration Code**.

   A base64-encoded URL is generated that includes the specified configuration settings.

The following is an example of the generated URL:

```
cmug://aHR0cDovL3ZvdHRtb2IxL2NzcDI-dmVyc2lvbj0xLjAmcGFzcz1vZmYmYXV0b
2R3bj1vZmYmZGlzcHNhbXA9b24mcHdkPW9uJnNhbHQ9UWlzQVJoTTNPaFVfJmhhc2g9Q
VFnQUFBQkliV0ZqVTBoQk1iV2U3SEJiUjhkczJBV2wrKzI0Y2d6cWxLMi8.
```

8. Copy the configuration URL and provide it to the Cognos Analytics Mobile Reports application users by email, chat, or by other methods.

   Ensure that the following conditions are met when copying and transmitting the URL:

   - All characters in the URL, including underscores (_), are selected when copying the URL.
   - The application that you use to transmit the configuration URL maintains the case of the URL. The URL is case-sensitive.

Results

When users tap on the configuration URL from the administrator, the Cognos Analytics Mobile Reports application is opened on their iOS or Android device. The users must confirm if they want to proceed with automatic configuration. If the mobile configuration password was specified in step 5, the users must enter the password when prompted. The application is then configured with the settings specified in the URL.

If the users enter an incorrect password or tap on the **Cancel** button, the application opens without applying any configuration settings.

Tip: Some email applications deliver the configuration URL to users as plain text. In this situation, the administrators can place the URL on a web page accessible to the users. On iOS, users can also copy and paste the URL into the browser and open it from there.

Specifying Cognos Analytics Mobile Reports advanced settings

You can configure IBM Cognos Analytics Mobile Reports advanced settings globally for all services, for a specific dispatcher, or for a specific Cognos Analytics Mobile Reports service.

When the settings are configured globally, the values that you specify are acquired by all instances of the Cognos Analytics Mobile Reports service. You can override the global values by specifying custom values at the dispatcher or Cognos Analytics Mobile Reports service level.

If the configuration entry contains child entries with settings that override the global settings, the custom settings on the child entries can be reset to use the default values. To reset the value of any setting to its default, delete the setting.

Procedure

1. In IBM Cognos Administration, on the **Configuration** tab, click **Dispatchers and Services** and complete one of the following actions:

   - To configure advanced settings globally, in the toolbar on the **Configuration** page, click the **Set properties - Configuration** icon, and proceed to step 3.
   - To configure advanced settings for a specific dispatcher, find the dispatcher, and in the **Actions** column, click its **Set properties** icon. Then, proceed to step 3.
   - To configure advanced settings for a specific Mobile service, click the dispatcher that includes this service. In the list of dispatcher services, find **MobileService**. In the **Actions** column, click the **Set properties** icon associated with the service, and proceed to step 3.
2. Click the **Settings** tab.
3. For **Advanced settings**, click **Edit**.

   If the parameter is not listed, type its name.

4. Specify the appropriate value for the setting and click **OK**.

   Tip: To delete an advanced setting, select its check box, and click **Delete**.

Configuring a Cognos Analytics Mobile Reports theme

The IBM Cognos Analytics Mobile Reports theme defines the appearance of the Cognos Analytics Mobile Reports application welcome page. By default, the client applications use the default theme that is built into the product. You can create your own Cognos Analytics Mobile Reports theme to customize the appearance of the application and configure the theme to make it available to the user groups and roles that you choose. At any time, administrators can revert to the default theme.

About this task

The configuration tasks include enabling support for Cognos Analytics Mobile Reports themes; adding, editing, or deleting the themes; and defining which groups and roles can use the themes.

The same user can belong to different groups and roles and can, therefore, have access to different themes. To ensure that proper themes are applied for the users, the administrators must carefully consider which groups and roles they can choose when configuring the theme.

The Cognos Analytics Mobile Reports default theme is defined in the `defaultTheme.zip` template that is installed with the product. Administrators can use this template as a starting point when creating a custom theme. Other than that, this template is not required for the product to function properly. For more information, see "Creating a custom Cognos Analytics Mobile Reports theme" on page 361.

Procedure

1. From a desktop browser, log on to IBM Cognos Analytics with mobile administrator privileges.
2. Go to IBM Cognos Administration, and click the **Mobile** tab.
3. Complete the following steps to ensure that theme support is enabled for the Mobile service:
   a) Click **Server Configuration**.
   b) In the **Policy** group of settings, locate the **Mobile theme support** setting and ensure that the value of **themesOn** is specified for this setting.
   c) Click the **Apply mobile configuration** button to save the configuration.
4. Open the **Mobile UI Configuration** page.
5. To add a new theme, click the **New Theme** 📂 icon.
6. In the **Mobile Theme Configuration** page, complete the following steps:
   a) In the **Specify a name for the theme** box, type the theme name. You can specify any name that is meaningful for your environment.
   b) In the **Specify a theme file to upload** box, browse for a zip file that contains the theme resources.
   c) In the **Specify a group or role** box, click the **Choose Group** button and choose the groups or roles that need to use the theme. You can choose groups and roles from the Cognos namespace or from other active namespaces.
   d) Click **OK** when all parameters are properly specified.

   The theme name appears in the **Mobile UI Configuration** page.
7. If you want to edit the theme, click its **Set properties** icon in the **Actions** column. You can edit any of the theme parameters.
8. If you want to delete the theme, select its check box and click the **Delete** icon ❌ in the toolbar.

To revert to the Cognos Analytics Mobile Reports default theme, delete the theme that is currently configured. The users who were using this theme automatically return to using the default theme when they connect to the Cognos Analytics server the next time.

9. Using iOS and Android devices, connect to server for which the theme was configured to test if your changes were properly applied.

Results

The users can continue using the application while the theme resources are downloaded to their devices. The theme is applied when the users connect to the Cognos Analytics server the next time or refresh their application.

When a user wants to connect to multiple servers that might have different themes configured, the theme that is applied for the user is the theme that is configured for the server to which the client successfully connected first. Connecting to other servers does not change the user's theme even if the servers use different themes. To change the theme to the one that is configured for a different server, remove the connection to the server with the current theme. Then, the user can connect to the server that uses the required theme.

Creating a custom Cognos Analytics Mobile Reports theme

You can create a custom IBM Cognos Analytics Mobile Reports theme to replace the default theme that is supplied with Cognos Analytics Mobile Reports.

Before you begin

Plan the design of your custom theme and prepare the required resources, such as image files.

About this task

When Cognos Analytics Mobile Reports is installed, the installation directory `*install_location*/templates/mobile` contains the `defaultTheme.zip` file. This is the default theme template. You can use this template as a starting point when creating your own custom theme.

The `defaultTheme.zip` file contains different directories and files. The `main_panel\index.html` file is the only file that is required for your custom theme. In this file you define all resources, such as images, that you want to use in your custom theme, and modify the color scheme and font styles.

The **nls** directory in the default theme template contains a directory structure for language-specific themes. You can emulate this structure or implement your own mechanism for creating language-specific themes.

You can use the following procedure as a guidance when creating a custom mobile theme based on the default theme.

Procedure

1. Go to the *install_location*`/templates/mobile` directory, make a copy of the `defaultTheme.zip` file, and save it under a different name.
2. Extract the files from the .zip file that you created in the previous step.
3. Edit the `main_panel\index.html` file as required. This file must contain references to all resources that are included with the theme.
4. Compress all of your theme resources in one .zip file. At minimum, the .zip file must contain the modified `main_panel\index.html` file.
5. Save your theme .zip file to a directory of your choice.

   Now, you can configure Cognos Analytics Mobile Reports to use the custom theme. For more information, see "Configuring a Cognos Analytics Mobile Reports theme" on page 360.

Configuring Cognos Analytics Mobile Reports services

You can globally configure all instances of the IBM Cognos Analytics Mobile Reports service.

About this task

Applying the Cognos Analytics Mobile Reports configuration settings globally ensures that all instances of the Cognos Analytics Mobile Reports service are synchronized, which helps to avoid errors.

Important: The settings cannot be customized for different tenants in a multitenant environment.

Procedure

1. From a desktop browser, log on to IBM Cognos Analytics with mobile administrator privileges.
2. Go to IBM Cognos Administration, and click the **Mobile** tab.
3. Click the **Server Configuration** page.
4. Locate the setting that you want to configure and specify its value as required.

   You can configure multiple settings. For a list of settings, see "Cognos Analytics Mobile Reports service configuration settings" on page 362.
5. Click the **Apply mobile configuration** button.

Cognos Analytics Mobile Reports service configuration settings

These settings are used to administer the delivery of IBM Cognos Analytics content to IBM Cognos Analytics Mobile Reports applications.

Policy settings

These settings define how to deliver Cognos Analytics content to Cognos Analytics Mobile Reports.

Maximum number of pages to store for each report

Pages over the specified limit are automatically discarded from the device.

This setting is applicable to drill-through target reports that are launched from IBM Cognos Workspace.

Default: 5

Tip: If your Cognos Analytics Mobile Reports environment includes only native clients, set up the default to 50 pages. Otherwise, use the suggested default of 5.

Maximum number of days to store a report

Specifies the maximum time, in days, that a report is stored in the database. Reports that exceed this limit are automatically removed from the device.

Value: 1 to 999

Default: 30

Maximum number of hours between runs of the source and target reports

Specifies, in hours, the maximum amount of time allowed between the runs of the source and target reports when using the application drill-through feature with active reports in the iOS native app. When the difference between the two runs exceeds this amount, the application drill-through target is not used.

The default value of 1 means that as long as the target report was run within 1 hour after the source report was run, the target report can be opened successfully.

The value of 0 disables the application drill-through functionality. When running the source report after the target report using this value, the target report does not open and an error message is displayed. The error message states that the target report does not exist and needs to be run first.

This setting is not applicable for the Android native app.

Permission to share report screen captures

Allows or disallows the users of a native client to share screen captures of the reports that they are viewing. Users can share report screen captures by email or by other methods.

Value: True or False

Default: True

Cognos Analytics Mobile Reports root folder

Specifies the name of the root folder that Cognos Analytics Mobile Reports users must start from when browsing or searching content from a mobile device.

Default: blank

The value for this setting must be the Content Manager search path in the following format: `/content/package[@name='`*`<root_folder_name>`*`']`.

If the setting is blank, Cognos Analytics Mobile Reports uses the root content folder or the root folder that is specified in the portal system.xml file stored in the *`install_location`*`/templates/ps` directory. If you add a root folder, use the syntax of the `consumer-root` setting in the `system.xml` file.

Tip: To find the search path in IBM Cognos Analytics, view the properties of the package or folder that you want to use as the Cognos Analytics Mobile Reports root folder. Then, click **View the search path, ID and URL**.

Mobile theme support

Specifies if custom mobile themes are supported for the Cognos Analytics Mobile Reports web application.

Values: **`themesOn`** and **`themesOff`**

Default: **`themesOff`**

Maximum number of hours to access Mobile local data stored on a device

Specifies the maximum number of hours when users of mobile devices can access the Cognos Analytics Mobile Reports local data stored on a device.

Value: 0 to 8760

Default: 36

The value of 0 disables the lease key mechanism.

Maximum number of hours to store cached credentials

If you do not want to store credentials on a device, type 0. To store credentials on a device, type any value that is greater than the current timeout setting for IBM Cognos Analytics. As long as users are logged on, they will have access to their cached credentials.

Value: 0 to 8760

Default: 0

Maximum number of hours that the client can remain out of date with scheduled reports

This setting applies to the cases where an administrator schedules reports for a user on the server and the user does not otherwise communicate with the server before the time expires, for example, to retrieve other reports or to browse the IBM Cognos Analytics portal. In the majority of cases, such as when reports originate from existing schedules or from user-initiated actions, this setting will not be a factor because, typically, the device lags behind the server by only seconds.

Value: 0 to 999

Default: 24

The value of 0 pushes reports to be downloaded on devices immediately.

Security settings

These settings are used to secure the Cognos Analytics Mobile Reports application.

Local storage encryption level for IBM Cognos Analytics Mobile Reports applications
Specifies the method by which data that is stored on iOS or Android devices is encrypted.

Values: NONE, AES128, AES256

Default: AES128

Tip: The web application does not store data locally and is not affected by this setting.

Security code session timeout in seconds
Specifies the need for a security code when accessing the Cognos Analytics Mobile Reports application and the maximum number of seconds that the application can remain inactive. The security code cannot contain consecutive or repeated numbers.

Value: 1 to 8760

Default: -1

A value of -1 means that no security code is needed. A value of 0 means that the user must create a security code and enter it every time to access the app.

A value greater than 0 indicates that the user must create a security code and can leave the app inactive for the number of seconds specified in the setting before needing to reenter the code to use the app. For example, if the value is set to 60, the user must enter a security code and can leave the Mobile app inactive for 60 seconds.

Maximum number of attempts to enter a security code when accessing the Cognos Analytics Mobile Reports application
Specifies the maximum number of times that users can try to enter their security code when accessing the Cognos Analytics Mobile Reports application.

Value: 1 to 99

Default: 10

Notification settings

These settings are used to configure Apple push notifications.

Notification email for Apple push notifications
Specifies the email address or addresses of administrators that are notified about the Apple push notifications certificate expiry date.

The value for this setting is an email address in the following format: `*admin*@*domain*.com`. Multiple email addresses must be separated with a semicolon (;). For example, `*admin1*@*domain*.com;*admin2*@*domain*.com`

Support for Apple push notifications
Enables Apple push notifications for the iOS native app, and specifies the wording of the message that is displayed to the iOS device users. The values are:

- None - Apple push notifications are disabled and messages are not sent from the server to the Apple Push Notification Service.
- Name - Apple push notifications are enabled. The messages sent from the server to the Apple Push Notification Service include the report name.
- Generic - Apple push notifications are enabled. The messages sent from the server to the Apple Push Notification Service do not include the report name. Instead, a generic message is displayed.

Default: Name

Frequency check for Apple push notification certificate expiry date in hours

Specifies, in hours, the frequency with which the Cognos Analytics Mobile Reports service checks for the Apple push notifications certificate expiry date. The first check is done when the Cognos Analytics Mobile Reports service is started.

Value: 1 to 8760

Default: 24

Feedback interval for Apple push notifications in hours

Specifies the time interval, in hours, for the Cognos Analytics Mobile Reports server to check the Apple push notifications feedback service for failed notifications. The feedback service maintains a list of devices for which there were repeated, failed attempts to deliver notifications. The Cognos Analytics Mobile Reports server will stop sending notifications to the devices that it obtained from the feedback service.

Values: 1 to 720

Default: 24

Expiry threshold for Apple push notifications in days

Specifies the number of days before the Apple push notifications certificate expiry date when the administrators start receiving emails about the approaching expiry date.

Value: 1 to 365

Default: 14

Configuration of Apple push notifications for the iOS native app

Apple push notifications notify the iOS native app users about the availability of new IBM Cognos Analytics reports.

To send push notifications, the IBM Cognos Analytics Mobile Reports server requires an SSL certificate from Apple. The SSL certificate is included with each released version of Cognos Analytics Mobile Reports, and it is valid for 12 months from the date when it was issued by Apple. The administrator must monitor the certificate expiry date and update the certificate before it expires. Otherwise, the users stop receiving push notifications. For more information, see "Managing the SSL certificate for Apple push notifications" on page 365.

The following TCP ports are used for communication between the Cognos Analytics Mobile Reports server, the Apple iOS device, and the Apple Push Notification Service (APNS):

- Port 2195 is used by Cognos Analytics Mobile Reports server to send notifications to APNS.
- Port 2196 is used by Cognos Analytics Mobile Reports server to reach the APNS feedback service.
- Port 5223 is used by the iOS device connecting to APNS using Wi-Fi.

Keep these ports open in the internet connection firewall.

Managing the SSL certificate for Apple push notifications

The administrator monitors the log files and emails for messages about the approaching certificate expiry date, and updates the certificate when needed.

About this task

The SSL certificate for Apple push notifications is valid for 12 months from the date when it was issued by Apple. Fourteen days before the certificate expiry date, the IBM Cognos Analytics Mobile Reports server starts logging warnings in the *install_location*\logs\mob.log file about the approaching certificate expiry date. To ensure that the warnings about the certificate expiry date are logged, server logging must be set to the Warn level at minimum. When the logging level is set to Error, the certificate expiry messages are not logged.

In addition to the log file warnings, the Cognos Analytics Mobile Reports server can also be configured to send emails to administrators about the approaching certificate expiry date.

The text of the warning in the log file or in the email body, in English only, specifies the certificate expiry date and the URL of the IBM Support website (http://www.ibm.com/support/) where the latest Cognos Analytics Mobile Reports fix pack with updated Apple SSL certificate is available.

Procedure

1. Ensure that the following configuration settings are specified in IBM Cognos Administration. These settings are used to configure the Cognos Analytics Mobile Reports server to send email messages to administrators about the certificate expiry date.

   - **Notification email for Apple push notifications**
   - **Frequency check for Apple push notification certificate expiry date in hours**
   - **Expiry threshold for Apple push notifications in days**

   For more information, see "Enabling Apple push notifications" on page 366.
2. Monitor the log messages and emails for information about the certificate expiry date.
3. To update the certificate, go to the IBM Support (http://www.ibm.com/support) website, and download the latest Cognos Analytics Mobile Reports fix pack that includes a valid certificate for Apple push notifications.
4. Install the new certificate on all affected servers.

Enabling Apple push notifications

The administrator must configure the IBM Cognos Analytics Mobile Reports service settings that are associated with Apple push notifications before users are able to receive push notifications.

About this task

The first time that a push-enabled application registers for push notifications, the users receive an alert asking them if they want to receive notifications. After responding to this alert, the users do not see the alert again unless their device is restored or the application was uninstalled for at least a day. Later, a text alert notifies the iOS device user every time a new report is available and the application icon is updated with the number of new reports. The user can open the application from the notification.

The Cognos Analytics Mobile Reports native iOS app can receive push notifications from multiple Cognos Analytics servers. If users no longer want notifications to be displayed, they must turn off notification settings for the application in iOS settings.

Procedure

1. In IBM Cognos Administration, click the **Mobile** tab.
2. Click **Server Configuration**.
3. Specify the following **Notification** settings:

   Support for Apple push notifications

   Enables Apple push notifications for the iOS native app, and specifies the wording of the message that is displayed to the iOS device users. The values are:

   - None - Apple push notifications are disabled and messages are not sent from the server to the Apple Push Notification Service.
   - Name - Apple push notifications are enabled. The messages sent from the server to the Apple Push Notification Service include the report name.
   - Generic - Apple push notifications are enabled. The messages sent from the server to the Apple Push Notification Service do not include the report name. Instead, a generic message is displayed.

Default: Name

Notification email for Apple push notifications

Specifies the email address or addresses of administrators that are notified about the Apple push notifications certificate expiry date.

The value for this setting is an email address in the following format: `*admin*@*domain*.com`. Multiple email addresses must be separated with a semicolon (;). For example, `*admin1*@*domain*.com;*admin2*@*domain*.com`

Expiry threshold for Apple push notifications in days

Specifies the number of days before the Apple push notifications certificate expiry date when the administrators start receiving emails about the approaching expiry date.

Value: 1 to 365

Default: 14

Feedback interval for Apple push notifications in hours

Specifies the time interval, in hours, for the Cognos Analytics Mobile Reports server to check the Apple push notifications feedback service for failed notifications. The feedback service maintains a list of devices for which there were repeated, failed attempts to deliver notifications. The Cognos Analytics Mobile Reports server will stop sending notifications to the devices that it obtained from the feedback service.

Values: 1 to 720

Default: 24

Frequency check for Apple push notification certificate expiry date in hours

Specifies, in hours, the frequency with which the Cognos Analytics Mobile Reports service checks for the Apple push notifications certificate expiry date. The first check is done when the Cognos Analytics Mobile Reports service is started.

Value: 1 to 8760

Default: 24

4. Click the **Apply mobile configuration** button.
5. Specify the **`Database.DeviceExpiryIntervalDays`** advanced setting for the Mobile service. For more information, see "Specifying Cognos Analytics Mobile Reports advanced settings" on page 359.

Report management on Cognos Analytics Mobile Reports

IBM Cognos Analytics Mobile Reports users can open saved active report outputs or delivered active reports on their mobile devices. The users can run the IBM Cognos workspaces.

Active reports can be delivered to users by using the following methods:

- Scheduling reports to be delivered to the users' devices at specified intervals.
- Sending bursted reports to the users' devices.
- Running a number of different reports as a job and sending them to the users' devices.
- Defining events that trigger a report to run and then be delivered to the users' devices.

Users can delete reports from their devices. If they do this, they delete only the copy on the device, not the actual report.

Cognos Analytics Mobile Reports shortcuts on a mobile device

While you are working with IBM Cognos Analytics Mobile Reports on your device, you can use a number of shortcuts for navigation and to perform other actions.

Table 79. Cognos Analytics Mobile Reports shortcuts on a mobile device

Action	Shortcut
Home	1
End	9
Up	2
Down	8
Left	4
Right	6
Enter	Open
Zoom In	Q
Zoom Out	A
Zoom	Z
Page	P
Mark Cell	5

Cognos Analytics Mobile Reports logging capabilities

Logging for IBM Cognos Analytics Mobile Reports is provided by the product own logging capabilities and by logging capabilities in IBM Cognos Analytics.

Both logging methods produce log files that are used to monitor activities and troubleshoot problems. These files are located in the *install_location*/logs directory. The configuration files located in the *install_location*/configuration directory, with the application tier components, are used to modify the Cognos Analytics Mobile Reports logging capabilities.

Both logging methods can coexist at the same time. For example, the default Cognos Analytics Mobile Reports logging mechanism can be used to track the Cognos Analytics Mobile Reports service activity and the Cognos Analytics logging mechanism can be used to enable debug tracing. Audit logging is available only through the Cognos Analytics logging capabilities.

Events associated with starting and stopping the Cognos Analytics Mobile Reports service are logged in the Cognos Analytics *install_location*/logs/cogaudit.log file.

In addition to the Cognos Analytics Mobile Reports and Cognos Analytics logging capabilities, you can use the iOS and Android diagnostic capabilities to log events associated with the Cognos Analytics Mobile Reports native apps.

Cognos Analytics Mobile Reports logging

IBM Cognos Analytics Mobile Reports records activities related to service startup, configuration setup, and running reports in the mob.log file in the *install_location*/logs directory. This is the default type of logging in Cognos Analytics Mobile Reports.

The logging information that appears in the mob.log file is determined by the *install_location*/configuration/mob.log4j.xml file.

When using the default mob.log4j.xml file, an administrator can monitor the Mobile service for events such as database schema upgrades, Cognos Analytics Mobile Reports service configuration settings and advanced settings changes, and warnings and errors. However, the default mob.log4j.xml file does not include the Debug logging level. If you need this level of logging in your mob.log file, you must enable debugging. For more information, see "Increasing default Cognos Analytics Mobile Reports logging capabilities to debug levels" on page 369.

The following table specifies the logging levels in the mob.log file, from the highest to the lowest level:

Table 80. Logging levels in mob.log

Logging level	Description
`Debug`	Provides debugging information. This level is typically used for debugging specific problems. This level is not available by default and must be enabled. For more information, see "Increasing default Cognos Analytics Mobile Reports logging capabilities to debug levels" on page 369.
`Info`	Provides information about Cognos Analytics Mobile Reports.
`Warn`	Indicates a suspicious occurrence that might warrant further investigation.
`Error`	Indicates a serious error condition that requires intervention.

The level of logging that the user chooses includes all the levels below it. For example, if the user chooses `Info`, then warning and error messages are also written to the log file.

Increasing default Cognos Analytics Mobile Reports logging capabilities to debug levels

You can enable the Debug logging level for the `mob.log` file.

About this task

The default `mob.log4j.xml` file does not include the Debug level logging. To enable debugging, use the *`install_location`*`/configuration/mob.log4j.xml.DEBUG.sample` file.

Procedure

1. Stop the Mobile service in IBM Cognos Configuration.
2. In the *`install_location`*`/configuration` directory, complete the following changes:
   a) Rename `mob.log4j.xml` to `mob.log4j.xml.original`.
   b) Rename `mob.log4j.xml.DEBUG.sample` to `mob.log4j.xml`.
3. Start the IBM Cognos Analytics Mobile Reports service.

Results

Full debug logging is now enabled for Cognos Analytics Mobile Reports.

Enabling Cognos Analytics logging for Cognos Analytics Mobile Reports server

IBM Cognos Analytics Mobile Reports records activities and debugging information as well as information about user and report activity.

About this task

The type of information that is logged in the Cognos Analytics Mobile Reports log files is determined by the logging level defined in the `ipfclientconfig.xml` file in the *`install_location`*`/configuration` directory. The same directory contains the `ipfMOBclientconfig.xml.sample` file. To enable logging, you only need to rename `ipfMOBclientconfig.xml.sample` to `ipfclientconfig.xml`.

The following logging levels can be defined for Cognos Analytics Mobile Reports:

Table 81. Cognos Analytics Mobile Reports logging levels

Logging level	**Description**
`Debug`	Provides debugging information. This logging level is typically used for debugging specific problems.
`Info`	Provides information about IBM Cognos services.
`Warn`	Indicates a suspicious occurrence that might warrant further investigation.
`Error`	Indicates a serious error condition that requires intervention.

The level of logging that the user chooses includes all the levels below it. For example, if the user chooses `Info`, then warning and error messages are also written to the log file.

You can also enable logging in IBM Cognos Administration. For more information, see "Setting up audit logging in IBM Cognos Administration" on page 371.

Procedure

1. Stop the Mobile service in IBM Cognos Configuration.
2. In the `*install_location*/configuration` directory, rename `ipfMOBclientconfig.xml.sample` to `ipfclientconfig.xml`.
3. Open the `ipfclientconfig.xml` file, specify the logging levels that you want, and save the file.
4. Start the IBM Cognos service.

Results

Depending on the logging levels specified in the `ipfclientconfig.xml` file, the following log files are generated in the *install_location*`/logs` directory.

- `ipf-MOB_`*xxxx*`.log`

  This file records Cognos Analytics Mobile Reports audit event information. If a logging database is defined in IBM Cognos Configuration under **Environment**, **Logging**, the audit events are also logged in this database. This type of logging is enabled by default in the `ipfMOBclientconfig.xml.sample` file.

  For information about setting up a logging database, see the *IBM Cognos Analytics Installation and Configuration Guide.*

- `ipfMOBtrace_`*xxxx*`.log`

  This file records Cognos Analytics Mobile Reports trace and debug log data. The type of data captured in this file is the same as the data in the mob.log file. However, this file can be configured to a different logging level to record more or less information. This type of logging is enabled by default in the `ipfMOBclientconfig.xml.sample` file.

- `ipfMOBperf_`*xxxx*`.log`

  This file records Cognos Analytics Mobile Reports performance data. This type of logging is disabled by default in the `ipfMOBclientconfig.xml.sample` file.

Setting up audit logging in IBM Cognos Administration

Use audit logs to view information about IBM Cognos Analytics Mobile Reports user and report activity.

About this task

Examples of actions recorded in audit logs include user logon and logoff times, expired user sessions, scheduled report delivery, saved output, and so on.

You can also enable audit logging in the `*install_location*/configuration/ipfclientconfig.xml` file. For more information, see "Enabling Cognos Analytics logging for Cognos Analytics Mobile Reports server" on page 369.

For more information about audit reporting, see the *IBM Cognos Analytics Administration and Security Guide*. This document also contains information about the sample Cognos Analytics Mobile Reports audit reports.

Procedure

1. Open Cognos Administration.
2. On the **Configuration** tab, click **Dispatchers and Services**.
3. Click the dispatcher name.
4. In the list of the dispatcher services, find the **MobileService**, and in the **Actions** column, click its **Set properties** icon.
5. Click the **Settings** tab, and under **Category**, choose **Logging**.
6. For **Audit logging level for mobile service**, select any value except for **Minimal**.

   The following logging levels can be specified to enable audit logging: **Basic**, **Request**, **Trace**, and **Full**. The **Minimal** logging level disables audit logging.
7. Click **OK**.
8. To apply the value, stop and restart the IBM Cognos service.

User diagnostics

Users can turn logging on and off in their native iOS and Android apps and choose the level of logging detail that is captured.

The following list shows the supported levels of logging, from the highest to the lowest level:

- Network
- Debug
- Info
- Warning
- Error

The level of logging that the user chooses includes all the levels below it. For example, if the user chooses Info, then Warning and Error messages are also written to the log file.

The maximum size of a logged message is 2 KB. If a message exceeds this size, it is truncated.

iOS applications

When logging is turned on, a directory named `SupportArtifacts` is created in the application documents directory. A file named `mobile_ios.log` is created in the `SupportArtifacts` directory. All logged events are written to this file.

The maximum size of an active log file is 1 MB. When this size is reached, the active log file contents are moved to a file named `mobile_ios.log.old`. If a `mobile_ios.log.old` file exists, it is removed first. A new `mobile_ios.log` file is created and becomes the active log file.

When logging is disabled, the directory and all its contents are removed from the application documents directory.

Android applications

When logging is turned on, a directory named `SupportArtifacts` is created in the `/Android/data/com.ibm.cogmob.artoo/files` directory. A file named `cogmob.log` is created in the `SupportArtifacts` directory. All logged events are written to this file.

The maximum size of an active log file is 1 MB. When this size is reached, the active log file contents are moved to a file named `cogmob.log.old`. If the `cogmob.log.old` file already exists, it is removed first. A new `cogmob.log` file is created and becomes the active log file.

When logging is disabled, the directory and all its contents are removed from the application documents directory.

Cognos Analytics Mobile Reports samples

The IBM Cognos Analytics samples include active reports that are optimized for use with IBM Cognos Analytics Mobile Reports on a mobile device.

Cognos Analytics Mobile Reports users can try out the interactive functionality of active reports. These reports let users compare different areas of their business to determine trends, for example, over time, by region, by departments or in combination, or compare business methods and statistics.

Cognos Analytics Mobile Reports sample active reports demonstrate the following product features.

- Interactive behavior between controls.
- Access to Details on Demand by leveraging drill-down functionality.
- Conditional palette and drill-down to details from a chart.
- Specific design tablet gestures, such as swiping and scrolling.
- Particular user interface design, such as cover page and color palette.
- Different type of active report items, such as Deck, Tab Control, Chart, Buttons, Drop-down list, Iterator and Slider

GO Data Warehouse (analysis) package

The GO Data Warehouse (analysis) package includes the following active reports.

Core products results
This active report shows revenue data for the core products Camping Equipment and Golf Equipment.

Financial report
This active report shows current performance and changes in the financial position of an enterprise. This type of information is useful to all users who are involved in making business decisions. However, the Finance department is most likely to benefit from this information when implementing the checks and controls in the system to comply with legal, tax, and accounting regulations and requirements, and when providing advice about future directions, performance, and opportunities for the business. This report is optimized for tablets.

Inventory turnover report
This active report shows information about the regional product inventory turnover, based on two years of comparative data. The report provides key inventory metrics that a company might use to manage its inventory. You can drill down on each product category to view the detailed inventory information and the number of failed orders related to the inventory. This report is optimized for tablets.

Sales target by region
This active report shows sales target by region, including the percentage differences between planned and actual revenue.

GO Data Warehouse (query) package

The GO Data Warehouse (query) package includes the following active reports.

Advertising-cost vs revenue
This active report shows the advertising cost vs revenue by year. Tab controls are used for grouping similar report items.

Customer Satisfaction
This active report compares the number of returns by customers by order method and region. The report provides additional information about the order method with the highest number of returns. It also shows customer survey results for different regions. This report is optimized for tablets.

Employee Recruitment
This active report compares the effectiveness of various employee recruitment methods for each department and country or region. It shows the organization names, positions filled, planned positions, and a bulleted chart of positions filled versus planned positions. This report is optimized for tablets.

Revenue by Product
This active report shows the revenue by selected product. This report is optimized for mobile phone devices.

Cognos Analytics Mobile Reports security

IBM Cognos Analytics Mobile Reports combines the security measures of IBM Cognos Analytics with the extra measures needed for mobile devices.

The security measures offer protection against loss and theft and against unauthorized access to the wireless network. The security applies whether the device is used in connected or disconnected mode.

The Cognos Analytics Mobile Reports solution includes the following security measures that are implemented in the IBM Cognos and device-specific environments:

- Standard IBM Cognos data encryption
- Standard IBM Cognos authentication, including support for custom IBM Cognos authentication providers
- PKCS12 certificates
- Lease key technology
- Device user authentication policies
- Device-based mobile encrypted database
- Standard device-specific secure data transmission and encryption
- Device-based password protection
- Remote device wiping

Cognos Analytics Mobile Reports supports web servers that are configured to use basic authentication, such as Microsoft Windows NTLM, Microsoft Active Directory, and some configurations of CA SiteMinder. These types of authentication allow an application to cache user credentials if the administrator enables the user credential cache option. For all other types of authentication, such as the HTML server response page, the application displays a page that allows the user to interact with the page, as intended by the authentication provider.

Note: For single sign-on security configurations, the user credential cache option is not available.

Cognos Analytics Mobile Reports supports single sign-on security configuration. Typically, however, mobile device users are not pre-authenticated against security domains in the same way that desktop users are. As a result, mobile device users usually must provide their single sign-on credentials each time they access the Cognos Analytics server.

Important: The Cognos Analytics Mobile Reports iPad application also supports single sign-on security configurations. Users can enable single sign-on from their iPad **Settings** by turning on the **Pass-through**

authentication setting for the IBM Cognos application. When this setting is enabled, the iPad users are prompted for sign-on credentials each time they access the Cognos Analytics server.

In some cases, logon credentials can be cached on the mobile device so that the user must log on only once to access both the device and Cognos Analytics Mobile Reports.

Note: Credentials can be cached only when the **Pass-through authentication** setting is off. For single sign-on security configurations, therefore, the option to cache user credentials is not available.

Cognos Analytics Mobile Reports offers encrypted database technology as the content store on the device. Access to local device storage is controlled by a centrally-granted lease key that must be renewed periodically. You can configure the length of the lease, so that if the device is lost or stolen, the data will be inaccessible.

You can have different levels of security, depending on the needs of your organization. In addition to storing logon credentials on the device, you can allow anonymous logon or rely on the network security features of the mobile device.

For a higher level of security, you can use Cognos security for all communication or use lease key technology to control access to data.

For information about Cognos Analytics security, see Chapter 10, “Security Model,” on page 161. For information about device security, see the documentation for that device.

Cognos Analytics Mobile Reports capabilities

The IBM Cognos Analytics Mobile Reports capabilities in IBM Cognos Administration are used to restrict access to Cognos Analytics Mobile Reports for users and administrators.

Tip: The IBM Cognos Analytics capabilities are also referred to as secured functions and features.

The Cognos Analytics Mobile Reports capabilities include:

- **Mobile**

  This secured function is used to restrict access to Cognos Analytics Mobile Reports for users. Only users, groups, or roles that have execute permissions for this secured function can log on to Cognos Mobile. When users who do not have the required permissions try to log on, they see an error message asking them to contact a Cognos Analytics administrator.

- **Mobile Administration**

  This secured feature of the **Administration** secured function is used to restrict access to the administration pages on the **Mobile** tab in Cognos Administration. Only users, groups, or roles that have execute permissions for this secured feature can access this tab to perform administration tasks, such as Mobile service configuration, for Cognos Analytics Mobile Reports.

To simplify the process of setting access permissions for the **Mobile** and **Mobile Administration** capabilities, you can use the predefined roles **Mobile Users** and **Mobile Adminsitrators** that exist in the **Cognos** namespace in Cognos Administration. The **Mobile Users** role contains permissions that are needed for access to Cognos Analytics Mobile Reports for regular users. The **Mobile Adminsitrators** role contains permissions that are needed for access to Cognos Analytics Mobile Reports administrative functions on the **Mobile** tab in Cognos Administration. You can add users, groups, or roles from your organization directory to these roles and include these roles in your Cognos Analytics security policies. You can also ignore these roles, or delete them, and create your own security groups or roles to use for setting access permissions to Cognos Analytics Mobile Reports.

Setting access permissions for the **Mobile** and **Mobile Administration** capabilities is one of the initial tasks that an administrator must perform when configuring Cognos Analytics Mobile Reports. For more information, see Chapter 13, “Capabilities,” on page 185.

Password protection

Typically, organizations want to have password protection on mobile devices.

After a specified period of inactivity, users are prompted to reenter their device password and there may be a limit on the number of times they can try to enter a password. When the limit is reached, the mobile device is reset, removing all data from the device. The user must then take the appropriate actions to restore the data on the device.

You can store IBM Cognos credentials for users on their mobile devices so that they need to enter their credentials only the first time they access IBM Cognos Analytics Mobile Reports. After that, they are still asked for their credentials each time they log on, but Cognos Analytics Mobile Reports automatically enters their passwords for them. Only when the time limit is reached on the stored credentials, users need to reenter their credentials.

If a device PIN is configured on an iOS device, Cognos Analytics Mobile Reports encrypts the manually imported Cognos active reports that are stored on the device. This feature applies to active reports that are manually imported through email, iTunes, or a file server.

For information about how to enable or set password policies for a mobile device, see the documentation for the device.

HTML and HTTP support during logon

The IBM Cognos Analytics Mobile Reports product used on mobile devices is a native application, as opposed to a web application. It does not use a web browser, and does not use HTML to display reports on mobile devices.

However, Cognos Analytics Mobile Reports does use HTTP to communicate with the IBM Cognos Analytics server, and so it must interoperate with any web-based security mechanisms that govern access to the Cognos Analytics server. To allow users to authenticate and to navigate through these security mechanisms, Cognos Analytics Mobile Reports shows basic HTML form elements and allows the user to perform the actions associated with them.

The following table shows the HTTP and HTML functions that are supported by Cognos Analytics Mobile Reports.

Table 82. HTTP and HTML functions supported by Cognos Analytics Mobile Reports

Function	Description
HTTP Redirects	Supports HTTP 301 Moved Permanently and HTTP 302 Moved Temporarily. It will follow both relative and absolute URLs given in the Location header.
HTML Redirects	Supports the HTML equivalent of an HTTP redirect, for example <meta http-equiv="Refresh" content="3;URL=http://...">.
HTTP Authentication	Supports HTTP 401 Unauthorized both with the basic scheme and with NTLM. NTLM is predominantly a Microsoft authentication scheme, known also as Windows Integrated Authentication.
HTML Forms	Shows the text of an HTML page (including text with anchor tags), buttons, and the input field types text, password, and hidden. It also shows the select input type, which is used to show a list of items that you can choose from, such as a list of security namespaces.

Certificate authentication

If your web server is configured to require client certificate authentication, you can use a client SSL certificate (client X509v3 certificate) to provide a seamless signon and secure communication between the IBM Cognos Analytics server and the native apps.

Tip: This type of authentication is also known as two-way SSL authentication or mutual authentication.

The certificate file must be in the PKCS12 format (extension .pkcs12) and must contain the identity of the client, in the form of a certificate and a private key. An administrator must set up a secure mechanism for importing the certificate file into the native apps and provide the certificate password to the users so that they can enter it when importing the certificate.

An administrator can provide the following mechanisms to import the client SSL certificate for IBM Cognos Analytics Mobile Reports iOS and Android apps:

- A link to the certificate file from a website.

  An administrator must direct users to a website that contains a link to the .pkcs12 file. Users tap on the link to import the file into the app. On Android devices, the users are prompted to save the file.
- An email with the attached certificate file.

  Users must download the attached .pkcs12 file. On Android devices, the users are prompted to save the file.
- Copying the certificate file to the device.

  In this scenario, the mobile device is tethered to a personal computer. For Android, the .pkcs12 file can be manually copied from the personal computer, to which an administrator securely supplies the file, to the mobile device. For iOS, the administrator or user can provide the .pkcs12 file through iTunes, by placing the file in the **IBM Cognos Documents** folder.

  This method is not scalable and useful only to resolve one-time issues or perform one-time setups.

When selecting the .pkcs12 file on their mobile devices, users must select **IBM Cognos Analytics Mobile Reports** from the **Open With** dialog box. The users are then prompted for the password associated with the .pkcs12 file in the **Client Certificate** dialog box. After the app opens, the certificate is stored in the password storage system, such as Keychain on iOS devices, on the user's mobile device.

Tip: On Android, if the Gmail app is unable to open a PKCS12 certificate, a possible workaround is to use another mail client, such as the default Email app. If that is not possible, using the .p12 certificate extension might allow the app to import it properly. When importing a certificate through a hyperlink, the .pkcs12 extension should be used.

Cognos Analytics Mobile Reports application security

A security code can be used to restrict access to the IBM Cognos Analytics Mobile Reports app for users of iOS and Android devices.

The Cognos administrator can specify that a mobile device user must enter a security code to access the Cognos Analytics Mobile Reports app, and the amount of time that the Cognos Analytics Mobile Reports app can remain inactive before the user must reenter the code to use the app. This functionality is controlled by the **Security code session timeout** configuration setting.

If the value of this setting indicates that the user needs a security code, this value also represents the number of seconds that the Cognos Analytics Mobile Reports app can remain inactive before the user is prompted to reenter the security code to access the Cognos Analytics Mobile Reports app.

In addition to this setting, there is also a default timeout value that is included with the Cognos Analytics Mobile Reports native apps. The value that you specify for the server setting overrides the default value in the app.

The users can turn off the server setting on their mobile devices, but they cannot change its value. If the setting is off, but the server setting requires the user to use a security code, the next time the user tries to run the app, he or she needs to re-authenticate with the server and is prompted to create a security code. Without this code, the users cannot see any local content.

The Cognos administrator can also set a limit on the number of failed attempts to enter the security code when logging on to the Cognos Analytics Mobile Reports apps. This is controlled by the **Maximum number of attempts to enter a security code when accessing the Cognos Analytics Mobile Reports application** configuration setting. If the user exceeds the maximum number of attempts, all Cognos content on their mobile devices is destroyed. If the user needs a PIN to access the server, the number of retries specified by the server overrides the retry value on the mobile device.

For more information, see the security settings in "Cognos Analytics Mobile Reports service configuration settings" on page 362.

Report data security in IBM Cognos Analytics Mobile Reports

All compiled and compressed versions of IBM Cognos Analytics reports are encrypted and stored locally in the mobile encrypted database of the mobile device. These reports can be read or otherwise interpreted only by the IBM Cognos Analytics Mobile Reports client application.

You can use lease key technology to set an expiry time for report data that is stored on the mobile device. After the expiry time, the report data cannot be accessed on the device until the device can reestablish communications with the server, and the user is able to re-authenticate with the server.

If a device PIN is configured on an iOS device, Cognos Analytics Mobile Reports encrypts the manually imported Cognos active reports that are stored on the device. This feature applies to active reports that are manually imported through email, iTunes, or a file server.

Erasing content from a device

You may need to erase all content from a mobile device. This may be necessary if a device is lost or stolen or an employee changes roles or leaves the company.

Device passwords and lease key technology ensure that content is available only to authorized users. For all devices, security and management is handled by third-party mobile device management solutions.

If IBM Cognos Analytics Mobile Reports is not connected to the server for a predetermined period of time, based on the hours specified in the **Maximum number of hours to access Mobile local data stored on a device** configuration setting, IBM Cognos data becomes inaccessible from the device. For more information about configuration settings, see "Cognos Analytics Mobile Reports service configuration settings" on page 362.

Setting a lease key

Cognos Analytics Mobile Reports uses the concept of a lease to govern access to data that is stored on mobile devices.

Data is leased from the server for a length of time controlled by the IBM Cognos administrator through the server setting named **Maximum number of hours to access Mobile local data stored on a device**. This setting specifies the maximum amount of time that a user can access data on a mobile device that is not in contact with the server. For example, the device is offline or out of wireless range. If the device is unable to renew its lease within the specified period of time, the data on the device becomes inaccessible. Valid range of values for this setting, in hours, is 0 to 8760. The default is 36 hours. The value of 0 disables the lease key mechanism. For information about specifying this setting, see "Configuring Cognos Analytics Mobile Reports services" on page 362.

Setting user authentication policies for a mobile device

Cognos Analytics Mobile Reports device user authentication policies define whether IBM Cognos Analytics authentication credentials are cached on the mobile device and how often users must reenter these credentials. Users must enter their credentials at least once.

All IBM Cognos Analytics timeouts apply to the mobile device user. The device user authentication policies are on top of timeouts associated with IBM Cognos Analytics.

To simplify the authentication process for the user, the IBM Cognos administrator can allow credentials to be cached on the mobile device by using the setting **Maximum number of hours to store cached credentials**. The range of values for this setting, in hours, is 0 to 8760. The default value of 0 means that you do not want to store credentials on a device. For information about specifying this setting, see "Configuring Cognos Analytics Mobile Reports services" on page 362.

The CAM (IBM Cognos security control mechanism) passport setting in IBM Cognos Analytics applies to all devices. When the passport setting limit expires, the user session ends. However, if the device authorization time limit exceeds the timeout that ended the session, the device authorization time limit remains in effect after the user session ends. Only when the device authentication time limit is reached, users need to reenter their credentials.

Procedure

Use the following procedure to set the timeout for the CAM passport.

1. Open **IBM Cognos Configuration** on the computer where IBM Cognos Content Manager is installed.
2. In the **Explorer** pane, click **Explorer** > **Authentication**.
3. In the **Properties** pane, for **Inactivity timeout in seconds**, type the required value.

   For more information about IBM Cognos Configuration, see the *IBM Cognos Analytics Installation and Configuration Guide*.

Appendix A. Accessibility features

IBM Cognos Administration has accessibility features that help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products.

The availability of accessibility features can vary however, if other pages and components that do not support accessibility are added to the Cognos Administration user interface.

For more information about the commitment that IBM has to accessibility, see the IBM Accessibility Center (http://www.ibm.com/able).

The following features support accessibility in Cognos Administration:

- To listen to what is displayed on the screen, people with limited vision can use screen-reader software, along with a digital speech synthesizer. Cognos Administration uses Web Accessibility Initiative-Accessible Rich Internet Applications (WAI-ARIA).
- To navigate in the software and to issue commands by using only a keyboard, you can use standard Microsoft Windows keyboard shortcuts. There are no unique keyboard shortcuts.
- To bypass links in headers and menus and to go directly to the main content of the page, JAWS users can select the **Skip to main** link in the list of links window. Keyboard users see the **Skip to main** option if they navigate to it.
- Administrators can specify system-wide settings for accessible report output that apply to all entries.
- Accessible output can also be set for individual reports, jobs, steps within jobs, and scheduled entries in PDF, HTML, and Microsoft Excel 2007 software formats.

Enabling system-wide accessible report output

You can specify system-wide settings for accessible report output that apply to all entries, including reports, jobs, and scheduled entries.

Accessible reports contain features, such as alternate text, that allow users with disabilities to access report content using assistive technologies, such as screen readers.

Accessibility settings in the user preferences and report properties can overwrite the system-wide settings in IBM Cognos Administration.

Accessible reports require more report processing and have a larger file size than non-accessible reports. Consequently, accessible reports affect performance. By default, support for accessible report output is disabled.

Accessible report output is available for the following formats: PDF, HTML, and Microsoft Excel.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Dispatchers and Services**.
2. From the **Configuration** page toolbar, click the set properties button ▤.
3. Click the **Settings** tab.
4. From the **Category** drop-down list, click **Administrator Override**.
5. For the **Administrator Override** category, next to **Accessibility support for reports**, in the **Value** column, click **Edit**.
6. In the **Accessibility support for reports** page, select one of the following options:

Option	Description
Disable	Accessible report output is not available to users.
Make mandatory	Accessible report output is always created.
Allow the user to decide	Accessible report output is specified by the user. If you set this option to **Not selected**, then accessible report output is not created automatically. This is the default. If you set this option to **Selected**, then accessible report output is created by default.

Cognos Analytics Mobile Reports accessibility features

IBM Cognos Analytics Mobile Reports is fully accessible on iOS 7 and greater devices. On these devices, when the **VoiceOver** feature is enabled, it acts as a screen reader. Users can then navigate with a Bluetooth keyboard or with screen gestures by using standard Apple keyboard shortcut commands. For more information, see your device documentation.

Cognos Analytics Mobile Reports includes extra keyboard shortcuts to help you navigate in different views.

Keyboard shortcuts in Cognos Analytics Mobile Reports

Keyboard shortcuts are defined for different views in IBM Cognos Analytics Mobile Reports.

Keyboard shortcuts are defined for the following screens, spaces, and views:

- Cognos Analytics Mobile Reports home screen.
- My Reports, Imported Content, and Samples spaces.
- Browse and Search views.
- Report viewer.
- **Enter Security Code** window.

Cognos Analytics Mobile Reports home screen

When the **VoiceOver** feature is enabled on your iOS mobile device, you can use IBM Cognos Analytics Mobile Reports keyboard shortcuts to navigate IBM Cognos Analytics in the Cognos Analytics Mobile Reports home screen.

In the Cognos Analytics Mobile Reports home screen, use the following keyboard shortcut to perform the following action:

Table 83. Cognos Analytics Mobile Reports home screen keyboard shortcuts

Action	Keyboard shortcut
If a space connection has focus, open the Delete window.	Ctrl+D

My Reports, Imported Content, and Samples spaces

When the **VoiceOver** feature is enabled on your iOS mobile device, you can use Cognos Mobile keyboard shortcuts to navigate IBM Cognos Analytics in the My Reports, Imported Content, and Samples spaces.

Keyboard shortcuts trigger different actions that depend on which mode you are in. The modes are default and edit.

Default mode

In default mode, use the following keyboard shortcuts to perform the following actions:

Table 84. My Reports, Imported Content, and Samples spaces, default mode keyboard shortcuts

Action	Keyboard shortcut
Exit or minimize a space.	Ctrl+X
Open browse and search views (My Reports space only).	Ctrl+B
Refresh the list of reports.	Ctrl+R
Edit the space title.	Ctrl+T
Open or close the user authentication settings (My Reports space only).	Ctrl+A
Open or close the wallpaper background settings.	Ctrl+W
Enter or exit the report preview mode.	Ctrl+P
Enter edit mode.	Ctrl+D

Edit mode

In edit mode, use the following keyboard shortcuts to perform the following actions:

Table 85. My Reports, Imported Content, and Samples spaces, edit mode keyboard shortcuts

Action	Keyboard shortcut
Return to default mode when you have finished editing.	Ctrl+D
Select all if none are selected, or select none when all are selected.	Ctrl+A
Swap a report with focus with the next report (retains focus on the moved report).	Ctrl+S
Delete the selected reports and return to default mode.	Delete

Browse and search views

When the **VoiceOver** feature is enabled on your iOS mobile device, you can use Cognos Mobile keyboard shortcuts to navigate IBM Cognos Analytics in the browse and search views.

In the My Reports space, you can browse and search. In the browse and search views, use the following keyboard shortcuts to perform the following actions:

Table 86. Browse and search views keyboard shortcuts

Action	Keyboard shortcut
Close the browse or the search view.	Ctrl+X
Refresh the current browse or search page.	Ctrl+R
Move to the next page.	Opt+left or right arrow
If the **Saved Output** window is open, close it.	Return or Enter

Report viewer

When the **VoiceOver** feature is enabled on your iOS mobile device, you can use Cognos Mobile keyboard shortcuts to navigate IBM Cognos Analytics in the report viewer.

In the My Reports space, you view reports in the report viewer. Keyboard shortcuts trigger different actions that depend on which mode you are in. The modes are default and draw.

Default mode

In default mode, use the following keyboard shortcuts to perform the following actions:

Table 87. Report viewer, default mode keyboard shortcuts

Action	Keyboard shortcut
Close or minimize the report viewer. When drilling through, go back to the source.	Ctrl+X
Open or close the page picker.	Ctrl+P
Open or close the actions menu.	Ctrl+A
Enter draw mode.	Ctrl+D
Go to the next page.	Ctrl+. (>)
Go to the previous page.	Ctrl+, (<)

Draw mode

In draw mode, use the following keyboard shortcuts to perform the following actions:

Table 88. Report viewer, draw mode keyboard shortcuts

Action	Keyboard shortcut
Discard changes and exit draw mode.	Ctrl+D
Share a report with annotation.	Ctrl+M
When the Draw Box menu is open, increase the Draw Box width by 10 pixels.	Ctrl+W
When the Draw Box menu is open, decrease the Draw Box width by 10 pixels.	Ctrl+Shift+W
When the Draw Box menu is open, increase the Draw Box height by 10 pixels.	Ctrl+H
When the Draw Box menu is open, decrease the Draw Box height by 10 pixels.	Ctrl+Shift+H
When the Draw Box menu is open, exit the Draw Box menu.	Ctrl+X

Enter Security Code window

When the **VoiceOver** feature is enabled on your iOS mobile device, you can use Cognos Mobile keyboard shortcuts to navigate IBM Cognos Analytics in the **Enter Security Code** window.

Use the following keyboard shortcuts to perform the following actions:

Table 89. Enter Security Code window keyboard shortcuts	
Action	**Keyboard shortcut**
Input your PIN.	Numbers on the keyboard
Clear the last number that you input.	Delete

Known issues

IBM Cognos Analytics Mobile Reports includes keyboard shortcuts to help you navigate and perform tasks in IBM Cognos Analytics by using only a keyboard. However, you might encounter known issues with the iOS **VoiceOver** feature.

When viewing report content Cognos keyboard shortcuts do not work

When the **VoiceOver** feature is enabled and you view report content such as the report content in the report viewer, or in the IBM Cognos Analytics Mobile Reports home screen, the Cognos Analytics Mobile Reports keyboard commands do not work. To resolve this issue, move the focus cursor back into the toolbar area.

Keyboard listener stops working when an item is tapped

When you view report content in the IBM Cognos Analytics Mobile Reports application, if you tap on an item, the **VoiceOver** feature stops working. The workaround is to turn the **VoiceOver** feature off and on again, or to navigate to another view and then return to the original view to reset the **VoiceOver** feature.

Delete key does not work in text input fields

If you are in **VoiceOver** mode, the delete key does not work in text input fields in the IBM Cognos Analytics Mobile Reports application. If you make a mistake and want to backspace to delete a character, use the keyboard shortcut, Ctrl+Delete.

Appendix B. Round Trip Safety Configuration of Shift-JIS Characters

Shift-JIS is a character encoding system for Japanese characters. It is equivalent to ASCII, a character encoding system for English characters.

Native Encoding and Unicode

Because Shift-JIS and ASCII both define characters for one language, they are native encoding systems. Unicode is a character encoding system that defines characters for all languages. Because software is used in a global, multilingual environment, characters for processing by computers must often be converted between native encoding systems and Unicode.

Round Trip Safety

Issues associated with conversions between native encoding systems and Unicode are referred to as round trip safety issues.

Using Unicode, applications are developed that can handle input from different languages at the same time. Input data, which is entered by users or retrieved from databases, may contain characters encoded in a native encoding system. For example, in Microsoft Windows operating system, English characters input by a user are encoded using Windows-1252.

When an application receives characters in a native encoding system, it converts the characters into Unicode for processing. After the processing is finished, the characters may be converted back into the native encoding system.

In most cases, the characters are converted without ambiguity because each native character is mapped to a single Unicode character. If the conversion of a native language character to and from Unicode results in the original character, the character is considered round trip safe.

For example, the character "A" is round trip safe in Windows-1252, as follows:

- The Windows-1252 character for "A" is 0x41.
- It converts to Unicode U+0041.
- No other Windows-1252 character converts to the same Unicode character, so it always converts back to 0x41.

Issues Specific to Shift-JIS

Although the characters from most native character encoding systems are round trip safe, the Shift-JIS encoding system is an exception. Approximately 400 characters in Shift-JIS are not round trip safe because multiple characters in this group can be mapped to the same Unicode character. For example, the Shift-JIS characters 0x8790 and 0x81e0 both convert to the Unicode character U+2252.

IBM Cognos Analytics and Shift-JIS

IBM Cognos Analytics uses Unicode. The round trip safety of characters is essential to ensure the accuracy of data in generated reports.

The Round Trip Safety Configuration utility ensures the round trip safety of Shift-JIS characters only when it is used both to convert characters:

- from Shift-JIS to Unicode
- from Unicode to Shift-JIS

If data is requested from a database that has its own automatic mechanism for Shift-JIS to Unicode conversion, IBM Cognos Analytics does not call the Round Trip Safety Configuration utility to convert the characters from Unicode to Shift-JIS. The round trip safety of characters in the data cannot be ensured.

For more information on The Round Trip Safety Configuration utility, see "The Round Trip Safety Configuration Utility" on page 386.

Example: Safe Conversion of Shift-JIS

The following example illustrates the problem with Shift-JIS conversion to Unicode:

- A database contains characters encoded in Shift-JIS.
- A record in the database contains the Shift-JIS character 0x8790.
- A user enters the Shift-JIS character 0x8790 into a data entry form in a browser.
- The application receives the input form and converts the Shift-JIS character 0x8790 to the Unicode character U+2252.
- Because the database contains Shift-JIS encoded characters, the Unicode character U+2252 cannot be specified as part of the query.
- The application must convert U+2252 back to a Shift-JIS character. Both 0x8790 and 0x81e0 convert to U+2252. If the conversion process selects 0x81e0, the query returns no records.

To resolve this problem, you can use the Round Trip Safety Configuration utility to ensure that conversion is to 0x8790 and the record is found.

The Round Trip Safety Configuration Utility

You can use the Round Trip Safety Configuration utility to configure the conversion process of Shift-JIS characters so that IBM Cognos Analytics always returns the right records.

This utility gives you control over the following two situations:

- More than one Shift-JIS character converts to the same Unicode character.

  If your data contains such Shift-JIS characters, you can use the utility to specify that the Unicode character always converts to the required Shift-JIS character. For more information, see "Specify Conversions" on page 386.
- More than one Unicode character represents the same or similar character after conversion.

  Such Unicode characters can be considered identical when processed by computers and can be substituted for one another. You can use the utility to ensure that the correct substitution is made. For more information, see "Specify Substitutions" on page 387.

Specify Conversions

If your data contains more than one Shift-JIS character that converts the same Unicode character, use the Round Trip Safety Configuration utility to specify that the Unicode character always converts to the required Shift-JIS character.

Before you choose the Shift-JIS character to use in a conversion, determine which Shift-JIS character is currently used in the environment. Only one of the possible Shift-JIS equivalents of a Unicode character can be used in a specific environment.

On the Conversion Tab, native encoding characters appears in the form 0xYYYY, and Unicode characters appear in the form U+YYYY, where YYYY represents the hexadecimal value of the Unicode character.

For example, the character "A" appears as follows:

- for native encoding, 0x41
- for Unicode, U+0041

Each row represents a mapping rule that associates two or three Shift-JIS characters with the Unicode character in the first column.

By default, all Shift-JIS characters in a row are converted to the associated Unicode character. For example, the Shift-JIS characters 0x8782 and 0xFA59 both convert to the Unicode character U+2116.

You can configure more than one character at a time.

Procedure

1. Start the Round Trip Safety Configuration utility in the *install_location*/bin:
   - for Microsoft Windows operating system, rtsconfig.exe
   - for UNIX operating system, rtsconfig
2. Click the **Conversion** tab.

   Tip: To see the glyph next to the Unicode character, from the **View** menu, click **Glyphs**. Depending on the type and size of fonts you use, some glyphs may not be visible.
3. From the **Edit** menu, click **Find a character,** and then enter the hexadecimal value of the Shift-JIS character.
4. Click **OK**.
5. In the **First Shift-JIS Character**, **Second Shift-JIS Character**, or **Third Shift-JIS Character** column, select the Shift-JIS character that you want the Unicode character to convert to.
6. Repeat steps 3 to 5 for each Shift-JIS character that you want to configure.
7. Save your specifications using one of the following methods:
   - To only save your specifications, from the **File** menu, click **Save**.
   - To save and apply your specifications, from the **Tools** menu, click **Configure**.

   If you save only, you can apply your specification later. For more information, see "Apply the Conversions and Substitutions" on page 388. You can also restore default settings. For more information, see "Restore the Default Conversion Settings" on page 388.

   The specifications are saved in the file shift-jis.xml in the *install_location/*bin directory.

Specify Substitutions

After the conversion, the Unicode data may contain characters that are identical in meaning, but different in appearance. For example, a full-width tilde (~) and a half-width tilde have different values in Unicode, but can be considered identical during processing.

You can use the Round Trip Safety Configuration utility to specify that specific pairs of similar characters be substituted by a single character. For example, you can specify that both widths of tilde are substituted by a full-width tilde.

On the Substitution tab, the first column contains pairs of characters that generally mean the same thing, but are represented by different values in Unicode. Each row represents a substitution rule. The first column lists the data before conversion. The second column lists the possible replacement characters.

Procedure

1. Start the Round Trip Safety Configuration utility in the *install_location*/bin:
   - for Microsoft Windows operating system, rtsconfig.exe
   - for UNIX operating system, rtsconfig
2. Click the **Substitution** tab.

   Tip: To see the glyph next to the Unicode character, from the **View** menu, click **Glyphs**. Depending on the type and size of fonts you use, some glyphs may not be visible.
3. In the **Original Code** column, click the character that you want to substitute.

4. In the **Substitute Code** column, click the equivalent character.

   A list of possible substitution options appears.
5. In the list, click the Unicode character that you want to use, or click **Do not substitute**.
6. Repeat steps 3 to 5 for each Unicode character that you want to substitute.
7. Save your specifications using one of the following methods:

   - To only save your specifications, from the **File** menu, click **Save**.
   - To save and apply your specifications, from the **Tools** menu, click **Configure**.

   If you only save, you can apply your specification later. For more information, see "Specify Conversions" on page 386. You can also restore default settings. For more information, see "Restore the Default Conversion Settings" on page 388.

   The specifications are saved in the file shift-jis.xml in the *install_location/*bin directory.

Apply the Conversions and Substitutions

If you do not apply changes when you save, you can apply the data later. Based on information saved in the file install_location/bin/shift-jis.xml, two files are generated:

- for substitution data, i18n_res.xml
- for conversion data, ibm-943_P14A-2000.cnv

About this task

When you apply the data, by default, characters are not checked for round trip safety. When you set the configuration mode, you may choose to check for round trip safety by selecting the option that returns a conversion error at run time for characters that are not round trip safe. This can be useful to initially detect which Shift-JIS characters must be configured.

Procedure

1. Stop IBM Cognos Analytics.
2. In the Round Trip Safety Configuration utility, from the **Tools** menu, click **Set the configuration mode**.
3. Specify whether you want characters checked for round trip safety.
4. From the **Tools** menu, click **Configure**.
5. Start IBM Cognos Analytics.

Restore the Default Conversion Settings

At any time, you can quickly restore the default settings in your configuration and substitution data. For example, you may want to restore the configuration in the following situations:

- after your application is set to use a different data source that requires a different configuration
- after prototyping

Procedure

1. Stop IBM Cognos Analytics.
2. In the Round Trip Safety Configuration utility, from the **Tools** menu, click **Restore defaults**.

   The conversion process is set to use the default values.
3. Start IBM Cognos Analytics.

Specify Conversions for Series 7 PowerPlay Web Reports

IBM Cognos Series 7 supplies a limited solution for the Japanese Vendor Defined Characters (VDC) in Shift-JIS encoding. To ensure data integrity and consistency when using PowerPlay Web reports with IBM Cognos Analytics, you must set the character mapping to default values.

Procedure

1. Stop IBM Cognos Analytics.
2. Start the Round Trip Safety Configuration utility, see "The Round Trip Safety Configuration Utility" on page 386.
3. From the **Tools** menu, click **Restore defaults**.
4. From the **Tools** menu, click **Configure**.

   The conversion tables are set to use the default values in the background.
5. Close the Round Trip Safety Configuration utility.
6. Start IBM Cognos Analytics.

Appendix C. Initial access permissions

In IBM Cognos Analytics, when Content Manager initializes a content store, it creates basic structures and security information. These structures include a hierarchy of folders.

Content Manager includes the following folders and folder contents:

/Root
All folders below /Root in the hierarchy.

/Root/Directory
Information about authentication providers and other information typically found in a directory service.

/Root/Directory/Cognos
The Cognos directory namespace containing Cognos groups, data sources, distribution lists, and contacts.

/Root/Directory/*other_providers*
Other security namespaces, such as LDAP, and Active Directory.

/Root/Public Content
All application data in Content Manager.

/Root/Directory/*application_packages*
A separate folder for each application containing information about the application.

/Root/Configuration
Configuration data for all Cognos components and templates.

/Root/Capabilities
Objects that can be secured through policies that restrict access to functionality, such as Administration, Reporting, and Query Studio; and to features, such as user defined SQL, and bursting.

We recommend that you modify the initial settings to secure IBM Cognos software. For more information, see Chapter 15, “Initial security,” on page 201 and Chapter 12, “Access Permissions and Credentials,” on page 173.

Initial access permissions for root and top-level Content Manager objects

In IBM Cognos Analytics, when Content Manager initializes a content store, it creates basic structures and security information. These structures include initial access permissions for the root and the top-level Content Manager objects.

The root object

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 90. The root object and permissions for related groups or roles

Object	Group or role	Read	Write	Execute	Set policy	Traverse
Root	Everyone	X		X		X

Top-level Content Manager objects

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 91. Top-level Content Manager objects and permissions for related groups and roles

Object	Group or role	Read	Write	Execute	Set policy	Traverse
Capabilities	Directory Administrators				X	X
	Everyone					X
Administration	Directory Administrators			X	X	X
	Library Administrators			X		X
	Mobile Administrators			X		X
	Modelers			X		X
	Portal Administrators			X		X
	PowerPlay Administrators			X		X
	Report Administrators			X		X
	Server Administrators			X		X
Configuration	Directory Administrators	X	X	X	X	X
	Everyone	X		X		X
Library	Library Administrators	X	X	X	X	X
	Everyone	X		X		X

Table 91. Top-level Content Manager objects and permissions for related groups and roles (continued)

Object	Group or role	Read	Write	Execute	Set policy	Traverse
Public content	Analysis Users	X		X		X
	Authors	X	X	X		X
	Consumers	X		X		X
	Information Distribution	X				X
	Modelers	X	X	X		X
	PowerPlay Administrators	X	X	X	X	X
	PowerPlay Users	X		X		X
	Query Users	X		X		X
	Readers	X				X
	Report Administrators	X	X	X	X	X
Directory	Everyone					X
Cognos	Directory Administrators	X	X	X	X	X
	Everyone	X		X		X

Initial access permissions for capabilities

In IBM Cognos Analytics, when Content Manager initializes a content store, it creates basic structures and security information. These structures include initial access permissions for the capabilities.

The capabilities are also referred to as secured functions and secured features.

Note: If you want to make changes to the initial access permissions, see "Setting access to capabilities" in the *IBM Cognos Analytics Managing Guide*.

Permission levels

There are five types of access permissions that can be assigned to a group or role: **Read**, **Write**, **Execute**, **Set policy**, and **Traverse**. For a description of the permitted actions that are available for each permission type, see Chapter 12, “Access Permissions and Credentials,” on page 173.

In addition, combinations of access permissions are granted for each capability. These combinations are defined as permission levels, as shown in the following table:

Permission level	Access permissions granted
Access	**Execute** and **Traverse**
Assign	**Traverse** and **Set Policy**
Manage	**Execute**, **Traverse**, and **Set Policy**
Custom	Any other combination not listed above.

Capability names

This section lists all the Cognos Analytics capabilities. For each capability, you can see which groups or roles can initially access the capability, as well as the access permissions that they were granted.

Adaptive Analytics capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 92. Adaptive Analytics capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓

Administration capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 93. Administration capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Manage			✓	✓	✓
Library Administrators	Access			✓		✓
Mobile Administrators	Access			✓		✓
Modelers	Access			✓		✓
Portal Administrators	Access			✓		✓

Table 93. Administration capability and permissions for related groups and roles (continued)

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
PowerPlay Administrators	Access			✓		✓
Report Administrators	Access			✓		✓
Server Administrators	Access			✓		✓

The secured features in the following table are children of the Administration capability.

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 94. Secured features of the Administration capability and permissions for related groups and roles

Secured feature	Group or role	Permission level	Permission type				
			Read	Write	Execute	Set policy	Traverse
Adaptive Analytics Administration	Adaptive Analytics Administrators				✓		✓
	Directory Administrators	Assign				✓	✓
Administration tasks	Server Administrators	Access			✓		✓
	Report Administrators	Access			✓		✓
	Directory Administrators	Assign				✓	✓
	PowerPlay Administrators	Access			✓		✓
Collaboration Administration	Directory Administrators	Manage			✓	✓	✓

Table 94. Secured features of the Administration capability and permissions for related groups and roles (continued)							
Secured feature	**Group or role**	**Permission level**	**Permission type**				
			Read	**Write**	**Execute**	**Set policy**	**Traverse**
Configure and manage the system	Server Administrators	Access			✓		✓
	Directory Administrators	Assign				✓	✓
Controller Administration	Directory Administrators	Assign				✓	✓
Data Sources Connections	Directory Administrators	Manage			✓	✓	✓
	Modelers	Access			✓		✓
Distribution Lists and Contacts	Directory Administrators	Manage			✓	✓	✓
Manage Visualizations	Directory Administrators	Assign				✓	✓
	Library Administrators	Access			✓		✓
Metric Studio Administration	Directory Administrators	Assign				✓	✓
Mobile Administration	Directory Administrators	Assign				✓	✓
	Mobile Administrators	Access			✓		✓
Planning Administration	Directory Administrators	Assign				✓	✓
PowerPlay Servers	Directory Administrators	Assign				✓	✓
	PowerPlay Administrators	Access			✓		✓
Printers	Directory Administrators	Manage			✓	✓	✓

Table 94. Secured features of the Administration capability and permissions for related groups and roles (continued)

Secured feature	Group or role	Permission level	Permission type				
			Read	Write	Execute	Set policy	Traverse
Query Service Administration	Directory Administrators	Assign				✓	✓
	Server Administrators	Access			✓		✓
Run activities and schedules	Report Administrators	Access			✓		✓
	Directory Administrators	Assign				✓	✓
	PowerPlay Administrators	Access			✓		✓
Set capabilities and manage UI profiles	Directory Administrators	Manage			✓	✓	✓
Styles and portlets	Portal Administrators	Access			✓		✓
	Directory Administrators	Manage			✓	✓	✓
	Library Administrators	Access			✓		✓
Users, Groups, and Roles	Directory Administrators	Manage			✓	✓	✓

AI capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 95. AI capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Explorers	Access			✓		✓

Table 95. AI capability and permissions for related groups and roles (continued)

Group or role	**Permission level**	**Permission type**				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Analytics Users	Access			✓		✓
Directory Administrators	Assign				✓	✓

The secured features in the following table are children of the AI capability.

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 96. Secured features of the AI capability and permissions for related groups and roles

Secured feature	**Group or role**	**Permission level**	**Permission type**				
			Read	**Write**	**Execute**	**Set policy**	**Traverse**
Learning	Analytics Explorers	Access			✓		✓
	Analytics Users	Access			✓		✓
	Directory Administrators	Assign				✓	✓
Use Assistant	Analytics Explorers	Access			✓		✓
	Analytics Users	Access			✓		✓
	Directory Administrators	Assign				✓	✓

Analysis Studio capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 97. Analysis Studio capability and permissions for related groups and roles

Group or role	**Permission level**	**Permission type**				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Analysis Users	Access			✓		✓

Table 97. Analysis Studio capability and permissions for related groups and roles (continued)

Group or role	**Permission level**	**Permission type**				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Authors	Access			✓		✓
Directory Administrators	Assign				✓	✓
Modelers	Access			✓		✓
Report Administrators	Access			✓		✓

Attach outputs capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 98. Attach Outputs capability and permissions for related groups and roles

Group or role	**Permission level**	**Permission type**				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Analytics Explorers	Access			✓		✓
Analytics Users	Access			✓		✓
Directory Administrators	Assign				✓	✓

Cognos Analytics for Mobile capability (on Demand only)

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 99. Cognos Analytics for Mobile capability and permissions for related groups and roles

Group or role	**Permission level**	**Permission type**				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Analytics Explorers	Access			✓		✓
Analytics Users	Access			✓		✓

Table 99. Cognos Analytics for Mobile capability and permissions for related groups and roles (continued)

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Viewers	Access			✓		✓
Directory Administrators	Assign				✓	✓
Report Administrators	Access			✓		✓

Cognos Insight capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 100. Cognos Insight capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓

Cognos Viewer capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 101. Cognos Viewer capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analysis Users	Access			✓		✓
Authors	Access			✓		✓
Consumers	Access			✓		✓
Directory Administrators	Assign				✓	✓
Analytics Viewers	Access			✓		✓
Modelers	Access			✓		✓

Table 101. Cognos Viewer capability and permissions for related groups and roles (continued)

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
PowerPlay Administrators	Access			✓		✓
PowerPlay Users	Access			✓		✓
Query Users	Access			✓		✓
Readers	Access			✓		✓
Report Administrators	Access			✓		✓

The secured features in the following table are children of the Cognos Viewer capability.

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 102. Secured features of the Cognos Viewer capability and permissions for related groups and roles

Secured feature	Group or role	Permission level	Permission type				
			Read	Write	Execute	Set policy	Traverse
Context Menu Selection Toolbar	Report Administrators	Access			✓		✓
	Authors	Access			✓		✓
	Consumers	Access			✓		✓
	Query Users	Access			✓		✓
	Analysis Users	Access			✓		✓
	Readers	Access			✓		✓
	Directory Administrators	Assign				✓	✓
	Analytics Viewers	Access			✓		✓
	Modelers	Access			✓		✓
	PowerPlay Administrators	Access			✓		✓
	PowerPlay Users	Access			✓		✓

Table 102. Secured features of the Cognos Viewer capability and permissions for related groups and roles (continued)

Secured feature	**Group or role**	**Permission level**	**Permission type**				
			Read	**Write**	**Execute**	**Set policy**	**Traverse**
Run With Options	Report Administrators	Access			✓		✓
	Authors	Access			✓		✓
	Consumers	Access			✓		✓
	Query Users	Access			✓		✓
	Analysis Users	Access			✓		✓
	Directory Administrators	Assign				✓	✓
	Modelers	Access			✓		✓
	PowerPlay Administrators	Access			✓		✓
	PowerPlay Users	Access			✓		✓

Collaborate capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 103. Collaborate capability and permissions for related groups and roles

Group or role	**Permission level**	**Permission type**				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Analysis Users	Access			✓		✓
Authors	Access			✓		✓
Consumers	Access			✓		✓
Directory Administrators	Assign				✓	✓
Modelers	Access			✓		✓

Table 103. Collaborate capability and permissions for related groups and roles (continued)

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
PowerPlay Administrators	Access			✓		✓
PowerPlay Users	Access			✓		✓
Query Users	Access			✓		✓
Report Administrators	Access			✓		✓

The secured features in the following table are children of the Collaborate capability.

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 104. Secured features of the Collaborate capability and permissions for related groups and roles

Secured feature	Group or role	Permission level	Permission type				
			Read	Write	Execute	Set policy	Traverse
Allow collaboration features Launch collaboration tools	Analysis Users	Access			✓		✓
	Authors	Access			✓		✓
	Consumers	Access			✓		✓
	Directory Administrators	Assign				✓	✓
	Modelers	Access			✓		✓
	PowerPlay Administrators	Access			✓		✓
	PowerPlay Users	Access			✓		✓
	Query Users	Access			✓		✓
	Report Administrators	Access			✓		✓

Controller Studio capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 105. Controller Studio capability and permissions for related groups and roles

Group or role	**Permission level**	**Permission type**				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Directory Administrators	Assign				✓	✓

Dashboard capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 106. Dashboard capability and permissions for related groups and roles

Group or role	**Permission level**	**Permission type**				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Analytics Explorers	Access			✓		✓
Analytics Users	Access			✓		✓
Analytics Viewers	Access			✓		✓
Directory Administrators	Assign				✓	✓

The secured features in the following table are children of the Dashboard capability.

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 107. Secured features of the Dashboard capability and permissions for related groups and roles

Secured feature	Group or role	Permission level	Permission type				
			Read	Write	Execute	Set policy	Traverse
Create/Edit	Analytics Explorers	Access			✓		✓
	Analytics Users	Access			✓		✓
	Directory Administrators	Assign				✓	✓

Data Manager capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 108. Data Manager capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓

Data sets capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 109. Data sets capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓
Everyone	Access			✓		✓

Desktop Tools capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 110. Desktop Tools capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Explorers	Access			✓		✓
Directory Administrators	Assign				✓	✓

Detailed Errors capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 111. Detailed Errors capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓

Develop Visualizations capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 112. Develop Visualizations capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Explorers	Access			✓		✓
Analytics Users	Access			✓		✓
Directory Administrators	Assign				✓	✓

Drill Through Assistant capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 113. Drill Through Assistant capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓

11.1.7 Email capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 114. Email capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Explorers	Access			✓		✓
Analytics Users	Access			✓		✓
Analytics Viewer	Access			✓		✓
Directory Administrators	Assign				✓	✓

The secured features in the following table are children of the Email capability.

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 115. Secured features of the Email capability and permissions for related groups and roles

Secured feature	Group or role	Permission level	Permission type				
			Read	Write	Execute	Set policy	Traverse
Email Delivery Option	Analytics Explorers	Access			✓		✓
	Analytics Users	Access			✓		✓
	Directory Administrators	Assign				✓	✓
Include link in email	Analytics Explorers	Access			✓		✓

Table 115. Secured features of the Email capability and permissions for related groups and roles (continued)

Secured feature	Group or role	Permission level	Permission type				
			Read	Write	Execute	Set policy	Traverse
	Analytics Users	Access			✓		✓
	Analytics Viewer	Access			✓		✓
	Directory Administrators	Assign				✓	✓
Share using email	Analytics Explorers	Access			✓		✓
	Analytics Users	Access			✓		✓
	Analytics Viewer	Access			✓		✓
	Directory Administrators	Assign				✓	✓
Type in external email	Analytics Explorers	Access			✓		✓
	Analytics Users	Access			✓		✓
	Analytics Viewer	Access			✓		✓
	Directory Administrators	Assign				✓	✓

Event Studio capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 116. Event Studio capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Authors	Access			✓		✓
Directory Administrators	Assign				✓	✓

Table 116. Event Studio capability and permissions for related groups and roles (continued)

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Modelers	Access			✓		✓
Report Administrators	Access			✓		✓

Execute Indexed Search capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 117. Execute Indexed Search capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analysis Users Authors Consumers Analytics Viewers Modelers PowerPlay Administrators PowerPlay Users Query Users Readers Report Administrators	Access			✓		✓
Directory Administrators	Assign				✓	✓

Executive Dashboard capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 118. Executive Dashboard capability and permissions for related groups and roles

Group or role	**Permission level**	**Permission type**				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Analysis Users	Access			✓		✓
Authors	Access			✓		✓
Consumers	Access			✓		✓
Directory Administrators	Assign				✓	✓
Analytics Viewers	Custom			Permission Denied		Permission Denied
Modelers	Access			✓		✓
PowerPlay Administrators	Access			✓		✓
PowerPlay Users	Access			✓		✓
Query Users	Access			✓		✓
Readers	Access			✓		✓
Report Administrators	Access			✓		✓

The secured features in the following table are children of the Executive Dashboard capability.

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 119. Secured features of the Executive Dashboard capability and permissions for related groups and roles

Secured feature	Group or role	Permission level	Permission type				
			Read	Write	Execute	Set policy	Traverse
Use Advanced Dashboard Features Use Interactive Dashboard Features	Authors	Access			✓		✓
	Directory Administrators	Assign				✓	✓
	Analytics Viewers	Custom					
	Modelers	Access					
	Query Users	Access			✓		✓
	Report Administrators	Access			✓		✓

Exploration capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 120. Exploration capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Explorers	Access			✓		✓
Directory Administrators	Assign				✓	✓
Analytics Viewers	Custom			Permission denied		Permission denied

External Repositories capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 121. External Repositories capability and permissions for related groups and roles						
Group or role	**Permission level**	**Permission type**				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Directory Administrators	Assign				✓	✓
Everyone	Access			✓		✓

The secured features in the following table are children of the External Repositories capability.

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 122. Secured features of the External Repositories capability and permissions for related groups and roles							
Secured feature	**Group or role**	**Permission level**	**Permission type**				
			Read	**Write**	**Execute**	**Set policy**	**Traverse**
Manage repository connections	Directory Administrators	Assign				✓	✓
View external documents	Directory Administrators	Assign				✓	✓
	Everyone	Access			✓		✓

Generate CSV Output

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 123. Generate CSV Output capability and permissions for related groups and roles						
Group or role	**Permission level**	**Permission type**				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Directory Administrators	Assign				✓	✓
Everyone	Access			✓		✓

Generate PDF Output capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 124. Generate PDF Output capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓
Everyone	Access			✓		✓

Generate XLS Output capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 125. Generate XLS Output capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓
Everyone	Access			✓		✓

Generate XML Output capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 126. Generate XML Output capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓
Everyone	Access			✓		✓

Glossary capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 127. Glossary capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Everyone	Assign			✓		✓
Directory Administrators	Access				✓	✓

Hide Entries capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 128. Hide Entries capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Everyone	Assign			✓		✓
Directory Administrators	Access				✓	✓

Import relational metadata capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 129. Import relational metadata capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Directory Administrators	Assign				✓	✓
Report Administrators	Access			✓		✓

Job capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 130. Job capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Explorers	Access			✓		✓
Analytics Users	Access			✓		✓
Directory Administrators	Assign				✓	✓
11.1.7 Report Administrators	Access			✓		✓

Lineage capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 131. Lineage capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Everyone	Access			✓		✓
Directory Administrators	Assign				✓	✓

Manage content capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 132. Manage content capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Library Administrators Mobile Administrators Portal Administrators PowerPlay Administrators Report Administrators Server Administrators	Access			✓		✓
Directory Administrators	Manage			✓	✓	✓

Manage own data source signons capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 133. Manage own data source signons capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓

Metric Studio capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 134. Metric Studio capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Explorers	Access			✓		✓

Table 134. Metric Studio capability and permissions for related groups and roles (continued)

Group or role	**Permission level**	**Permission type**				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Directory Administrators	Assign				✓	✓

The secured features in the following table are children of the Metric Studio capability.

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 135. Secured features of the Metric Studio capability and permissions for related groups and roles

Secured feature	**Group or role**	**Permission level**	**Permission type**				
			Read	**Write**	**Execute**	**Set policy**	**Traverse**
Edit View	Analytics Explorers	Access			✓		✓
	Directory Administrators	Assign				✓	✓

Mobile capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 136. Cognos Analytics Mobile Reports capability and permissions for related groups and roles

Group or role	**Permission level**	**Permission type**				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Directory Administrators	Assign				✓	✓
Analytics Viewers	Access			✓		✓
Mobile Administrators	Access			✓		✓
Mobile Users	Access			✓		✓

Notebook capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 137. Notebook capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓

Planning Contributor capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 138. Planning Contributor capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓

PowerPlay Studio capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 139. PowerPlay Studio capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Authors	Access			✓		✓
Directory Administrators	Assign				✓	✓
Modelers	Access			✓		✓
PowerPlay Administrators	Access			✓		✓
PowerPlay Users	Access			✓		✓

Query Studio capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 140. Query Studio capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Authors	Access			✓		✓
Directory Administrators	Assign				✓	✓
Modelers	Access			✓		✓
Query Users	Access			✓		✓
Report Administrators	Access			✓		✓

The secured features in the following table are children of the Query Studio capability.

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 141. Secured features of the Query Studio capability and permissions for related groups and roles

Secured feature	Group or role	Permission level	Permission type				
			Read	Write	Execute	Set policy	Traverse
Create Advanced	Authors	Access			✓		✓
	Modelers	Access			✓		✓
	Query Users	Access			✓		✓
	Report Administrators	Access			✓		✓
	Directory Administrators	Assign				✓	✓

Report Studio capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 142. Reporting capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Authors	Access			✓		✓
Directory Administrators	Assign				✓	✓
Library Administrators	Access			✓		✓
Modelers	Access			✓		✓
Report Administrators	Access			✓		✓

The secured features in the following table are children of the Reporting capability.

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 143. Secured features of the Reporting capability and permissions for related groups and roles

Secured feature	Group or role	Permission level	Permission type				
			Read	Write	Execute	Set policy	Traverse
Bursting HTML Items in Report User Defined SQL Create/Delete	Authors	Access			✓		✓
	Library Administrators	Access			✓		✓
	Modelers	Access			✓		✓
	Report Administrators	Access			✓		✓
	Directory Administrators	Assign				✓	✓
Allow External Data	Directory Administrators	Assign				✓	✓
	Library Administrators	Access					

Save to Cloud capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 144. Save to Cloud capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Explorers	Access			✓		✓
Analytics Users	Access			✓		✓
Directory Administrators	Assign				✓	✓
Report Administrators	Access			✓		✓

The secured feature in the following table is a child of the Save to Cloud capability.

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 145. Secured features of the Save to Cloud capability and permissions for related groups and roles

Secured feature	Group or role	Permission level	Permission type				
			Read	Write	Execute	Set policy	Traverse
Manage Connections	Directory Administrators	Assign				✓	✓
	Report Administrators	Access			✓		✓

Scheduling capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 146. Scheduling capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analysis Users	Access			✓		✓
Authors	Access			✓		✓
Consumers	Custom					✓

Table 146. Scheduling capability and permissions for related groups and roles (continued)

Group or role	**Permission level**	**Permission type**				
		Read	**Write**	**Execute**	**Set policy**	**Traverse**
Directory Administrators	Assign				✓	✓
Modelers	Access			✓		✓
PowerPlay Administrators	Access			✓		✓
PowerPlay Users	Access			✓		✓
Query Users	Access			✓		✓
Report Administrators	Access			✓		✓

The secured features in the following table are children of the Scheduling capability.

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 147. Secured features of the Scheduling capability and permissions for related groups and roles

Secured feature	Group or role	Permission level	Permission type				
			Read	Write	Execute	Set policy	Traverse
Schedule by day Schedule by hour Schedule by minute Schedule by month Schedule by trigger Schedule by week Schedule by year	Analysis Users	Access			✓		✓
	Authors	Access			✓		✓
	Consumers	Custom (Except for Schedule by day, where permission level = Access)					✓
	Directory Administrators	Assign				✓	✓
	Modelers	Access			✓		✓
	Query Users	Access			✓		✓
	Report Administrators	Access			✓		✓
	PowerPlay Administrators	Access			✓		✓
	PowerPlay Users	Access			✓		✓
Scheduling Priority	Report Administrators	Access			✓		✓
	Directory Administrators	Assign				✓	✓
	PowerPlay Administrators	Access			✓		✓

Self Service Package Wizard capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 148. Self Service Package Wizard capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Manage			✓	✓	✓

Set Entry-Specific Capabilities capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 149. Set Entry-Specific Capabilities capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓

Share Pin Board (on Demand only)

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 150. Share Pin Board capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Explorers	Access			✓		✓
Analytics Users	Access			✓		✓
Directory Administrators	Assign				✓	✓
Report Administrators	Access			✓		✓

Snapshots capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 151. Snapshots capability and initial permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓
Everyone	Access			✓		✓
Modelers	Access			✓		✓

Specification Execution capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 152. Specification Execution capability and initial permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓

Upload files capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 153. Upload files capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Everyone	Access			✓		✓
Directory Administrators	Assign				✓	✓
Analytics Viewers	Custom			Permission denied		Permission denied
Modelers	Access			✓		✓

Visualization Alerts capability (on Demand only)

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 154. Visualization Alerts capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Explorers	Access			✓		✓
Analytics Users	Access			✓		✓
Directory Administrators	Assign				✓	✓
Report Administrators	Access			✓		✓

Watch Rules capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 155. Watch Rules capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analysis Users	Access			✓		✓
Authors	Access			✓		✓
Consumers	Access			✓		✓
Directory Administrators	Assign				✓	✓
Modelers	Access			✓		✓
PowerPlay Administrators	Access			✓		✓
PowerPlay Users	Access			✓		✓
Query Users	Access			✓		✓
Report Administrators	Access			✓		✓

Web-based modeling capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 156. Web-based modeling capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	Assign				✓	✓
Analytics Viewers	Custom			Permission denied		Permission denied
Everyone	Access			✓		✓
Modelers	Access			✓		✓

Appendix D. Localization of Samples Databases

The samples databases provided with IBM Cognos software demonstrate a multilingual reporting environment.

The samples store a selection of text fields, such as names and descriptions, in 23 languages.

This appendix provides information about how data is stored in the samples databases and how the samples databases are set up to use multilingual data.

For more information on the samples, see *IBM Cognos Analytics Samples Guide*.

One Column Per Language

In this structure, tables contain sets of 23 columns, one for each language.

A logical naming convention is used to indicate which language a column contains. The name of each column ends with a language code suffix, such as _EN for English and _FR for French. For example, the column that contains information about countries and regions is named COUNTRY_FR for French data and COUNTRY_DE for German data. All tables use this structure except for PRODUCT_LOOKUP

Determining the Language (Columns) in the Model

In Framework Manager, you can insert a macro in the SQL of the data source query subject to return a specific column of data. The query subject uses the macro to apply the locale setting and to return a language code. The locale specifies linguistic information and cultural conventions for character type, collation, format of date and time, currency unit, and messages.

The macro, runLocale, uses a parameter map to convert the user's desired content language into a complete or partial column name. This column name is then substituted in the SQL before the query runs.

Because the samples databases use a language code as the suffix for the column name, the macro uses a parameter map to convert valid run locales into a language code and then concatenates the language code to the base column name.

Sample Query

The macro in this sample query uses the runLocale session variable as the Language_lookup parameter map key.

It returns the language code to be used as the suffix of the column name. In the following Select statement, where French is the language, the macro generates the column name COUNTRY_FR.

```
Select
COUNTRY.COUNTRY_CODE,
#'COUNTRY.COUNTRY_' + $Language_lookup{$runLocale}# as
Product_Line
from
[great_outdoors].COUNTRY
```

Because Framework Manager is flexible, your multilingual columns do not have to use the naming system used in the samples. In fact, your multilingual columns can use any naming system. You can encode your naming scheme into the parameter map, as required. You can use any session variable as the parameter map key and return any SQL syntax that you require to substitute at run-time. For more information, see the Framework Manager *User Guide*.

One Row Per Language

In this structure, each string value has a separate row with a code column that identifies the language.

Data is filtered to return only the row that contains the required language data. Normally, multilingual data is stored in a separate table to avoid duplicating non-descriptive or monolingual data.

In the samples databases, the data table contains the primary key and monolingual data, such as date information. The multilingual table contains data and a compound key composed of the foreign key and language code. For example, the PRODUCT_NAME_LOOKUP table contains the PRODUCT_NUMBER, PRODUCT_LANGUAGE, and PRODUCT_NAME columns, where PRODUCT_NUMBER and PRODUCT LANGUAGE form the primary key. Each of the localized items is expressed in 23 rows, one for each language.

The following foreign key table contains one or more localized items.

Table 157. Example of a foreign key table that contains localized items

Primary key table	**Foreign key table**	**Database**
PRODUCT	PRODUCT_NAME _LOOKUP	GOSALES
SLS PRODUCT DIM	SLS_PRODUCT _LOOKUP	GOSALESDW

The samples databases use ISO language codes to identify each row of data.

Determining the Language (Rows) in the Model

In Framework Manager, you can insert a macro in the SQL of the data source query subject to return a specific row of data.

The query subject uses the macro to apply the locale setting and to return a language code.

Sample Query

The macro in the sample query below uses the runLocale session variable as the Language_lookup parameter map key and returns the corresponding language code. The sq() function specifies that the return value of the macro be enclosed in single quotation marks to produce a valid SQL filter predicate. In the following Select statement, where German is the language, the macro identifies the language as DE (German), and product the filter (PRODUCT_MULTILINGUAL."LANGUAGE" = 'DE').

```
Select
P.INTRODUCTION_DATE,
P.PRODUCT_TYPE_CODE,
P.PRODUCTION_COST,
P.MARGIN,
PRODUCT_LOOKUP.PRODUCT_NUMBER as PRODUCT_NUMBER1,
PRODUCT_LOOKUP."PRODUCT_LANGUAGE",
PRODUCT_LOOKUP.PRODUCT_NAME,
PRODUCT_LOOKUP.PRODUCT_DESCRIPTION
From
gosales].PRODUCT as P,
[gosales].PRODUCT_LOOKUP
Where
P.PRODUCT_NUMBER = PRODUCT_LOOKUP.PRODUCT_NUMBER
and
(PRODUCT_LOOKUP."PRODUCT_LANGUAGE" = #sq($Language_lookup{$runLocale})#)
```

Transliterations and Multiscript Extensions

For transliteration of Asian languages, a table contains two columns with equivalent information.

One column shows string values using only Latin characters. The other column shows string values using both Asian and Latin characters. The naming convention is to add the suffix _MB.

In the Latin-only columns, transliteration defines the phonetic equivalent of the value defined in the _MB column.

The following tables include columns that contain transliterated values.

Table 158. Columns with equivalent, translated values, example

Table	Database
ORDER_HEADER	GOSALES
RETAILER	GOSALES
RETAILER_SITE _MB	GOSALES
BRANCH	GOSALES
EMPLOYEE	GOSALES

Transliterations in the Model

The following example creates a single data source, based on a query subject of two tables. The tables are identical except for the use of Asian characters in one table.

Column with names that end with the suffix _MB store Asian-related data using Asian characters, such as Chinese ideograms. This removes some duplication and makes it easier to define relationships to other query subjects in the model.

```
Select
RS.RTL_RETAILER_SITE_CODE,
RS.RTL_RETAILER_CODE,
RS.RTL_ADDRESS1,
RS.RTL_ADDRESS2,
RS.RTL_CITY,
RS.RTL_REGION,
RS.RTL_POSTAL_ZONE,
RS.RTL_COUNTRY_CODE,
RS.RTL_ACTIVITY_STATUS_CODE,
RS_MB.RTL_ADDRESS1 as Address1_MB,
RS_MB.RTL_ADDRESS2 as Address2_MB,
RS_MB.RTL_CITY as City_MB,
RS_MB.RTL_REGION as Region_MB
from
[goretailers].RETAILER_SITE as RS,
[goretailers].RETAILER_SITE_MB
as RS_MB
where
RETAILER_SITE.RETAILER_SITE_CODE = RETAILER_SITE_MB.RETAILER_SITE_CODE
```

Multiscript Extensions

After defining the query subjects in the model, items with the _MB extension are renamed with a multiscript extension, such as Address 1 (multiscript) to ease use and readability.

Using Multi-Script Extensions for Conditional Formatting

An example of multi-script usage is a mailing address in which the multiscript values ensure that mailing labels are formatted for local handling and delivery.

To add more value to mailing labels, the GO Sales and Retailers model applies conditional formatting to generate international address formats.

In the following example, Address line 3 is the name of a user-defined calculation that is used to generate line three of a mailing label. The expression uses a Country or region code value to specify how to format the line.

```
if ([Retailers].[Retailer
site].[Country or region code] = 6) then
(' ' + [Retailers].[Retailer
site].[Address 1 (multiscript)])
```

```
else
if ([Retailers].[Retailer site].[Country or region
code] = 8) then
([Retailers].[Retailer site].[Address
2 (multiscript)])
else
if ([Retailers].[Retailer site].[Country or region
code] = 13) then
([Retailers].[Retailer site].[Region
(multiscript)] + ' ' + [Retailers].[Retailer
site].[City (multiscript)]
+ ' ' + [Retailers].[Retailer
site].[Address 1 (multiscript)] + '
' + [Retailers].[Retailer site].[Address
2 (multiscript)])
else
if ([Retailers].[Retailer site].[Country or region
code] = 14) then
([Retailers].[Retailer site].[Address
2 (multiscript)])
else
([Retailers].[Retailer site].[Address
1 (multiscript)])
```

Multiscript extensions allow a user in any language to use the same model columns to create an address block and see the address properly formatted for each delivery location. For more information, see the Mailing address data source query subjects in the gosales_goretailers sample model.

Appendix E. Schema for Data Source Commands

When you work with data source connections, you can also add or edit data source commands.

Data source commands are run when the query engine performs specific actions on a database, such as opening a connection or closing a user session. For example, you can use data source commands to set up an Oracle proxy connection or virtual private database. For more information, see "Passing IBM Cognos context to a database" on page 128.

A data source command block is an XML document that is used to specify the commands that the database should run.

This document contains reference material about each element in the XML schema that defines the command blocks.

After the description of each element, separate sections describe

- the child elements that the element can or must have
- the parent elements that can contain the element

There are also code samples that show how you can use elements in a command block.

The list of children for each element is presented as a DTD model group, and elements are listed in the order that they must occur. The following standard notation is used.

Table 159. Standard notation for editing data source commands

Symbol	Meaning
Plus sign (+)	The preceding element may be repeated more than once but must occur at least once.
Question mark (?)	The preceding element is optional. It may be absent or it may occur exactly once.
Asterisk (*)	An asterisk (*) after an element specifies that the element is optional. It may occur zero or more times.
None	If an element has no plus sign (+), question mark (?), or asterisk (*) following it, the element must occur only once.
Parentheses	Parentheses group elements. Element groups are controlled using the same symbols as elements.
Bar (|)	A bar (|) between elements specifies that one of the listed elements must be present.
Comma (,)	The elements that it separates must be present in the specified order.

commandBlock

Defines a group of commands that the database runs when specific events occur. This is the root element of the schema.

Child Elements of commandBlock Element

(commands) +

Parent Elements of commandBlock Element

The commandBlock element has no parent elements.

commands

Specifies the set of commands that the database runs. The commands run in the order that they appear within the commandBlock.

Here is an example of how you can use this element in a commandBlock.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>
```

Child Elements of commands Element

(sessionStartCommand|sessionEndCommand|setCommand|sqlCommand) *

Parent Elements of commands Element

commandBlock

sessionStartCommand

Defines a command used to begin a proxy session in the database.

There should be only one sessionStartCommand per commandBlock. If the commandBlock contains more than one sessionStartCommand, only the last one will be used to create a proxy session.

Here is an example of how you can use this element in a commandBlock.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
        <argument>
            <name>OCI_ATTR_PASSWORD</name>
            <value>password1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
```

Child Elements of sessionStartCommand Element

(arguments) ?

Parent Elements of sessionStartCommand Element

commands

sessionEndCommand

Defines a command used to terminate a proxy session in the database.

If no sessionEndCommand is supplied, the proxy session will be terminated upon disconnecting from the database.

Here is an example of how you can use this element in a commandBlock.

```
<commandBlock>
  <commands>
    <sessionEndCommand>
      <arguments/>
    </sessionEndCommand>
  </commands>
</commandBlock>
```

Child Elements of sessionEndCommand Element

(arguments) ?

Parent Elements of sessionEndCommand Element

commands

arguments

Specifies the argument values to be used with the command.

Here is an example of how you can use this element in a commandBlock.

```
<commandBlock>
  <commands>
    <sessionEndCommand>
      <arguments/>
    </sessionEndCommand>
  </commands>
</commandBlock>
```

Child Elements of arguments Element

(argument) *

Parent Elements of arguments Element

- sessionStart
- sessionEnd

argument

Defines an argument value for a call to a database API.

Here is an example of how you can use this element in a commandBlock.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
        <argument>
            <name>OCI_ATTR_PASSWORD</name>
            <value>password1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>
```

Child Elements of argument Element

(name and value)

Parent Elements of argument Element

arguments

setCommand

This element is reserved for future use.

sqlCommand

Defines a command that represents a native SQL statement to be run by the database.

Here is an example of how you can use this element in a commandBlock.

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql> BEGIN PKG1.STORED_PROC1; END; </sql>
    </sqlCommand>
  </commands>
</commandBlock>
```

Child Elements of sqlCommand Element

(sql)

Parent Elements of sqlCommand Element

commands

sql

Specifies the SQL statement for the database to run. The SQL statement must be in native SQL.

Here is an example of how you can use this element in a commandBlock.

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql> BEGIN PKG1.STORED_PROC1; END; </sql>
    </sqlCommand>
  </commands>
</commandBlock>
```

Child Elements of sql Element

The sql element has no child elements.

Parent Elements of sql Element

sqlCommand

name

Identifies the argument to be set.

The value of the name element must be one of:

- OCI_ATTR_USERNAME
- OCI_ATTR_PASSWORD

Here is an example of how you can use this element in a commandBlock.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>
```

Child Elements of name Element

The name element has no child elements.

Parent Elements of name Element

- argument
- setCommand

value

Specifies the value to be used for the argument.

Here is an example of how you can use this element in a commandBlock.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
      </arguments/>
    </sessionStartCommand>
  </commands>
</commandBlock>
```

Child Elements of value Element

The value element has no child elements.

Parent Elements of value Element

- argument
- setCommand

Appendix F. Data Schema for Log Messages

If you configure IBM Cognos software to send log messages to a database, the tables and the columns in each table are automatically created when you start the IBM Cognos services.

To avoid name conflicts with database keywords, all column names in the log database have the prefix "COGIPF". If you have created your own log database model, you must add the prefix "COGIPF" to the column names of the logging database tables in the model.

Table Definitions

Log messages are recorded in a table in the logging database under certain conditions. These conditions depend on the logging level that you configure in the Web portal.

For information about logging levels, see "Log messages" on page 13.

When a user logs on to IBM Cognos software, a session ID is assigned and recorded in all log messages. You can use the session ID to identify all actions performed by a user.

COGIPF_ACTION Table

Stores information about operations performed on objects.

Table 160. COGIPF_ACTION table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_HOST_IPADDR	The host IP address where the log message is generated	VARCHAR (128)
COGIPF_HOST_PORT	The host port number	INTEGER
COGIPF_PROC_ID	The process ID assigned by the operating system	INTEGER
COGIPF_LOCAL TIMESTAMP	The local date and time when the log message was generated	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	The time zone, offset from GMT	INTEGER
COGIPF_SESSIONID	The alphanumeric identification of the user session	VARCHAR (255)
COGIPF_REQUESTID	The alphanumeric identification of the request	VARCHAR (255) NOT NULL
COGIPF_STEPID	The alphanumeric identification for the step within a job run (empty if there is none)	VARCHAR (255)
COGIPF_SUBREQUESTID	The alphanumeric identification of the component subrequest	VARCHAR (255)
COGIPF_THREADID	The alphanumeric identification of the thread where the request is run	VARCHAR (255)

Table 160. COGIPF_ACTION table columns, descriptions, and data types (continued)

Column name	Description	Data type
COGIPF_ COMPONENTID	The name of the component that generates the indication	VARCHAR (64)
COGIPF_ BUILDNUMBER	The major build number for the component that generates the indication	INTEGER
COGIPF_ LOG_LEVEL	The level of the indication	INTEGER
COGIPF_ OPERATION	The action performed on the object	VARCHAR (255)
COGIPF_ TARGET_TYPE	The object on which the operation is run	VARCHAR (255)
COGIPF_ TARGET_PATH	The target object path	VARCHAR (1024)
COGIPF_STATUS	The status of the operation: blank if execution has not completed, success, warning, or failure	VARCHAR (255)
COGIPF_ ERRORDETAILS	Error details	VARCHAR (2000)

COGIPF_AGENTBUILD Table

Stores information about agent mail delivery.

Table 161. COGIPF_AGENTBUILD table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_ HOST_IPADDR	The host IP address where the log message is generated	VARCHAR (128)
COGIPF_HOST_PORT	The host port number	INTEGER
COGIPF_PROC_ID	The process ID assigned by the operating system	INTEGER
COGIPF_ LOCALTIMESTAMP	The local date and time when the log message was generated	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	The time zone, offset from GMT	INTEGER
COGIPF_SESSIONID	The alphanumeric identification of the user session	VARCHAR (255)
COGIPF_REQUESTID	The alphanumeric identification of the request	VARCHAR (255) NOT NULL

Table 161. COGIPF_AGENTBUILD table columns, descriptions, and data types (continued)

Column name	**Description**	**Data type**
COGIPF_STEPID	The alphanumeric identification for the step within a job run (empty if there is none)	VARCHAR (255)
COGIPF_ SUBREQUESTID	The alphanumeric identification of the component subrequest	VARCHAR (255)
COGIPF_THREADID	The alphanumeric identification of the thread where the request is run	VARCHAR (255)
COGIPF_ COMPONENTID	The name of the component that generates the indication	VARCHAR (64)
COGIPF_BUILD NUMBER	The major build number for the component that generates the indication	INTEGER
COGIPF_LOG_LEVEL	The level of the indication	INTEGER
COGIPF_OPERATION	The operation	VARCHAR (128)
COGIPF_ TARGET_TYPE	The object on which the operation is run	VARCHAR (255)
COGIPF_TARGET_ NAME	The target name	VARCHAR (512)
COGIPF_ TARGET_PATH	The target path	VARCHAR (1024)
COGIPF_STATUS	The status of the operation: blank, success, warning, or failure	VARCHAR (255)
COGIPF_ ERRORDETAILS	Error details	VARCHAR (2000)
COGIPF_AGENT_ PATH	The agent name	VARCHAR (1024)
COGIPF_ SCHEDULETIME	The target schedule time	INTEGER
COGIPF_USER	The user who created the agent	VARCHAR (512)
COGIPF_EMAIL	The email address	VARCHAR (512)

COGIPF_AGENTRUN Table

Stores information about agent activity including tasks and delivery.

Table 162. COGIPF_AGENTRUN table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_ HOST_IPADDR	The host IP address where the log message is generated	VARCHAR (128)
COGIPF_HOST_PORT	The host port number	INTEGER
COGIPF_PROC_ID	The process ID assigned by the operating system	INTEGER
COGIPF_ LOCALTIMESTAMP	The local date and time when the log message was generated	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	The time zone, offset from GMT	INTEGER
COGIPF_SESSIONID	The alphanumeric identification of the user session	VARCHAR (255)
COGIPF_REQUESTID	The alphanumeric identification of the request	VARCHAR (255) NOT NULL
COGIPF_STEPID	The alphanumeric identification for the step within a job run (empty if there is none)	VARCHAR (255)
COGIPF_ SUBREQUESTID	The alphanumeric identification of the component subrequest	VARCHAR (255)
COGIPF_THREADID	The alphanumeric identification of the thread where the request is run	VARCHAR (255)
COGIPF_ COMPONENTID	The name of the component that generates the indication	VARCHAR (64)
COGIPF_BUILD NUMBER	The major build number for the component that generates the indication	INTEGER
COGIPF_LOG_LEVEL	The level of the indication	INTEGER
COGIPF_OPERATION	The operation	VARCHAR (128)
COGIPF_ TARGET_TYPE	The object on which the operation is run	VARCHAR (255)
COGIPF_ TARGET_PATH	The target path	VARCHAR (1024)
COGIPF_STATUS	The status of the operation: blank, success, warning, or failure	VARCHAR (255)

Table 162. COGIPF_AGENTRUN table columns, descriptions, and data types (continued)

Column name	Description	Data type
COGIPF_ ERROR_DETAILS	Error details	VARCHAR (2000)
COGIPF_AGENTPATH	The agent name	VARCHAR (1024)
COGIPF_ SCHEDULETIME	The target schedule time	INTEGER
COGIPF_TARGET_ NAME	The target name	VARCHAR (512)
COGIPF_USER	The user who created the agent	VARCHAR (512)
COGIPF_EMAIL	The email address	VARCHAR (512)
COGIPF_MESSAGEID	The identification of the message	VARCHAR (255)

COGIPF_ANNOTATIONSERVICE Table

Stores audit information about Annotation service operations.

For more information, see Chapter 4, “System Performance Metrics,” on page 21.

Table 163. COGIPF_ANNOTATIONSERVICE table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_ HOST_IPADDR	The host IP address where the log message is generated	VARCHAR (128)
COGIPF_HOST_PORT	The host port number	INTEGER
COGIPF_PROC_ID	The process ID assigned by the operating system	INTEGER
COGIPF_ LOCALTIMESTAMP	The local date and time when the log message was generated	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	The time zone, offset from GMT	INTEGER
COGIPF_SESSIONID	The alphanumeric identification of the user session	VARCHAR (255)
COGIPF_REQUESTID	The alphanumeric identification of the request	VARCHAR (255) NOT NULL
COGIPF_STEPID	The alphanumeric identification of the step, empty if none	VARCHAR (255)

Table 163. COGIPF_ANNOTATIONSERVICE table columns, descriptions, and data types (continued)

Column name	Description	Data type
COGIPF_SUBREQUESTID	The alphanumeric identification of the subrequest.	VARCHAR (255)
COGIPF_ THREADID	The alphanumeric identification of the thread where the request is run	VARCHAR (255)
COGIPF_ COMPONENTID	The name of the component that generates the indication	VARCHAR (64)
COGIPF_BUILDNUMBER	The major build number for the component that generates the indication	INTEGER
COGIPF_ LOG_LEVEL	The level of the indication	INTEGER
COGIPF_OPERATION	The action performed on the object	VARCHAR (255)
COGIPF_TARGET_TYPE	The target type	VARCHAR (255)
COGIPF_ TARGET_PATH	The object path	VARCHAR (1024)
COGIPF_ ANNOTATION	The alphanumeric identification of the annotation	BIGINT
COGIPF_USER	The userid of the user who performed the operation on the annotation, for example, create, update, or delete.	VARCHAR (1024)
COGIPF_PARENT_ID	The identification of the parent object	VARCHAR (1024)
COGIPF_ CREATION_TIME	The date and time when the annotation was created	TIMESTAMP
COGIPF_ UPDATE_TIME	The date and time when the annotation was updated	TIMESTAMP

COGIPF_EDITQUERY Table

Stores information about query runs.

Table 164. COGIPF_EDITQUERY table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_ HOST_IPADDR	The host IP address where the log message is generated	VARCHAR (128)

Table 164. COGIPF_EDITQUERY table columns, descriptions, and data types (continued)

Column name	Description	Data type
COGIPF_HOST_PORT	The host port number	INTEGER
COGIPF_PROC_ID	The process ID assigned by the operating system	INTEGER
COGIPF_ LOCALTIMESTAMP	The local date and time when the log message was generated While the report is executing, this is the time that the report execution started. After the report execution is complete, this is the end time of report execution. To check if execution is complete, see COGIPF_STATUS. A blank entry means an incomplete execution. A filled entry means execution completed. To calculate the execution start time for a report that has already completed execution, subtract COGIPF_RUNTIME from COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	The time zone, offset from GMT	INTEGER
COGIPF_SESSIONID	The alphanumeric identification of the user session	VARCHAR (255)
COGIPF_REQUESTID	The alphanumeric identification of the request	VARCHAR (255) NOT NULL
COGIPF_STEPID	The alphanumeric identification for the step within a job run (empty if there is none)	VARCHAR (255)
COGIPF_ SUBREQUESTID	The alphanumeric identification of the component subrequest	VARCHAR (255)
COGIPF_THREADID	The alphanumeric identification of the thread where the request is run	VARCHAR (255)
COGIPF_ COMPONENTID	The name of the component that generates the indication	VARCHAR (64)
COGIPF_ BUILDNUMBER	The major build number for the component that generates the indication	INTEGER
COGIPF_LOG_LEVEL	The level of the indication	INTEGER
COGIPF_ TARGET_TYPE	The object on which the operation is run	VARCHAR (255)

Table 164. COGIPF_EDITQUERY table columns, descriptions, and data types (continued)

Column name	Description	Data type
COGIPF_ QUERYPATH	The report path	VARCHAR (1024)
COGIPF_STATUS	The status of the operation: blank, success, warning, or failure	VARCHAR (255)
COGIPF_ ERRORDETAILS	Error details	VARCHAR (2000)
COGIPF_RUNTIME	The number of milliseconds it took the query to run	INTEGER
COGIPF_ QUERYNAME	The name of the report that was queried	VARCHAR (512)
COGIPF_PACKAGE	The package that the report is associated with	VARCHAR (1024)
COGIPF_MODEL	The model that the report is associated with	VARCHAR (512)

COGIPF_HUMANTASKSERVICE Table

Stores audit information about Human Task service operations (tasks and corresponding task states).

For more information, see Chapter 4, “System Performance Metrics,” on page 21.

Table 165. COGIPF_HUMANTASKSERVICE table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_ HOST_IPADDR	The host IP address where the log message is generated	VARCHAR (128)
COGIPF_HOST_PORT	The host port number	INTEGER
COGIPF_PROC_ID	The process ID assigned by the operating system	INTEGER
COGIPF_ LOCALTIMESTAMP	The local date and time when the log message was generated	TIMESTAMP
COGIPF_ TIMEZONE_OFFSET	The time zone, offset from GMT	INTEGER
COGIPF_SESSIONID	The alphanumeric identification of the user session	VARCHAR (255)
COGIPF_REQUESTID	The alphanumeric identification of the request.	VARCHAR (255)

Table 165. COGIPF_HUMANTASKSERVICE table columns, descriptions, and data types (continued)

Column name	Description	Data type
COGIPF_STEPID	The alphanumeric identification for the step within a job run (empty if there is none)	VARCHAR (255)
COGIPF_SUBREQUESTID	The alphanumeric identification of the subrequest.	VARCHAR (255)
COGIPF_ THREADID	The alphanumeric identification of the thread where the request is run	VARCHAR (255)
COGIPF_ BUILDNUMBER	The major build number for the component that generates the indication	INTEGER
COGIPF_ OPERATION	The action performed on the object, for example, ADD, UPDATE	VARCHAR (128)
COGIPF_TARGET_TYPE	The target type	VARCHAR (255)
COGIPF_ TARGET_PATH	The object path	VARCHAR (1024)
COGIPF_STATUS	The status of the operation: blank if execution has not completed, success, warning, or failure	VARCHAR (50)
COGIPF_ LOGENTRYID	The primary key used to link the tables COGIPF_HUMANTASKSERVICE and COGIPF_HUMANTASKSERVICE _DETAIL	VARCHAR (50) NOT NULL
COGIPF_TASKID	The task identification	VARCHAR (50)
COGIPF_ TRANSACTION_TYPE	The operation that is performed, specific to the Human Task service, for example, claim, setPriority, getTaskInfo, changeSubscription.	VARCHAR (255)
COGIPF_USER	The user who performed the transaction in COGIPF_TRANSACTION_TYPE.	VARCHAR (255)
COGIPF_TASK_PRIORITY	The priority of the task: • 1 = high • 3 = medium • 5 = low	INTEGER
COGIPF_TASK_STATUS	The status of the task: blank if execution has not completed, success, warning, or failure	VARCHAR (255)

Table 165. COGIPF_HUMANTASKSERVICE table columns, descriptions, and data types (continued)

Column name	Description	Data type
COGIPF_TASK_ ACTIVATION_TIME	The time that the task was activated. A date/time value which is stored in the database in long numeric form.	BIGINT
COGIPF_TASK_ EXPIRATION_TIME	The date and time when the task expired	BIGINT
COGIPF_TASK_NAME	The name of the task	NTEXT
COGIPF_TASK_SUBJECT	The subject of the task	NTEXT
COGIPF_TASK_ DESCRIPTION	The description of the task	NTEXT
COGIPF_TASK_ TIMEZONEID	The time zone id of the task	VARCHAR (50)
COGIPF_TASK_ ACTUAL_OWNER	The owner of the task	VARCHAR (255)
COGIPF_TASK_ INITIATOR	The initiator (creator) of the task	VARCHAR (255)
COGIPF_TASK_CLASS _NAME	The name of the task class which the task is an instance of	VARCHAR (255)
COGIPF_TASK_ CLASS_OPERATION	The action performed on the object	VARCHAR (255)
COGIPF_TASK_ COMMENT	Comments that are related to the task	VARCHAR (2048)

COGIPF_HUMANTASKSERVICE_DETAIL Table

Stores additional details about Human Task service operations (not necessarily required for every audit entry, for example, notification details and human role details).

For more information, see Chapter 4, “System Performance Metrics,” on page 21.

Table 166. COGIPF_HUMANTASKSERVICE_DETAIL table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_ HOST_IPADDR	The host IP address where the log message is generated	VARCHAR (128)
COGIPF_HOST_PORT	The host port number	INTEGER
COGIPF_SESSIONID	The alphanumeric identification of the user session	VARCHAR (255)

Table 166. COGIPF_HUMANTASKSERVICE_DETAIL table columns, descriptions, and data types (continued)

Column name	Description	Data type
COGIPF_REQUESTID	The alphanumeric identification of the request	VARCHAR (255)
COGIPF_STEPID	The alphanumeric identification of the step, empty if none	VARCHAR (255)
COGIPF_SUBREQUESTID	The alphanumeric identification of the SUBrequest.	VARCHAR (255)
COGIPF_ TASKID	The alphanumeric identification of the task	VARCHAR (50)
COGIPF_ LOGENTRYID	The primary key used to link the tables COGIPF_ HUMANTASKSERVICE and COGIPF_HUMANTASKSERVICE _DETAIL	VARCHAR (50) NOT NULL
COGIPF_NOTIFICATION_DETAILS	Details about notification emails sent about the task	NTEXT
COGIPF_HUMANROLE_USER	The userid of the user who performs a role for a task Combines with COGIPF_HUMANROLE to define the role of the user for the task	VARCHAR (255)
COGIPF_HUMANROLE_ROLE	The role of the user Combines with COGIPF_HUMAN_USER to define the role of the user for the task	VARCHAR (50)
COGIPF_SUBSCRIPTION_ OPERATION	The subscription operation, for example, SUBSCRIBE or UNSUBSCRIBE	VARCHAR (50)
COGIPF_SUBSCRIPTION_EVENT	The task event for which the user is subscribing or unsubscribing	SMALLINT
COGIPF_SUBSCRIPTION_USER	The user who is subscribing or unsubscribing for a task event	VARCHAR (255)
COGIPF_TASK_MESSAGE	The task message	NTEXT
COGIPF_TASK_MESSAGE_TYPE	The type of message stored in COGIPF_TASK_MESSAGE Values can be INPUT, OUTPUT, or FAULT	VARCHAR (20)
COGIPF_DETAIL_ID	The sequence number of the detail record	VARCHAR (50) NOT NULL

COGIPF_NATIVEQUERY Table

Stores information about queries that IBM Cognos software makes to other components.

Table 167. COGIPF_NATIVEQUERY table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_HOST_ IPADDR	The host IP address where the log message is generated	VARCHAR (128)
COGIPF_HOST_ PORT	The host port number	INTEGER
COGIPF_PROC_ID	The process ID assigned by the operating system	INTEGER
COGIPF_ LOCALTIMESTAMP	The local date and time when the log message was generated	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	The time zone, offset from GMT	INTEGER
COGIPF_SESSIONID	The alphanumeric identification of the user session	VARCHAR (255)
COGIPF_REQUESTID	The alphanumeric identification of the request	VARCHAR (255) NOT NULL
COGIPF_STEPID	The alphanumeric identification for the step within a job run (empty if there is none)	VARCHAR2 (255)
COGIPF_ SUBREQUESTID	The alphanumeric identification of the component subrequest	VARCHAR (255)
COGIPF_THREADID	The alphanumeric identification of the thread where the request is run	VARCHAR (255)
COGIPF_ COMPONENTID	The name of the component that generates the indication	VARCHAR (64)
COGIPF_ BUILDNUMBER	The major build number for the component that generates the indication	INTEGER
COGIPF_LOG_LEVEL	The level of the indication	INTEGER
COGIPF_ REQUESTSTRING	The query request string made to other components	NTEXT (1G)

COGIPF_PARAMETER Table

Stores parameter information logged by a component.

Table 168. COGIPF_PARAMETER table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_REQUESTID	The alphanumeric identification of the request	VARCHAR (255) NOT NULL
COGIPF_STEPID	The alphanumeric identification for the step within a job run (empty if there is none)	VARCHAR (255)
COGIPF_OPERATION	The action performed on the object	VARCHAR (255)
COGIPF_TARGET_ TYPE	The object on which the operation is run	VARCHAR (255)
COGIPF_ PARAMETER_NAME	The name of the parameter logged by a component	VARCHAR (255)
COGIPF_ PARAMETER_VALUE	The value of the parameter logged by a component	VARCHAR (512)
COGIPF_LOCALTIMESTAMP	The local date and time when the log message was generated	TIMESTAMP
COGIPF_SESSIONID	The alphanumeric identification of the user session	VARCHAR (255)
COGIPF_SUBREQUESTID	The alphanumeric identification of the component subrequest	VARCHAR (255)
COGIPF_PARAMETER_VALUE_BLOB	The report prompt parameters and report run options	NTEXT

COGIPF_RUNJOB Table

Stores information about job runs.

Table 169. COGIPF_RUNJOB table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_HOST_IPADDR	The host IP address where the log message is generated	VARCHAR (128)
COGIPF_HOST_PORT	The host port number	INTEGER
COGIPF_PROC_ID	The process ID assigned by the operating system	INTEGER

Table 169. COGIPF_RUNJOB table columns, descriptions, and data types (continued)

Column name	Description	Data type
COGIPF_ LOCALTIMESTAMP	The local date and time when the log message was generated While the report is executing, this is the time that the report execution started. After the report execution is complete, this is the end time of report execution. To check if execution is complete, see COGIPF_STATUS. A blank entry means an incomplete execution. A filled entry means execution completed. To calculate the execution start time for a report that has already completed execution, subtract COGIPF_RUNTIME from COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	The time zone, offset from GMT	INTEGER
COGIPF_SESSIONID	The alphanumeric identification of the user session	VARCHAR (255)
COGIPF_REQUESTID	The alphanumeric identification of the request	VARCHAR (255) NOT NULL
COGIPF_STEPID	The alphanumeric identification for the step within a job run (empty if there is none)	VARCHAR (255)
COGIPF_SUBREQUESTID	The alphanumeric identification of the component subrequest	VARCHAR (255)
COGIPF_THREADID	The alphanumeric identification of the thread where the request is run	VARCHAR (255)
COGIPF_COMPONENTID	The name of the component that generates the indication	VARCHAR (64)
COGIPF_BUILDNUMBER	The major build number for the component that generates the indication	INTEGER
COGIPF_LOG_LEVEL	The level of the indication	INTEGER
COGIPF_TARGET_TYPE	The object on which the operation is run	VARCHAR (255)
COGIPF_JOBPATH	The job path	VARCHAR (512)
COGIPF_STATUS	The status of the operation: blank, success, warning, or failure	VARCHAR (255)
COGIPF_ ERRORDETAILS	Error details	VARCHAR (2000)
COGIPF_RUNTIME	The number of milliseconds it took the job to run	INTEGER

COGIPF_RUNJOBSTEP Table

Stores information about job step runs.

Table 170. COGIPF_RUNJOBSTEP table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_HOST_IPADDR	The host IP address where the log message is generated	VARCHAR (128)
COGIPF_HOST_PORT	The host port number	INTEGER
COGIPF_PROC_ID	The process ID assigned by the operating system	INTEGER
COGIPF_ LOCALTIMESTAMP	The local date and time when the log message was generated While the report is executing, this is the time that the report execution started. After the report execution is complete, this is the end time of report execution. To check if execution is complete, see COGIPF_STATUS. A blank entry means an incomplete execution. A filled entry means execution completed. To calculate the execution start time for a report that has already completed execution, subtract COGIPF_RUNTIME from COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	The time zone, offset from GMT	INTEGER
COGIPF_SESSIONID	The alphanumeric identification of the user session	VARCHAR (255)
COGIPF_REQUESTID	The alphanumeric identification of the request	VARCHAR (255) NOT NULL
COGIPF_STEPID	The alphanumeric identification for the step within a job run (empty if there is none)	VARCHAR (255)
COGIPF_SUBREQUESTID	The alphanumeric identification of the component subrequest	VARCHAR (255)
COGIPF_THREADID	The alphanumeric identification of the thread where the request is run	VARCHAR (255)
COGIPF_COMPONENTID	The name of the component that generates the indication	VARCHAR (64)
COGIPF_BUILDNUMBER	The major build number for the component that generates the indication	INTEGER
COGIPF_LOG_LEVEL	The level of the indication	INTEGER
COGIPF_ TARGET_TYPE	The object on which the operation is run	VARCHAR (255)

Table 170. COGIPF_RUNJOBSTEP table columns, descriptions, and data types (continued)

Column name	Description	Data type
COGIPF_JOBSTEPPATH	The job step path	VARCHAR (512)
COGIPF_STATUS	The status of the operation: blank, success, warning, or failure	VARCHAR (255)
COGIPF_ERRORDETAILS	Error details	VARCHAR (2000)
COGIPF_RUNTIME	The number of milliseconds it took the jobstep run	INTEGER

COGIPF_RUNREPORT Table

Stores information about report runs.

Table 171. COGIPF_RUNREPORT table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_HOST_IPADDR	The host IP address where the log message is generated	VARCHAR (128)
COGIPF_HOST_PORT	The host port number	INTEGER
COGIPF_PROC_ID	The process ID assigned by the operating system	INTEGER
COGIPF_ LOCALTIMESTAMP	The local date and time when the log message was generated While the report is executing, this is the time that the report execution started. After the report execution is complete, this is the end time of report execution. To check if execution is complete, see COGIPF_STATUS. A blank entry means an incomplete execution. A filled entry means execution completed. To calculate the execution start time for a report that has already completed execution, subtract COGIPF_RUNTIME from COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	The time zone, offset from GMT	INTEGER
COGIPF_SESSIONID	The alphanumeric identification of the user session	VARCHAR (255)
COGIPF_REQUESTID	The alphanumeric identification of the request	VARCHAR (255) NOT NULL

Table 171. COGIPF_RUNREPORT table columns, descriptions, and data types (continued)

Column name	Description	Data type
COGIPF_STEPID	The alphanumeric identification for the step within a job run (empty if there is none)	VARCHAR (255)
COGIPF_SUBREQUESTID	The alphanumeric identification of the component subrequest	VARCHAR (255)
COGIPF_THREADID	The alphanumeric identification of the thread where the request is run	VARCHAR (255)
COGIPF_COMPONENTID	The name of the component that generates the indication	VARCHAR (64)
COGIPF_BUILDNUMBER	The major build number for the component that generates the indication	INTEGER
COGIPF_LOG_LEVEL	The level of the indication	INTEGER
COGIPF_TARGET_TYPE	The object on which the operation is run. The values include: • Report ReportService is an interactive report • PromptForward ReportService is a report generated after a prompt • PromptBackward ReportService is a report generated after the user moved to the previous prompt page • Report BatchReportService is a batch or scheduled run report **Note**: The value of this column is expressed in two parts: the object type of execution and from which service the report is run, for example "Report ReportService" and "Query BatchReportService".	VARCHAR (255)
COGIPF_REPORTPATH	The report path	VARCHAR (1024)
COGIPF_STATUS	The status of the operation: blank, success, warning, or failure	VARCHAR (255)
COGIPF_ERRORDETAILS	Error details	VARCHAR (2000)
COGIPF_RUNTIME	The number of milliseconds it took the report to run	INTEGER
COGIPF_REPORTNAME	The name of the report that was run	VARCHAR (512)
COGIPF_PACKAGE	The package that the report is associated with	VARCHAR (1024)
COGIPF_MODEL	The model that the report is associated with	VARCHAR (512)

COGIPF_THRESHOLD_VIOLATIONS Table

Stores information about threshold violations for system metrics.

For more information, see Chapter 4, “System Performance Metrics,” on page 21.

Table 172. COGIPF_THRESHOLD_VIOLATIONS table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_ HOST_IPADDR	The host IP address where the log message is generated	VARCHAR (128)
COGIPF_HOST_PORT	The host port number	INTEGER
COGIPF_PROC_ID	The process ID assigned by the operating system	INTEGER
COGIPF_ LOCALTIMESTAMP	The local date and time when the log message was generated	TIMESTAMP
COGIPF_TIMEZONE OFFSET	The time zone, offset from GMT	INTEGER
COGIPF_COMPONENTID	The alphanumeric identification of the component	VARCHAR (64)
COGIPF_BUILDNUMBER	The alphanumeric identification of the build	INTEGER
COGIPF_LOG_LEVEL	The logging level. Should always be 1 to ensure that threshold violation information is available.	INTEGER
COGIPF_ OPERATION	A threshold for the metric has been crossed	VARCHAR (128)
COGIPF_TARGET_TYPE	The target type	VARCHAR (255)
COGIPF_ TARGETNAME	The target name	VARCHAR (512)
COGIPF_ TARGET_PATH	The target path of the dispatcher that conatins the threshold manager	VARCHAR (1024)
COGIPF_RESOURCE_ TYPE	The resource type that exceeds the threshold	VARCHAR (128)
COGIPF_ RESOURCE_PATH	The path of the resource that exceeded the threshold value	VARCHAR (512)
COGIPF_METRIC_NAME	The name of the metric	VARCHAR (255)
COGIPF_METRIC_VALUE	The value of the metric	VARCHAR (128)
COGIPF_METRIC_ HEALTH	The status of the metric: good, average, or poor	VARCHAR (128)

Table 172. COGIPF_THRESHOLD_VIOLATIONS table columns, descriptions, and data types (continued)

Column name	Description	Data type
COGIPF_LOWER_AVG_ THRSHLD	The lower average threshold setting. If COGIPF_LOWER_AVG_THRSHLD_XCL is 1, the metric score is average when the metric is less than this threshold setting. The metric score is good when the metric is greater than or equal than this value. If COGIPF_LOWER_AVG_THRSHLD_XCL is 0 (zero), the metric score is average when the metric is less than or equal to this value. The metric score is good when the metric is greater than this value.	VARCHAR (128)
COGIPF_LOWER_AVG_ THRSHLD_EXCL	The flag that indicates if the threshold setting in COGIPF_LOWER_AVG_THRSHLD is included when determining the metric score. If it is 0, the threshold setting is included when the metric score is determined. If it is 1, the threshold setting is not included when the metric score is determined.	DECIMAL (1,0)
COGIPF_LOWER_POOR_ THRSHLD	The lower poor threshold setting. If COGIPF_LOWER_POOR_THRSHLD_XCL is 1, the metric score is poor when the metric is less than this threshold setting. If COGIPF_LOWER_POOR_THRSHLD_XCL is 0 (zero), the metric score is poor when the metric is less than or equal to this value.	VARCHAR (128)
COGIPF_LOWER_POOR_ THRSHLD_EXCL	The flag that indicates if the threshold setting in COGIPF_LOWER_POOR_THRSHLD is included when determining the metric score. If it is 0, the threshold setting is included when the metric score is determined. If it is 1, the threshold setting is not included when the metric score is determined.	DECIMAL (1,0)
COGIPF_UPPER_AVG_ THRSHLD	The upper average threshold setting If COGIPF_UPPER_AVG_THRSHLD_XCL is 1, the metric score is poor when the metric is less than this threshold setting. If COGIPF_UPPER_AVG_THRSHLD_XCL is 0 (zero), the metric score is average when the metric is greater than or equal to this value. The metric score is good when the metric is less than or equal to this value.	VARCHAR (128)

Table 172. COGIPF_THRESHOLD_VIOLATIONS table columns, descriptions, and data types (continued)

Column name	Description	Data type
COGIPF_UPPER_AVG_ THRSHLD_EXCL	The flag that indicates if the threshold setting in COGIPF_UPPER_AVG_THRSHLD is included when determining the metric score. If it is 0, the threshold setting is included when the metric score is determined. If it is 1, the threshold setting is not included when the metric score is determined.	DECIMAL (1,0)
COGIPF_UPPER_POOR_ THRSHLD	The upper poor threshold setting. If COGIPF_UPPER_POOR_THRSHLD_XCL is 1, the metric score is poor when the metric is less than this threshold setting. If COGIPF_UPPER_POOR_THRSHLD_XCL is 0 (zero), the metric score is poor when the metric is greater than or equal to this value.	VARCHAR (128)
COGIPF_UPPER_POOR_ THRSHLD_EXCL	The flag that indicates if the threshold setting in COGIPF_UPPER_POOR_THRSHLD is included when determining the metric score. If it is 0, the threshold setting is included when the metric score is determined. If it is 1, the threshold setting is not included when the metric score is determined.	DECIMAL (1,0)

COGIPF_USERLOGON Table

Stores user logon and logoff information.

Table 173. COGIPF_USERLOGON table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_CAMID	The user's CAMID	VARCHAR(512)
COGIPF_ HOST_IPADDR	The host IP address where the log message is generated	VARCHAR (128)
COGIPF_ HOST_PORT	The host port number	INTEGER
COGIPF_PROC_ID	The process ID assigned by the operating system	INTEGER
COGIPF_ LOCALTIMESTAMP	The local date and time when the log message was generated	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	The time zone, offset from GMT	INTEGER

Table 173. COGIPF_USERLOGON table columns, descriptions, and data types (continued)

Column name	Description	Data type
COGIPF_SESSIONID	The alphanumeric identification of the user session	VARCHAR (255)
COGIPF_REQUESTID	The alphanumeric identification of the request	VARCHAR (255) NOT NULL
COGIPF_STEPID	The alphanumeric identification for the step within a job run (empty if there is none)	VARCHAR (255)
COGIPF_ SUBREQUESTID	The alphanumeric identification of the component subrequest	VARCHAR (255)
COGIPF_THREADID	The alphanumeric identification of the thread where the request is run	VARCHAR (255)
COGIPF_ COMPONENTID	The name of the component that generates the indication	VARCHAR (64)
COGIPF_ BUILDNUMBER	The major build number for the component that generates the indication	INTEGER
COGIPF_LOG_LEVEL	The level of the indication	INTEGER
COGIPF_STATUS	The status of the operation: blank, success, warning, or failure	VARCHAR (255)
COGIPF_ ERRORDETAILS	Error details	VARCHAR (2000)
COGIPF_ LOGON_OPERATION	Logon, logoff, or logon expired	VARCHAR (255)
COGIPF_USERNAME	The display name of the user	VARCHAR2 (255)
COGIPF_USERID	The username of the user	VARCHAR (255)
COGIPF_ NAMESPACE	The namespace ID	VARCHAR (255)
COGIPF_REMOTE_IPADDR	The IP address of the user	VARCHAR (128)
COGIPF_TENANTID	The tenant ID	VARCHAR(255)

COGIPF_VIEWREPORT Table

Stores information about report view requests.

Table 174. COGIPF_VIEWREPORT table columns, descriptions, and data types

Column name	Description	Data type
COGIPF_HOST_IPADDR	The host IP address where the log message is generated	VARCHAR (128)
COGIPF_HOST_PORT	The host port number	INTEGER
COGIPF_PROC_ID	The process ID assigned by the operating system	INTEGER
COGIPF_ LOCALTIMESTAMP	The local date and time when the log message was generated While the report is executing, this is the time that the report execution started. After the report execution is complete, this is the end time of report execution. To check if execution is complete, see COGIPF_STATUS. A blank entry means an incomplete execution. A filled entry means execution completed. To calculate the execution start time for a report that has already completed execution, subtract COGIPF_RUNTIME from COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_ OFFSET	The time zone, offset from GMT	INTEGER
COGIPF_SESSIONID	The alphanumeric identification of the user session	VARCHAR (255)
COGIPF_REQUESTID	The alphanumeric identification of the request	VARCHAR2 (255) NOT NULL
COGIPF_STEPID	The alphanumeric identification for the step within a job run (empty if there is none)	VARCHAR (255)
COGIPF_SUBREQUESTID	The alphanumeric identification of the component subrequest	VARCHAR (255)
COGIPF_THREADID	The alphanumeric identification of the thread where the request is run	VARCHAR (255)
COGIPF_COMPONENTID	The name of the component that generates the indication	VARCHAR (64)
COGIPF_BUILDNUMBER	The major build number for the component that generates the indication	INTEGER
COGIPF_LOG_LEVEL	The level of the indication	INTEGER
COGIPF_TARGET_TYPE	The object on which the operation is run	VARCHAR (255)
COGIPF_REPORTPATH	The report path	VARCHAR (1024)
COGIPF_STATUS	The status of the operation: blank, success, warning, or failure	VARCHAR (255)
COGIPF_ERRORDETAILS	Error details	VARCHAR (2000)

Table 174. COGIPF_VIEWREPORT table columns, descriptions, and data types (continued)

Column name	**Description**	**Data type**
COGIPF_REPORTNAME	The name of the report that was viewed	VARCHAR (512)
COGIPF_PACKAGE	The package with which the report is associated	VARCHAR (1024)
COGIPF_REPORTFORMAT	The format of the report. For more information, see "Report formats" on page 325	VARCHAR (255)
COGIPF_MODEL	The model that the report is associated with	VARCHAR (512)

Appendix G. Advanced settings configuration

You can configure advanced settings globally, for the whole IBM Cognos environment, or individually, for a dispatcher or a dispatcher service. The best practice is to specify the settings globally, and then customize the values for specific dispatchers or dispatcher services, if required.

Advanced settings are associated with the configuration entry in IBM Cognos Administration. The settings are grouped in the logging, tuning, environment, and administrator override categories.

When you specify the advanced settings globally for the configuration entry, the values you specify are acquired by all contained entries, unless the property of the contained entry is set to override the global settings. You can override the global settings to provide customized values for specific entries; however, this can increase the administration overhead.

You must have the following access permissions for the configuration entry and the affected child entries to change advanced settings:

- Read and write permissions for the entry that you want to update
- Traverse permissions for the parent of the entry that you want to update

Configuring advanced settings globally

You can configure advanced settings globally for the whole IBM Cognos environment.

About this task

The values that you specify are acquired by all contained entries. You can override the global values by specifying custom values at the dispatcher or dispatcher service level.

If the configuration entry contains child entries with settings that override the global settings, the custom settings on the child entries can be reset to use the default values.

You can configure advanced settings globally for the logging, tuning, environment, and administrator override categories.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Dispatchers and Services**.
2. In the toolbar on the **Configuration** page, click the **Set properties – Configuration** icon.
3. Click the **Settings** tab.
4. To filter the list of settings, from the **Category** list, select a category.
5. Choose the required setting from the list, and specify a value in one of the following ways:
   - Enter a value
   - Select a value from a list
   - Click **Edit** and add a parameter name and value
6. Optional: To reset the child entries to use the default settings, select the **Delete the configuration settings of all child entries** check box.
7. Click **OK**.
8. To apply the values, stop and restart the IBM Cognos services. For more information, see the *IBM Cognos Analytics Installation and Configuration Guide.*

Configuring advanced settings for specific dispatchers

You can configure advanced settings for a specific dispatcher. This allows you to specify customized configuration settings for the dispatcher that override the global configuration settings specified for the IBM Cognos environment.

About this task

If the dispatcher contains child entries with settings that override the global settings, you can reset the custom settings on the child entries to use the default values

You can specify advanced settings at a dispatcher level for the following categories: logging, tuning, and environment.

Important: Certain advanced settings associated with the environment category cannot be specified at the dispatcher level. They must be specified globally, or for a dispatcher service.

For more information, see "Configuring advanced settings globally" on page 463 and "Configuring advanced settings for specific services" on page 464

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Dispatchers and Services**.
2. Find the dispatcher, and in the **Actions** column, click its **Set properties** icon .
3. Click the **Settings** tab.
4. To filter the list of settings, from the **Category** list, select a category.
5. Choose a configuration setting from the list, and specify a value in one of the following ways:
   - Enter a value
   - Select a value from a list
   - Clicking **Edit**, select the **Override the settings acquired from the parent entry** check box, and add the parameter name and value
6. Optional: To reset the custom settings on the child entries to use the default settings, select the **Delete the configuration settings of all child entries** check box.
7. Click **OK**.
8. To apply the values, stop and restart the IBM Cognos services. For more information, see the *IBM Cognos Analytics Installation and Configuration Guide.*

Configuring advanced settings for specific services

You can configure advanced settings for specific dispatcher services, such as the AgentService. This allows you to specify customized configuration settings for the service that override the global configuration settings specified for the IBM Cognos environment.

About this task

You can set advanced settings for a dispatcher service for the following categories: logging, tuning, and environment.

For more information, see "Configuring advanced settings globally" on page 463 and "Configuring advanced settings for specific dispatchers" on page 464.

Procedure

1. In **IBM Cognos Administration**, on the **Configuration** tab, click **Dispatchers and Services**.
2. Click the dispatcher name.

3. In the list of the dispatcher services, find the required service, and in the **Actions** column, click the **Set properties** icon ▤.
4. Click the **Settings** tab.

   You can filter the list of settings by **Category**. The category choices are: **All**, **Environment**, **Logging**, and **Tuning**.
5. Define the setting in one of the following ways:
   - Find the setting that you want to customize, and type or select a value for the setting in the space provided.
   - If the setting is not listed, for **Advanced settings**, click the associated **Edit** link. In the page that is displayed, select the **Override the settings acquired from the parent entry** check box, and add the setting name and value.
6. Click **OK**.
7. To apply the values, stop and restart the IBM Cognos services. For more information, see the *IBM Cognos Analytics Installation and Configuration Guide*.

Enabling larger email attachments

You can configure the applicable Cognos services to enable IBM Cognos Analytics users to email larger attachments. If users encounter problems with email attachments, you might need to change the default MB size setting for uncompressed email attachments.

About this task

If users email attachments that are larger than the default MB size setting for uncompressed email attachments, the following problems might occur:

- An empty report file is attached to the email. The run history of the report does not indicate any issues and the whole process seems to proceed successfully.
- The delivery service rejects email attachments even if they are not too large after compression.
- Attachments are always compressed or always uncompressed.

The behavior of email attachments is controlled by the email attachment settings. You can configure the following settings for the associated Cognos services:

DeliveryService

Maximum size of an email message for delivery service in MB.

The setting is set at a higher value than all the other email attachment settings, or left at the default value of 0. To allow any size of email attachment, use the default value of 0.

Maximum size of an uncompressed email attachment for delivery service in MB.

Attachments that exceed the specified limit are compressed before they are sent. A value greater than 0 means that the delivery service will compress (zip) the output when the attachment size is higher than the specified value.

When setting a value for the uncompressed email attachment, you should allow an expansion factor for base64 encoding. This expansion increases the attachment size by a factor of approximately 4/3. So when a report being attached is 3 MB in size, the attached report in the email may become nearly 4 MB in size after the base64 encoding gets applied for internet transmission.

This expansion depends on the content of the attached report data and varies accordingly. You should consider this expansion factor when you are deciding what the maximum values should be.

AgentService

Maximum size of an uncompressed email attachment for agent service in MB.

Attachments that exceed the specified limit are not sent.

Default value: 15

BatchReportService

Maximum size of an uncompressed email attachment for batch report service in MB.

Attachments that exceed the specified limit are not sent.

Default value: 15

ReportService

Maximum size of an uncompressed email attachment for report service in MB.

Attachments that exceed the specified limit are not sent.

Default value: 15

Procedure

1. Follow the steps in the section "Configuring advanced settings for specific services" on page 464.
2. For the **DeliveryService**, specify a value for the setting **Maximum size of an uncompressed email attachment for delivery service in MB.** To allow any size of email attachment, use the default value of 0.
3. For the **AgentService**, **BatchReportService**, or **ReportService**, specify a value for the associated email attachment setting.
4. If more than one dispatcher is configured, perform the same steps for each dispatcher.

Advanced settings reference

This section describes advanced settings for IBM Cognos services.

Agent service advanced settings

This section describes advanced settings for the agent service.

asv.preview.maxRows

Specifies the maximum number of rows to display in a **Preview All** request from IBM Cognos Event Studio.

Data type:
Integer

Default:
`500`

Note:

You must restart the service for this setting to take effect.

housekeeping.run.startup

Specifies whether state objects from previously run tasks are removed from the content store during startup. If false, the cleanup is only performed at the interval specified by housekeeping.run.interval.

Data type:
Boolean

Default:
`false`

Note:

You must restart the service for this setting to take effect.

housekeeping.run.interval

Specifies the interval, in hours, when housekeeping operations will take place for previously run agents. This value is used only if housekeeping.run.startup is set to false.

Data type:
Integer

Default:
`12`

Note:

You must restart the service for this setting to take effect.

primary.wait.asv

Specifies the time, in seconds, for the primary wait threshold for the agent service. This setting is used if a value is not set in the request.

Data type:
Integer

Default:
`120`

secondary.threshold

Specifies the time, in seconds, for the secondary wait threshold for asynchronous requests. The agent service only uses this service in running its tasks (rss, report, sql, and webservice tasks).

Data type:
Integer

Default:
`30`

Content Manager service advanced settings

This section describes advanced settings for the Content Manager service.

CM.CMSync_CheckActiveTime

Specifies the period within which an active Content Manager enters standby mode if another Content Manager becomes active.

Data type:
Integer

Default:
`10000`

CM.CMSync_NegotiationTime

Specifies failover election time in milliseconds.

The election time is the wait period after a Content Manager instance fails, before other Content Manager instances attempt to become the active service. This period ensures that another Content Manager service instance does not become active unless the original Content Manager is truly failing.

Data type:
Integer

Default:
`2000`

CM.CMSync_NegotiationTimeForStartUp

Specifies startup election time in milliseconds, after a computer shutdown.

This election time is the wait period during which the default Content Manager is expected to start before other standby Content Manager instances try to start. This ensures that the preferred Content Manager is started after a computer shutdown.

Data type:
Integer

Default:
`60000`

CM.CMSync_PingTimeout

Specifies maximum time, in milliseconds, within which a busy Content Manager should send a response.

After the timeout period, the election process begins to select a new Content Manager from the standby Content Manager instances, if any instances exist.

Data type:
Integer

Default:
`120000`

CM.CMSync_ShortNetworkInterruptionTime

Specifies a short network interruption time, in milliseconds, within which failover will not occur.

Data type:
Integer

Default:
`3000`

CM.DbConnectPoolMax

Specifies the maximum number of concurrent database connections allowed to the content store.

Valid settings are -1, or 5 to 2147483647, or the database setting; whichever value is less.

A setting of -1 means connections are unlimited.

This setting applies to Content Manager connection pool settings only. If you have other services that access the same content store, there may be more concurrent database connections than specified in this parameter.

Data type:
Integer

Default:
`-1`

CM.DbConnectPoolTimeout

Specifies the maximum time, in milliseconds, that a thread waits for a connection to be available from the pool.

A setting of 0 specifies that threads never wait for a connection if one is not available immediately. A setting of -1 means the wait time is unlimited.

Data type:
Integer

Default:
`-1`

CM.DbConnectPoolIdleTime

Specifies the minimum time, in milliseconds, that a connection stays idle in the pool.

This setting is valid only if the value of `DbConnectPoolCleanUpPeriod` setting is positive.

A setting of 0 or `-1` specifies that idle connections are closed when Content Manager restarts.

Data type:
Integer

Default:
`300000`

CM.DbConnectPoolCleanUpPeriod

Specifies the time, in milliseconds, between invocations of a cleanup thread that closes idle connections in the pool that exceed the setting of `DbConnectPoolIdleTime`.

A setting of 0 or `-1` specifies no cleanup thread.

Data type:
Integer

Default:
`300000`

CM.DeploymentIncludeConfiguration

Specifies if configuration objects should be imported from the entire content store archive during deployment.

These objects include dispatchers and the configuration folders used to group dispatchers. For example, you may want to import the configuration because you have a series of advanced settings for your services that you want to bring in from the source environment.

For best results, do not import configuration objects. Configure dispatchers in your target environment before you import data from a source environment.

Data type:
Boolean

Default:
`false`

CM.DeploymentSkipAllReportOutput

If this setting is set to `true`, report outputs and their child objects (graphic and page) in both **My content** and **Team content** are neither exported nor imported. Use this setting to reduce the size of the content store archives and improve deployment performance.

Data type:
Boolean

Default:
`false`

CM.DeploymentSkipUserReportOutput

If this setting is set to `true`, report outputs and their child objects (graphic and page) under user accounts are not exported or imported. Use this setting to reduce the size of the content store archives and improve deployment performance.

Data type:
Boolean

Default:
`false`

CM.DeploymentDetailErrorsOnly

If set to `true`, this setting generates only summary and error information for package and folder deployments. By default, Content Manager generates full details for package and folder deployment histories. Use this settting to reduce the size of the content store archives and to improve deployment performance.

Data type:
Boolean

Default:
`false`

CM.DeploymentDetailEntireContent

If set to `true`, this setting generates full details for an entire content store deployment history. By default, Content Manager generates only summary and error information for an entire content store deployment.

Data type:
Boolean

Default:
`false`

CM.DeploymentUpdateScheduleCredential

If set to true and the **takeOwnership** option is used during the import of a deployment archive, the credential property of all imported schedule objects is changed to reference the credential contained in the account used to import the deployment.

Data type:
Boolean

Default:
`false`

CM.OutPutLocation

Specifies the file system location where generated report outputs will be saved.

Each output file also has an output descriptor of the same name, with an XML extension.

Old report versions are not deleted when a new one is saved. You must manage the content of the output directory to keep only the report versions that you want.

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.

Data type:
String

Default:
none

CM.OutputScript

Specifies the location and name of an external script that runs each time a report output is saved.

The script parameters are the report output and output descriptor file names.

Data type:
String

Default:
none

CM.OutputByBurstKey

Specifies whether or not the outputs should be organized on the file system by burst key.

If set to `true`, the output is placed in a subdirectory of the same name as the burst key.

Data type:
Boolean

Default:
`false`

CM.SecurityQueryRequiresRead

Controls whether Content Manager forces a read permission filter for external namespace query results.

When enabled, Content Manager can prevent browsing of external namespaces, if the external namespace policy is also updated to deny read permission to users or groups.

Data type:
Boolean

Default:
`false`

CM.SortCollation

The name of the database-specific collation used for sorting in some databases, such as Oracle and SQL Server.

If left empty, the database uses its default collation.

For example, in Oracle, if you specify the collation sequence as Binary at the database level, you must provide the same collation sequence value in the connection string.

An example connection string for an Oracle database that uses the sample gosl database is: `ORACLE@GOSL0703@GOSL/GOSL0703@COLSEQ=Binary`

For information about supported collations, see the Oracle and SQL Server documentation.

The `CM.SortCollation` value has no effect on Content Managers running against IBM Db2 or Sybase databases.

Data type:
String

Default:
none

CM.UpdateInitialContentNamesAfterImport

Adds localized object names for previously unsupported locales.

In some locales, if you want to upgrade to IBM Cognos Analytics from IBM Cognos Business Intelligence version 10.1.1 or earlier, and you plan to import a content store that was created with an older version of Cognos BI, use this advanced setting to ensure that all object names are properly localized.

The following locales are affected: Catalan, Croatian, Danish, Greek, Kazakh, Norwegian, Slovak, Slovenian, and Thai. Support for these locales was added in IBM Cognos Business Intelligence versions 10.1.1 and 10.2. If your content store was created with an earlier version, and the

CM.UpdateInitialContentNamesAfterImport setting was not specified before importing the content store, some object names might appear in English, and not in the specified language.

Specify the affected locales, separating each with a comma. For example, for Slovenian and Croatian content locales, type: `sl,hr`

Note: Remove this advanced setting when support for the older content store is no longer needed because there is a performance impact associated with this setting.

Data type:
String

Default:
none

Common configuration settings

This section describes advanced settings common to all services.

trustedSession.pool.max

Specifies the maximum number of trusted sessions that can be used concurrently. Trusted sessions use an internal security mechanism to encrypt the communications of internal components.

The sessions are implemented as a resource pool.

Data type:
Integer

Default:
`100`

Note:

You must restart the service for this setting to take effect.

axis.timeout

Specifies the timeout value, in seconds, for the internal axis server. This is the time that Axis will wait for a response to service calls before timing out.

Axis is an open-source tool for converting XML objects to Java objects.

Data type:
Integer

Default:
`0`

COGADMIN.filterInteractiveActivitiesOfUnknownUsers

Specifies whether activities in IBM Cognos Administration are hidden when the user doesn't have permission to view the user performing the activity.

Data type:
Boolean

Default:
`false`

COGADMIN.restrictInteractiveActivitiesToSystemAdministrators

Specifies whether interactive activities in IBM Cognos Administration are restricted to system administrators.

If this setting is set to `true`, the Current Activities tool will provide non-system administrators access to background activities only.

Data type:
Boolean

Default:
`false`

DISP.InteractiveProcessUseLimit

Forces the dispatcher to stop sending requests to a report server process after the prescribed limit.

For example, setting the limit to 500 forces the dispatcher to stop sending requests to a process after 500 requests.

Data type:
Integer

Default:
`0`

DISP.BatchProcessUseLimit

Forces the dispatcher to stop sending requests to a batch report server process after the prescribed limit.

Data type:
Integer

Default:
`0`

VIEWER_CW_BACKWARDS_COMPATIBLE_DRILL

Specifies whether legacy drill functionality is used in IBM Cognos Workspace.

By default, this setting is not specified and current drill up and down functionality is used in Cognos Workspace.

When this setting is set to `true`, drill functionality in Cognos Workspace reverts to its behavior in version 10.2.0 and earlier.

When this setting is set to `false`, current Cognos Workspace drill functionality is used.

Specify this setting at the configuration level on your system. Do not set for individual services.

Data type:
Boolean

Default:
`false`

Presentation service advanced settings

This section describes advanced settings for the presentation service.

CPSMaxCacheSizePerPortlet

Specifies the number of markup fragments cached for each portlet, per page, per user.

For example, a value of 5 with 1000 users, 10 pages, and 4 portlets per page can generate a maximum of 200000 entries in the cache (1000 x 10 x 4 x 5).

The following settings are valid:

- -1 saves an unlimited number of markups.
- 0 disables markup caching.
- 1 or an integer greater than 1 limits the number of markups to the specified number.

Data type:
Integer

Default:
`-1`

properties.config.cps.cache.timeToIdleSeconds

Specifies the length of time, in seconds, to keep the page markup fragments in the cache during a period of inactivity.

If the page is not accessed during that time, its cache contents are deleted.

The cache data saved on disk can be encrypted if the value of **Encrypt temporary files** is set to **True** under the **Environment** folder in IBM Cognos Configuration.

Data type:
Integer

Default:
`1800 (30 minutes)`

properties.config.cps.cache.timeToLiveSeconds

Specifies the length of time, in seconds, that page markup fragments are saved in the cache.

After the specified time, the markup is deleted, even if the cache is still active.

The cache data saved on disk can be encrypted if the value of **Encrypt temporary files** is set to **True** under the **Environment** folder in IBM Cognos Configuration.

Data type:
Integer

Default:
`86400 (24 hours)`

properties.config.cps.cache.checkExpiryIntervalSeconds

Specifies the length of time, in seconds, that represents the frequency with which the system checks for expired markup fragments in the cache.

The cache data saved on disk can be encrypted if the value of **Encrypt temporary files?** is set to **True** under the **Environment** folder in IBM Cognos Configuration.

Data type:
Integer

Default:
`300 (5 minutes)`

xts.tempdir

Specifies the location of the folder on the local drive where the markup fragments are stored.

The value can be any path on the local drive. If no value is specified, the default application server work area is used.

Data type:
String

Default:
`blank`

CPSPropagatePassport

Specifies whether IBM Cognos passport ID is transferred as a URL parameter.

When set to 0, this flag prevents the transfer of the IBM Cognos passport ID as a URL parameter.

Any value other than 0 allows the transfer of the passport ID.

Data type:

Default:
`None`

CPSPropagateTicket

Specifies whether IBM Cognos Configuration ticket ID is transferred as a URL parameter.

When set to 0, this flag prevents the transfer of the IBM Cognos Configuration ticket ID as a URL parameter.

Any value other than 0 allows the transfer of the ticket ID.

Data type:

Default:
`None.`

CPSProtocolScheme

Overrides the protocol scheme used when generating the Web Service Definition Language (WSDL) endpoint for Portal Services for Web Services Remote Portlets (WSRP) Producers.

To generate WSDL for WSRP, Portal Services uses the protocol scheme specified in the IBM Cognos Configuration gateway parameter. When there are multiple gateways that cannot all be configured using the same protocol scheme, for example http or https, this parameter overrides all other settings.

Valid settings are `http` and `https`

Data type:
String

Default:
`None`

portal.showTenantInfoForAllUsers

When set to true, users that do not have administrator permissions, can see tenant information.

For example, on the Set properties page, the tenant of an object is displayed. In object lists, users can see the tenant field.

Users are not able to change tenancy or to impersonate tenants.

Data type:
Boolean

Default:
`False`

Delivery service advanced settings

This section describes advanced settings for the delivery service.

emf.archive.filetimestamp.enabled

Forces timestamp on archived files.

Data type:
Boolean

Default:
`true`

max.smtp.connections

Specifies the maximum number of SMTP connections.

This setting limits the number of threads that the delivery service can spawn to send messages.

Valid settings are integers greater than or equal to 1.

Data type:
Integer

Default:
`10`

Tip: You must restart the service for this setting to take effect.

primary.wait.dls

Specifies the primary wait threshold, in seconds, for the delivery service.

This setting is used if a value is not set in a request.

If the setting is less than 0, it is ignored. If the setting is 0, the client will wait indefinitely.

Data type:
Integer

Default:
`120`

smtp.reconnection.delay

Specifies the time interval, in seconds, before an attempt to reconnect with an SMTP server is made.

Data type:

Default:
`10`

Tip: You must restart the service for this setting to take effect.

enable.tide.metrics.smtpqueue

Enables the collection and display of the metrics for the delivery service in the IBM Cognos Administration Console.

The following metrics are tracked:

- Time in queue high water mark
- Time in queue low water mark
- Time in queue
- Number of queue requests

- Queue length high water mark
- Queue length low water mark

Data type:
Boolean

Default:
`false`

dls.connection.pool.force.clean

Forces the cleanup of SMTP transport connections. This avoids the need to call the close() method, causing sockets to wait. Instead, variables are just set to null.

Data type:
Boolean

Default:
`false`

Set to true to force a cleanup.

Tip: After you apply changes, set to true to test the setting.

dls.connection.pool.used

Specifies whether the DLS Transport connection pool is used.

Data type:
Boolean

Default:
`true`

Set to true to use the connection pool.

Tip: Set to false so that the connection pool is not used. The result is that each email causes DLS to open a new SMTP transport connection with the email server. This can be helpful if mail server sockets are dropped after each use.

Customizing error-handling on the SMTP mail server

The way in which an SMTP mail server handles errors can differ depending on your mail server implementation. For this reason, you can customize the actions that the delivery service should take when it encounters specific errors by setting up SMTP rules in an XML file.

A set of default rules for error-handling is stored in a sample file provided with IBM Cognos software. To customize the rules, you should create a copy of this file and amend it. You then configure the delivery service to use this file.

Procedure

1. Edit the existing file `*installation_location*\configuration\smtpRules-default.xml` or create a new custom SMTP Rules file and add it in the `*installation_location*\configuration` folder.
2. Open the required file in an XML or text editor.
3. Amend the file to customize the rules.
4. Click **Manage**, **Administration Console**.
5. On the **Status** tab, click **System**.
6. From the **All Servers** drop-down menu, click **Services**, **Delivery**.
7. From the drop-down menu next to **DeliveryService**, click **Set properties**.

8. Click the **Settings** tab.
9. Next to **Environment**, click **Edit**.
10. In the **Parameter** column, type the parameter name **smtp.rules.properties.location**.
11. In the **Value** column, type the name of the customized xml file you are using.
12. In the **Parameter** column, type the parameter name **smtp.rules.properties.reread**.

    Although not mandatory, it is useful to set this parameter for testing purposes so that the SMTP rules are read for every request.
13. In the **Value** column, type **true**.
14. Click **OK**.
15. In the **Set properties** page, click **OK**.

    When you have finished testing the rules, you must reset the smtp.rules.properties.reread parameter.
16. Repeat steps 6 to 11 to access the advanced settings.
17. In the **Value** column for the smtp.rules.properties.reread parameter, type **false**.
18. Click **OK**.

SMTP Rules

Use the <smtpRule> tag to define an SMTP rule and the <smtpError> tag to define the error code for which you are applying a rule.

For example:

```
<smtpRule>
    <smtpError>
        <errorCode>502</errorCode>
    </smtpError>
```

```
    ...
```

```
    <smtpError>
```

```
        <errorCode>550</errorCode>
    </smtpError>
```

```
    ...
```

```
</smtpRule>
```

Note: The priority of rules is determined by the order in which they appear in the XML file.

You can define the following types of SMTP errors:

- transport errors

  For example, there is no connection to the mail server, the mail server does not exist or is not configured correctly, or the user has no access to the mail server.

  Use `<transport>true</transport>` to include this type of error in your rules.
- recipient errors

  For example, there are invalid recipients, too many recipients, or no recipients.

  Use `<invalidRecipients>true</invalidRecipients>` to include this type of error in your rules.
- other specified errors

  Any standard SMTP error code generated by the mail server.

  Use `<errorCode>nnn</errorCode>` to include this type of error in your rules.

The following actions can be performed for each error type, and are defined as behaviors in the XML file:

- resend behavior

  Specifies how many times to resend an email (n) and the resend interval in seconds (x).

  Use `<resends number="n" delaySeconds="x" />` to apply this behavior.

  Note: To resend an email indefinitely, use `<resends number="-1">.`
- keep mail behavior

  Specifies whether the delivery service should keep the failed email in a separate queue after it has been resent the required number of times and is unsuccessful. The queue is named SMTPBackupQueue.

  Note: No further action is performed on emails in the backup queue. To add emails from SMTPBackupQueue to the regular SMTPQueue, you must change the queue name in the database table and restart the server.

  Use `<keepMail>true</keepMail>` to apply this behavior.
- fail mail behavior

  Allows you to customize the email notification that is sent when an email delivery has failed.

  Use the `<failMail>` tag to apply this behavior.

  There are two further optional attributes you can use to specify the email notification subject (`<subject>`) and recipient (`<recipients>`).

  Tip: If you omit these tags, the email notification is sent by default to original recipients list with the subject "Send failed:".

  To remove all current recipients, use `<recipients sendToCurrentRecipients="false">`.

  To send an email notification to the agent owner, use `<owner>true</owner>` and, if required, use `<recipient address="name@address.com">` to specify an email address.
- default behavior

  Defines the action to perform when no matching rule is found.

  Use the `<defaultSmtpBehaviour>` tag to apply this behavior.

Examples - SMTP Rules

The first example shows how to set up a rule for the default behavior.

Here, the delivery service attempts to resend the undelivered e-mail three times at hourly intervals. If it is unsuccessful, it sends an e-mail notification using the default fail mail behavior.

```
<defaultSmtpBehaviour>
    <smtpBehaviour name="default">
        <keepMail>false</keepMail>
        <resends number="3" delaySeconds="3600" />
        <failMail />
    </smtpBehaviour>
 </defaultSmtpBehaviour>
```

The second example shows how to set up a rule for a transport error. Here, the delivery service resends the e-mail indefinitely, at 30 second intervals, until it is successful.

```
<smtpRule>
    <smtpError>
        <transport>true</transport>
    </smtpError>
    <smtpBehaviour name="transport">
        <keepMail>false</keepMail>
        <resends number="-1" delaySeconds="30" />
    </smtpBehaviour>
</smtpRule>
```

The third example shows how to set up a rule for a recipient error. Here, the e-mail notification is sent to the agent owner using the e-mail address stored in their user ID. The original e-mail recipients are removed from the recipient list.

```
<smtpRule>
    <smtpError>
        <invalidRecipients>true</invalidRecipients>
    </smtpError>
    <smtpBehaviour name="invalidRecips">
        <keepMail>false</keepMail>
        <failMail>
            <recipients sendToCurrentRecipients="false">
                <owner>true</owner>
            </recipients>
        </failMail>
    </smtpBehaviour>
 </smtpRule>
```

The fourth example shows how to set up a rule for a specified error code. Here, the undelivered e-mail is sent to the backup queue whenever error 550 occurs. It remains there until you process it manually. A customized e-mail subject is set up for the fail mail notification.

```
<smtpRule>
    <smtpError>
        <errorCode>550</errorCode>
    </smtpError>
    <smtpBehaviour name="specialErrorCode-550">
        <keepMail>true</keepMail>
        <failMail>
            <subject>Error code 550 keep mail</subject>
        </failMail>
    </smtpBehaviour>
</smtpRule>
```

Dispatcher service advanced settings

This section describes advanced settings for the dispatcher.

DISP.InteractiveProcessUseLimit

Forces the dispatcher to stop sending requests to a report server process after the prescribed limit.

For example, setting the limit to 500 forces the dispatcher to stop sending requests to a process after 500 requests.

Data type:
Integer

Default:
0

DISP.BatchProcessUseLimit

Forces the dispatcher to stop sending requests to a batch report server process after the prescribed limit.

Data type:

Default:
0

Event management service advanced settings

This section describes advanced settings for the event management service.

run.task.max.thread

Specifies the maximum number of threads that are allocated to transfer scheduled requests to a holding queue.

When the event management service runs a task, the task is placed in a queue, awaiting resources to run it. A thread is created to handle the request for the scheduler thread of the event management service.

Default value: 20

Data type:
Integer

Default:
`20`

Note:

You must restart the service for this setting to take effect.

authenticate_when_scheduled

Determines whether a runAt request header is checked for `execute` permission for the object that will be executed.

If a check is required and it fails, an exception is thrown.

If set, this check also fails if the user has the permissions but the credentials necessary to run the task at a scheduled time can not be retrieved.

Data type:
Boolean

Default:
`false`

enable.tide.metrics.jobqueue

Enables the collection and display of specific metrics for the event management service in IBM Cognos Administration.

The following metrics are included:

- Time in queue high water mark
- Time in queue low water mark
- Time in queue
- Number of queue requests
- Queue length high water mark
- Queue length low water mark

Data type:
Boolean

Default:
`false`

ems.action.requires.permissions.check

Forces the checking of object permissions.

If enabled, a caller with the canUseMonitorActivityTool user capability must also meet one of the following conditions before calling the runSpecification() method against the event management service:

- The account of the caller must match the account credential used to schedule the event.
- The caller must have traverse and execute permissions on the target object.

Data type:
Boolean

Default:
`false`

emf.schedule.validation.enabled

Validates schedule properties such as start date, end date, data types, and user account credentials when Content Manager processes requests to add or update schedules. Disables invalid schedules.

Details of disabled schedules are logged in log files.

Data type:
Boolean

Default:
`false`

emf.dls.attachment.timestamp.enabled

When set to true, email attachments have report names with a date time stamp. The default format for the timestamp is: yyyy.MM.dd, where yyyy is the four-digit year, MM is the two-digit month, and dd is the two-digit day.

For example, if you attach the report Annual Result in a message, the email that is sent has the following attachment: Annual result - 2014.07.15.pdf.

Set this advanced property if you need to add a date time stamp to report attachments in email. Optionally, change the default dateTime format by setting the advanced property emf.dls.attachment.timestamp.format.

Data type:
Boolean

Default:
`false`

emf.dls.attachment.timestamp.format

Specifies the dateTime format that is added to report names in email attachments when the emf.dls.attachment.timestamp.enabled advanced property is set to true.

Possible values include various date formats. For example, 15.07.2014 has the format `dd.MM.yyyy` and 140704120856-0700 has the format `yyMMddHHmmssZ`. For more information on SimpleDateFormat, see the Oracle website. Do not use a slash or special characters in the format.

Data type:
String

Default:
`yyyy-MM-dd`

emf.preview.max.items

Use this setting to increase the maximum number of events that can be shown in the event list.

Increasing this value can affect the performance of the system which will need to read more data and render the data in the user interface.

Data type:
Integer

Default:
`50`

Job service advanced settings

This section describes advanced settings for the job service.

primary.wait.js

Specifies the time, in seconds, for the primary wait threshold for the job service.

This value is used if a value is not set in the request.

Data type:
Integer

Default:
`120`

Metrics manager service advanced settings

This section describes advanced settings for the metrics manager service.

initialConnections

Specifies the number of connections to create when the connection pool is initialized.

Data type:
Integer

Default:
`5`

Tip: You must restart the service for these settings to take effect.

incrementConnections

Specifies the number of connections to increment when the connections pool must be increased.

Data type:
Integer

Default:
`5`

Tip: You must restart the service for these settings to take effect.

maximumConnections

Specifies the maximum number of connections this pool can use.

Data type:
Integer

Default:
`200`

Tip: You must restart the service for these settings to take effect.

Monitor service advanced settings

This section describes advanced settings for the monitor service.

emf.scheduling.priority.capability.check.disabled

When set to True, a scheduled task is run with the priority specified in the task regardless of whether the user has the Schedule Priority capability. When set to False (Default), the tasks schedule will run as the default priority.

This scenario can occur when a Users task is modified by an Administrator to have a higher priority.

Data type:
Boolean

Default:
`false`

enable.session.affinity

Indicates whether session affinity is enabled.

This setting is used in conjunction with the `session.affinity.services` advanced setting.

Data type:
Boolean

Default:
`false`

event.check.active

Specifies whether the consistency check is active.

Possible values: 1 for true, 0 (or anything else) for false

Data type:
Integer

Default:
`0`

event.check.interval

Specifies the interval, in minutes, when a consistency check is made to ensure that the monitor service record of events matches that in Content Store.

An event consistency checker thread cleans up any discrepancies.

Data type:
Integer

Default:
`10`

event.finished.check.active

Enables or disables the bulk cleanup process of finished tasks in NC tables. The process uses the `BulkFinishedTaskCleanerThread` script. The script is initiated by the monitor service when the service starts as part of the Cognos service startup.

When the system detects that this property is enabled, the cleanup script is loaded from `BulkCleanStmtsObjectFactory`. The script is database-specific and runs in a single transaction to delete any finished records that fulfill the removal criteria.

Data type:
Boolean

Default:
`true`

event.finished.check.interval

Specifies the interval, in seconds, when the bulk cleanup process checks for finished tasks in NC tables. The tasks that are finished more than 24 hours ago are candidates for the bulk cleanup.

The default is 3600 seconds (1 hour), but ideally it should be 86400 seconds (24 hours).

Data type:
Integer

Default:
`3600`

event.finished.check.threshold

Defines the maximum number of finished tasks in the NC tables that are selected for removal.

Data type:
Integer

Default:
`10`

primary.wait.ms

Specifies the primary wait threshold, in seconds, for the monitor service.

This setting is used if a value is not set in the request.

Data type:
Integer

Default:
`120`

session.affinity.services

If `enable.session.affinity` is set to `true`, this setting specifies the services to configure for session affinity.

In an N/N-1 scenario, this setting is supported by the following IBM Cognos Planning services only: `planningAdministrationConsoleService`, `planningDataService`, `planningRuntimeService`, and `planningTaskService`. Otherwise, in a homogeneous distributed environment, this setting is supported by all services.

To specify the service(s), use the mandatory `serviceName` parameter. To configure multiple services, separate each with a semi-colon (;). Here are two examples:

- `serviceName=planningTaskService`
- `serviceName=planningTaskService;serviceName=planningDataService`

Two optional parameters provide more specific configuration choices:

- `serverGroup`: Specifies the name of the server group.
- `numThreads`: Specifies the maximum number of concurrent tasks allowed. Default is 2.

Parameters must be separated by a comma (,). For example,

```
serviceName=planningTaskService,serverGroup=mygroup,numThreads=4
```

Data type:
String

Default:
None

sds.instance.interval

Specifies the update interval, in seconds, for service instances to register that they are running.

The monitor service uses this mechanism to determine that other monitor services are active. If a monitor service fails, another monitor service can elect to clean up on behalf of the failed service, including updating the history for tasks that failed.

Services can elect to clean up on behalf of another service if that service has not updated its registration within a reasonable time limit. Currently that limit is twice the `sds.instance.interval` setting.

Data type:
Integer

Default:
`30`

Note:

You must restart the service for this setting to take effect.

enable.tide.metrics.taskqueue

Enables the collection and display of specific metrics for the monitor service in IBM Cognos Administration.

The following metrics are included:

- Time in queue high water mark
- Time in queue low water mark
- Time in queue
- Number of queue requests
- Queue length high water mark
- Queue length low water mark

Data type:
Boolean

Default:
`false`

sdk.service.poll.interval

The length of time in seconds that the monitor service waits before retrying a client application request to a reconnecting service.

Data type:
Integer

Default:
`30`

advanced.history.write

Indicates whether final histories are written using the advanced (enhanced) thread pool.

If `true`, the final histories are written using multiple threads. If `false`, the final histories are written on a single thread.

Data type:
Boolean

Default:
`true`

advanced.parent.history.threads

The number of worker threads used to create root history objects in the content store.

Set `advanced.history.write` to `true` to enable this setting.

Data type:
Integer

Default:
2

Note:

You must restart the service for this setting to take effect.

advanced.child.history.threads

The number of threads used to create child history objects for steps in the content store.

Set `advanced.history.write` to `true` to enable this setting.

Data type:
Integer

Default:
5

Note:

You must restart the service for this setting to take effect.

write.child.histories

Controls the writing of child history objects to the content store.

When `true`, the final history objects for all child tasks are written. When `false`, only the final history object for the root task is written and the history objects for the child tasks are discarded. You can use this setting to improve performance for tasks where child history object write time is very high.

Data type:
Boolean

Default:
`true`

Note:

You must restart the service for this setting to take effect.

write.child.histories.during.failover

Specifies whether final history objects for a task are written to the content store during a failover.

If the value of `write.child.histories` is set to `true`, child history objects and history objects for root tasks are written.

Data type:
Boolean

Default:
`true`

Note:

You must restart the service for this setting to take effect.

connection.tracker.use

Tracks connection usage.

When `true`, java proxy objects are used to track the activities of JDBC objects.

Data type:
Boolean

Default:
`false`

Note:

You must restart the service for this setting to take effect.

connection.write.maxwaittime

The maximum period of time, in seconds, that an object waits to get a read-write connection from the JDBC connection pool.

Data type:
Integer

Default:
`10`

Note:

You must restart the service for this setting to take effect.

connection.write.maxConnections

The maximum number of read-write JDBC connections used in the connection pool.

Any value set that is less than the minimum has no effect and the minimum value that is specified is applied.

Minimum value: 5

Data type:
Integer

Default:
`10`

connection.read.maxwaittime

The maximum period of time, in seconds, that an object waits to get a read-only connection from the JDBC connection pool.

Data type:
Integer

Default:
`10`

Note:

You must restart the service for this setting to take effect.

connection.read.maxConnections

The maximum number of read-only JDBC connections that are used in the connection pool.

Any value that is set less than the minimum has no effect and the minimum value that is specified is applied.

Data type:
Integer

Default:
8

Note:

You must restart the service for this setting to take effect.

Query service advanced settings

This section describes advanced settings for the query service. This service supports the dynamic query mode.

qsMaxCrossjoinInteractiveOrderOfMagnitude

Specifies the order of magnitude of the maximum number of cells for an interactive query, for example, a dashboard or an exploration.

The default value is 5, which allows visualizations with 100000 cell values. This setting prevents the query service from attempting to load an excessive number of cells that could cause the query execution to time out. It also prevents the query service from running out of recurses and crashing.

Note: If a visualization exceeds the maximum allowable number of cells, the following error message appears:

Error XQE-MDX-0020 - The query: *query_name* requires more resources than allowed. The estimated number of cells *nnnnnn* exceeds the allowable value of 100000. Apply filtering to projected sets to reduce the number of cells.

In this case, the user should filter the sets before projecting them.

Data type:
Integer

Default:
5

qs.queryExecution.flintServer.loadingPolicy

Specifies the loading policy for the Compute service. This service can be started when the query service starts, or be deferred until a query that requires the Compute service is needed.

If a Cognos Application tier server uses a large percentage of available RAM and there is no workload that uses uploaded files or data sets, delaying the process until the server starts provides a small memory saving.

The following values can be used:

- `eager` - the Compute service starts when the query service starts.
- `lazy` - the Compute service is deferred until a query that requires this co-process is needed.

Data type:
String

Default:
`eager`

qs.queryExecution.flintServer.maxHeap

Specifies the maximum amount of memory that the Compute service is allowed to use.

The value can be 4096 (default), or a positive integer greater than 4096. Using a higher value might be required when workloads need more memory to complete.

Data type:
Positive integer

Default:
`4096`

qs.queryExecution.flintServer.minHeap

The minimum amount of memory that the Compute service is allowed to use.

The value can be `1024` (default), or a positive integer greater than `1024`.

Data type:
Positive integer

Default:
`1024`

qs.queryExecution.flintServer.sparkThreads

Specifies the maximum number of threads that the Compute service can use to service queries.

The specified value must be a positive integer greater than `1`.

Data type:
Positive integer

qs.queryExecution.flintServer.extraJavaOptions

Specifies additional parameters that can be passed to the Compute service.

Data type:
String

Report service and batch report service advanced settings

This section describes advanced settings for the report service and batch report service.

BDS.split.maxKeysPerChunk

Specifies the maximum key limit for burst reports processing. Setting the key limit lets you avoid complex SQL clauses when the RSVP.BURST_DISTRIBUTION setting is set to `true`. The value of `0` sets no limit on this parameter.

Data type:
Positive integer

Default:
`1000`

EnableChartTransparencyIE

Specifies whether charts use Internet Explorer display filters to enable transparency.

Data type:
Boolean

Default:
`true`

HyperlinkButtonNewWindow

Specifies that when a hyperlink button is clicked, a new window is created.

Data type:
Boolean

Default:
`false`

HyperlinkMultipleToolbars

Specifies that duplicate toolbars in HTML reports are permitted. Set to false to eliminate duplicate toolbars from appearing.

Data type:
Boolean

Default:
`true`

RSVP.ATTACHMENTENCODING.BASE64EXTENDED

Specifies whether base64 encoding is used when generating report output in MHT or XWLA format.

In some instances, if custom applications specify `MHT` or `XLWA` output format for reports, problems with end of line characters used in the XML output can prevent applications from opening the report.

Data type:
Boolean

Default:
`false`

RSVP.BURST_DISTRIBUTION

Specifies whether burst reports run in parallel or sequentially. If you use the default value of `false`, jobs run sequentially, which takes more time.

This setting corresponds to the **Run in parallel** burst option in the user interface. This setting is valid only when **Run in parallel** is set to **Default**. When the **Run in parallel** option is set to **Disabled** or **Enabled**, it overrides this setting.

Data type:
Boolean

Default:
`false`

RSVP.BURST_QUERY_PREFETCH

When you set this option to `true`, you enable query prefetching. As a result, the burst report outputs are produced much faster because the queries run in parallel with the report rendering. This setting is applicable to dynamic query mode relational models only.

Data type:
Boolean

Default:
`false`

RSVP.CHARTS.ALTERNATECOLOURS

Specifies that each chart instance assigns colors in palette order, and does not attempt to preserve the color of items from one chart instance to another.

Data type:
Boolean

Default:
`false`

RSVP.CONCURRENTQUERY.ENABLEDFORINTERACTIVEOUTPUT

Enables concurrent query execution when the report service is producing interactive output.

Data type:
Boolean

Default:
`false`

RSVP.CONCURRENTQUERY.MAXNUMHELPERSPERREPORT

Specifies the maximum number of query execution helpers for each report. This parameter is used to prevent a single report from consuming all available query execution helpers.

Data type:
Integer

Default:
`1`

RSVP.CONCURRENTQUERY.NUMHELPERSPERPROCESS

Enables concurrent query execution and set the maximum number of query execution helpers for each report service or batch report service process. The default value is `0`, meaning that concurrent query execution is disabled.

Data type:
Integer

Default:
`0`

RSVP.CSV.DELIMITER

Specifies the field delimiter character used for CSV output.

Data type:
String

Default:
TAB

RSVP.CSV.ENCODING

Specifies the encoding that is used when generating CSV output.

Data type:
String

Default:
`utf-16le`

RSVP.GROUP_METADATA_REQUESTS

Specifies if metadata requests are grouped, when possible, to improve performance. Users can disable the grouping of metadata requests by setting this parameter to false.

Data type:
Boolean

Default:
`true`

RSVP.CSV.MIMETYPE

Specifies the MIME type that is attributed to the CSV output.

Data type:
String

Default:
`application/vnd.ms-excel/`

RSVP.CSV.QUALIFIER

Specifies the string qualifier that is used for CSV output.

Data type:
String

Default:
`"`

RSVP.CSV.REPEAT_XTAB_LABELS

Specifies whether to repeat the edge labels in a nested crosstab report.

Data type:
Boolean

Default:
`false`

RSVP.CSV.TERMINATOR

Specifies the line terminator that is used for CSV output.

Data type:
String

Default:
`LF`

RSVP.DRILL.clearAllMappedParamsOnMismatch

Specifies how mapping of passed parameter values is processed during a drill-through operation when some parameters fail to map. The parameter mapping is continued (default), or all the mapping is discarded and the user is prompted for values.

When you set this property to 1, if any parameter fails to map, all other mapped parameters are removed from the mapping table. This could cause re-prompting for all missing parameters. When you set this property to 0, if any parameter fails to map while the drill-through component attempts to map the parameters, the mapping of the remaining parameters is not affected.

Data type:
Integer

Default:
`0`

RSVP.CSV.TRIMSPACES

Specifies that trailing spaces are removed from CSV output.

Data type:
Boolean

Default:
`false`

RSVP.DRILL.DynamicFilterUsesBusinessKey

Specifies dynamic drill-through filter behavior. Set this option to 1 if you want drill-through to generate a filter using the Member Business Key instead of the default Member Caption.

Data type:
Positive integer

Default:
`0`

RSVP.DRILL.ExtractSourceContextFromRequest

Specifies whether the report server makes an attempt to extract the metadata for the parameters of the drill-through request from the source context of the request instead of issuing a new metadata request. This type of processing improves performance of a drill-through operation. It is turned on by default.

When you set this property to 0, metadata requests are always issued.

Data type:
Integer

Default:
`1`

RSVP.EXCEL.EXCEL_XLS2007_ENABLE_SHARED_STRINGS_TABLE_SIZE_LIMIT

This setting determines whether RSVP.EXCEL.EXCEL_2007_XLS2007_SHARED_STRINGS_TABLE_SIZE_LIMIT is enabled.

Data type:
Boolean

Default:
`true`

RSVP.EXCEL.EXCEL_2007_LARGE_WORKSHEET

Enables support for large Microsoft Excel 2007 worksheets. When this option is set to `true`, worksheets with up to 1,048,576 rows are supported.

Data type:
Boolean

Default:
`false`

RSVP.EXCEL.EXCEL_2007_OUTPUT_FRAGMENT_SIZE

Adjusts the internal memory fragment size, in rows, that the IBM Cognos Analytics server generates before flushing to a disk. This property can be useful when there are issues, such as running out of memory, when generating reports with the default value. The values might need to be lowered to allow the report to run successfully.

Data type:
Integer

Default:
`45000` (approximate)

RSVP.EXCEL.EXCEL_2007_XLS2007_SHARED_STRINGS_TABLE_SIZE_LIMIT

This setting determines whether to limit the shared strings in the Excel output. Limiting shared strings increases the file size of the excel output. When shared strings are unlimited and too high it can cause Excel performance problems.

Data type:
Integer

Default:
`10000`

RSVP.EXCEL.EXCEL_2007_WORKSHEET_MAXIMUM_ROWS

Specifies the number of rows to output before moving to a new worksheet.

Data type:
Integer

RSVP.EXCEL.PAGEGROUP_WSNAME_ITEMVALUE

Specifies that, when producing output in Microsoft Excel 2007 format and page breaks are specified, the worksheet tabs are named for the data items used to break the pages.

Note: This property does not apply to Analysis Studio.

Data type:
Boolean

Default:
`false`

RSVP.EXCEL.XLS2007_ALLOW_WRAPPING_SINGLE_CELL

Specifies whether text is wrapped within a cell in Excel outputs.

Data type:
Boolean

Default:
`false`

RSVP.EXCEL.XLS2007_COLUMN_WIDTH_CONTROL

Prevents cell merging in Excel 2007 report outputs if you set the Size and Overflow values for a column.

Data type:
Boolean

Default:
`false`

RSVP.EXCEL.XLS2007_FULLDECIMALPRECISION

When set to true, numbers in Excel output are rendered with up to 15 decimal places. When set to false (the default value), numbers can contain a maximum of 12 decimal places.

Data type:
Boolean

Default:
`false`

RSVP.EXCEL.XLS2007_PRINT_MEDIA

Specifies whether the Don't Print style is applied to Excel 2007 report outputs.

Data type:
Boolean

Default:
`true`

RSVP.FILE.EXTENSION.XLS

Specifies to use XLS as the file extension on XLS output format email attachments instead of HTML.

Data type:
String

Default:
`false`

RSVP.PARAMETER_CACHE

Specifies whether parameters caching is enabled or disabled at the server level. By default, parameters caching is enabled.

When RSVP issues a getParameters request, it stores the results in a child object under the report object in IBM Cognos Content Manager. This allows the cache to be created or updated without modifying the report specification. When RSVP needs parameter information, it uses the cached information from Content Manager. If the cache does not contain the information required by RSVP, RSVP calls the query engine directly to get the information.

The cache is populated by making a ReportService getParameters SOAP request to the batch report service with the run option `http://developer.cognos.com/ceba/constants/runOptionEnum#createParameterCache`. This way, if RSVP determines the cache is missing or stale, creating the cache does not affect the execution of the report, since the cache is created by an independent request. However, since the request is handled by the batch report service, a history entry is created which is visible in the run history of a report.

The cache creation is triggered when a report is created or updated from Cognos Analytics Reporting as well as when a report is executed and RSVP determines the existing cache is stale. RSVP uses the version of the module or root model of the report to determine if the cache is stale.

Data type:
Boolean

Default:
`true`

RSVP.PARAMETERS.LOG

Specifies whether the report run options and prompt parameters must be logged to the logging system.

Data type:
Boolean

Default:
`false`

RSVP.PARAMETERS.SAVE

Specifies that report prompt values that are entered by a user are saved automatically.

Data type:
Boolean

Default:
`false`

RSVP.PRINT.POSTSCRIPT

Specifies which interface to use to print PDF documents from a UNIX operating system. When this option is set to `false`, the Adobe Acrobat PDF interface is used. Otherwise, the internal postscript interface is used.

Data type:
Boolean

Default:
`true`

RSVP.PROMPT.CASTNUMERICSEARCHKEYTOSTRING

Specifies to convert numeric data items into a string (varchar) format. This may be required if your data source does not convert numeric data items to strings.

Data type:
Boolean

Default:
`true`

RSVP.PROMPT.EFFECTIVEPROMPTINFO.IGNORE

Disables the issuing of the `effectivePromptInfo` attribute in metadata requests and effectively disables moving the prompt information from under the caption attribute of a level to the level itself. This is the default behavior.

Data type:
Boolean

Default:
`false`

RSVP.PROMPT.RECONCILIATION

Specifies a system-wide configuration that defines how queries and query groups are processed.

See the topic on setting query prioritization in the *IBM Cognos Analytics Administration and Security Guide* for a description of the possible values of this setting.

Data type:
Positiver integer or string

Default:
`0` or `COMPLETE`

RSVP.PROMPT.RECONCILIATION.CHUNKSIZE

Specifies the chunk size when the value of the RSVP.PROMPT.RECONCILIATION setting is `CHUNKED GROUPED` or `CHUNKED`.

Data type:
Positive integer

Default:
`5`

RSVP.PROMPTCACHE.LOCALE

Specifies the locale to use instead of the locale specified in the report whenever prompt cache data is created, updated, or used. This means that a single prompt cache is used for each report regardless of the report user's locale.

Data type:
String

RSVP.RENDER.PDF_FONT_SWITCHING

Specifies that each character in a string is displayed in the preferred font. The preferred font is any font listed in a report specification, followed by the fonts listed in the global styles cascading stylesheet (css) file. When a character is not available in the preferred font, it is displayed using the next font on the list.

In previous versions, a font was used only if all characters in a string could be displayed using that font. Starting with IBM Cognos Business Intelligence 10.1, the preferred font is applied at the character level. As a result, one word can be displayed using different fonts, or some fonts might be bigger, which can cause word wrapping.

Set the parameter value to false to restore the font-choosing behavior of earlier versions.

Data type:
Boolean

Default:
`true`

RSVP.RENDER.ROUNDING

Specifies the rounding rule for data formatting.

In previous versions, the `halfEven` rule was used when rounding numbers. This rule is often used in bookkeeping. However, precision regulations in some regions require different rounding rules, for example, the `halfUp` rule. Starting with version IBM Cognos Business Intelligence 10.2.0, you can choose a rounding rule that complies with the precision regulations in your organization.

The following rounding rules are available:

halfEven
Rounds to the nearest neighbor, where an equidistant value is rounded to the nearest even neighbor.

halfDown
Rounds to the nearest neighbor, where an equidistant value is rounded down.

halfUp
Rounds to the nearest neighbor, where an equidistant value is rounded up.

ceiling
Rounds to a more positive number.

floor
Rounds to a more negative number.

down
Rounds towards zero.

up
Rounds away from zero.

Data type:
String

Default:
`halfEven`

RSVP.RENDER.VALIDATEURL

Specifies whether IBM Cognos Application Firewall validation is imposed on URLs that are contained within a report specification (including URLs on image tags, buttons, hyperlinks, and background images in CSS rules) or are specified by the cssURL run option of the report.

When this option is set to `true` and CAF in enabled, validation occurs using the following rules:

- Fully qualified, or absolute URLs:

  `protocol://host[:port]/path[?query]`

  Where `protocol` is either 'http' or 'https' and the `host` is validated against the valid domain list
- URLs relative to the server installation web root:

  `/<install root>/.*`

  Where `<install root>` is the gateway file path, taken from the Gateway URI in IBM Cognos Configuration. For example, `/ibmcognos/ps/portal/images/action_delete.gif`
- One of the following specifically allowed URLs:
  - `about:blank` (case insensitive)
  - `JavaScript:window.close()` (case insensitive, with or without trailing semi-colon)
  - `JavaScript:parent.close()` (case insensitive, with or without trailing semi-colon)
  - `JavaScript:history.back()` (case insensitive, with or without trailing semi-colon)
  - `parent.cancelErrorPage()` (case insensitive, with or without trailing semi-colon)
  - `doCancel()` (case insensitive, with or without trailing semi-colon)

Data type:
Boolean

Default:
`false`

RSVP.REPORTSPEC.LOG

Specifies whether report specifications must be logged to the logging system.

Data type:
Boolean

Default:
`false`

Repository service advanced settings

This section describes advanced settings for the repository service.

repository.maxCacheDocSize

The maximum size, in MB, of an individual report that can be stored in the cache.

The value must be a positive integer (greater than 0). Reports greater than the specified size will not be cached and will be retrieved from the repository.

Data type:
Integer

Default:
`10`

UDA advanced settings

This section describes advanced settings for Universal Data Access (UDA).

The following database names are recognized in UDA advanced settings:

- SYBASE ASE
- IBM Db2
- INFORMIX
- MICROSOFT SQL SERVER
- NETEZZASQL
- NCLUSTER
- WEBSPHERE CLASSIC FEDERATION
- GREENPLUM
- INTERBASE
- INGRES
- SYBASE IQ
- INGRES_VECTORWISE
- PARACCEL
- POSTGRESQL
- TERADATA
- VERTICA DATABASE
- ORACLE
- SAP R3
- XML

If the database name is not recognized, then the setting is not read. If you have other databases that are not listed, or your ODBC drivers return a different database name, then use the database name that is obtained from the SQL_DBMS_NAME of ODBC SQLGetInfo() attribute.

UDA.CALL_ODBC_SQLNUMRESULTCOLS

Retrieves the column count that is set for a query.

Syntax:
UDA.CALL_ODBC_SQLNUMRESULTCOLS= "database name: boolean value"

Data type:
Boolean

Default:
`True`

UDA.CONVERT_TIMESTAMP_LITERAL_TO_DATE_LITERAL

Because the Oracle DATE column contains the date and time parts, UDA reports the Oracle DATE datatype as TIMESTAMP.

IBM Cognos product treats the Oracle DATE column as a TIMESTAMP, and generates a TIMESTAMP literal in the filter.

When you compare the DATE column and the TIMESTAMP literal, then the Oracle optimization adds an internal function on the DATE column to make the comparison compatible. This impacts the performance of Oracle.

This entry is specific to Oracle only. When the boolean value is set to true, then UDA converts the TIMESTAMP literal with 0 time value to a DATE literal. Oracle uses index scan on a DATE column.

Syntax:
UDA.CONVERT_TIMESTAMP_LITERAL_TO_DATE_LITERAL= "database name: boolean value"

Data type:
Boolean

Default:
`False`

UDA.INCLUDE_DST_TIMEZONE

Use this setting to include daylight saving time (DST) in the timestamp with time zone data type.

When this setting is set to true, DST is included in all operations that use the data type timestamp with time zone, such as current_timestamp. When this setting is false, DST is excluded from such operations.

Syntax:
UDA.INCLUDE_DST_TIMEZONE= boolean value

Data type:
Boolean

Default:
`True`

UDA.NATIVE_SQL_IN_CTE

Controls how the native SQL in the command table expression of a WITH clause is processed.

When the boolean value is set to KEEP, then the native SQL as part of a WITH clause is pushed to the underlying database.

When the boolean value is set to PT, then the native SQL is considered as a pass-through native SQL. The SQL itself is pushed to the database.

When the boolean value is set to DT, the WITH clause is removed, and all command table expressions are converted to derived tables.

Syntax:
UDA.NATIVE_SQL_IN_CTE= "database name:string value"

Data type:
Boolean

Default:
KEEP

UDA.PARSE_ANSI_NUMERIC_LITERAL

Specifies whether the UDA SQL parser reads the numeric literal with decimal points (for example 1.23), as an exact numeric value (for example decimal), or as an approximate value (for example double).

When the setting is true, then the UDA SQL parser reads the numeric literal with decimal points as an exact numeric value. Values with the number of digits less than 9 are read as an integer with scale. Values with the number of digits 10 - 18 are read as a quad with scale. Values with the number of digits 19 - 77 are read as a decimal (precision, scale). The value with the number of digits greater than 77 are read as a double. When the setting is false, then the UDA SQL parser reads the numeric literal with decimal points as a double.

Syntax:
UDA.PARSE_ANSI_NUMERIC_LITERAL= boolean value

Data type:
Boolean

Default:
`True`

UDA.PARSE_STRING_LITERAL_AS_VARCHAR

This setting indicates whether a string literal is parsed as a char data type or a varchar data type.

When the setting value is false, UDA SQL parser reads the string literal as char, and the string literal with prefix N as nchar. When the setting value is true, UDA SQL parser reads the string literal as varchar, and the string literal with prefix N as nvarchar.

Syntax:
UDA.PARSE_STRING_LITERAL_AS_VARCHAR= boolean value

Data type:
Boolean

Default:
`False`

UDA.REPREPARE_QUERY_FOR_PARAMETER_VALUE

Specifies whether the UDA ODBC gateways are re-preparing the query for every parameter value.

Syntax:
UDA.REPREPARE_QUERY_FOR_PARAMETER_VALUE= "database name: boolean value"

Data type:
Boolean

Default:
`False`

UDA.SET_READONLY_TRANSACTION_AUTOCOMMIT

When attaching multiple databases, set this property to true to enable the autocommit mode for an individual database if the database supports autocommit transactions.

By default, if one of the databases in the attach operation does not support autocommit transactions, the attach operation does not support these transactions for all databases. By setting this property to true, you enable autocommit for read-only transactions. The value of false disables this functionality.

If a database does not support autocommit transactions, enabling this functionality might result in the following exception:

```
UDA-SQL-0178 The "start " parameter block option is not supported.
```

Syntax:
UDA.SET_READONLY_TRANSACTION_AUTOCOMMIT= "database name: boolean value"

Data type:
Boolean

Default:
`False`

UDA.THREADSTART_TIMEOUT

Specifies a timeout in seconds on waiting to start a thread in the UDA sqlAOpen API. In the sqlAOpen API, UDA uses a separate thread to create a result set, so that the result set could be canceled by the sqlCancelOpen API.

For backward capability, the UDA_THREADSTART_TIMEOUT advanced property, that is set in Cognos Configuration, is still supported. However, if the UDA.THREADSTART_TIMEOUT advanced property is present in the Advanced Settings, then UDA_THREADSTART_TIMEOUT advanced property from Cognos Configuration is ignored.

Syntax:
UDA.THREADSTART_TIMEOUT= numeric value

Data type:
Positive Integer (1 - 600)

Default:
`20`

Index