

IBM Cognos Analytics  
Version 11.2.0

*Managing User Guide*



©

## Product Information

This document applies to IBM Cognos Analytics version 11.2.0 and may also apply to subsequent releases.

## Copyright

Licensed Materials - Property of IBM

© Copyright IBM Corp. 2015, 2021.

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

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

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

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

Microsoft product screen shot(s) used with permission from Microsoft.

© **Copyright International Business Machines Corporation .**

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

---

# Contents

- Chapter 1. Managing people.....1**
  - The Cognos namespace and the Cognos Users namespace..... 1
  - Standard roles..... 4
  - Creating and managing groups and roles..... 5
  - Creating and managing users.....6
  - Customizing roles..... 7
  - Authentication providers..... 13
    - Managing OpenID Connect namespaces.....14
  - Finding users, groups, and roles..... 17
  - Creating contacts, distribution lists, and folders..... 18
    - Creating contacts..... 18
    - Creating distribution lists..... 18
  
- Chapter 2. Managing content..... 21**
  
- Chapter 3. Configuring content sharing..... 23**
  - Integrating with a collaboration platform..... 23
    - Creating a Slack application.....23
    - Creating a Microsoft Teams application..... 24
    - Adding a collaboration platform in Cognos Analytics..... 25
  - Enabling content sharing by email..... 27
    - Example: Selectively disabling content sharing by email..... 28
  
- Chapter 4. Managing data access..... 29**
  - Data servers..... 29
    - Creating a data server connection..... 29
    - Data server types - connection details..... 33
    - Isolation levels..... 51
    - Command blocks..... 55
    - Trusted IBM Db2 Database Connections..... 60
    - Cognos-specific connection parameters..... 61
    - Loading metadata..... 69
    - Reference and troubleshooting ..... 72
    - Updates by release..... 77
  - Data modules..... 77
    - Creating data modules from Planning Analytics cubes..... 78
    - Example: Modifying a PA data source to have only one measure hierarchy..... 79
  - Packages..... 80
    - Enriching packages..... 80
  - Data sets..... 82
    - Creating data sets..... 83
    - Reusing report queries in data sets..... 86
  - Uploaded files..... 87
    - Uploading files..... 89
    - Updating data in uploaded files..... 90
    - Best practices for improving query performance on uploaded files and data sets..... 92
    - Data types used to store data in uploaded files and data sets..... 93
  
- Chapter 5. Configuring system settings..... 95**
  - Configuring appearance..... 95

Configuring security.....	96
Managing data file uploads.....	98
Logging.....	98
Setting up logging.....	99
Diagnostic logging.....	101
Enabling IBM Cognos Analytics for Jupyter Notebook.....	103
Enabling access to external Watson Studio notebooks.....	104
Advanced settings.....	105
Customizing messages in the alerts banner.....	105
Defining authentication parameters for login URLs.....	107
Setting the SameSite attribute on cookies.....	107
Enabling an option to include performance details.....	108
Adjusting the chunk size of files uploaded to the cloud.....	108
Setting response headers for HTTP requests.....	109
Changing the query operator in searches.....	109
Limiting the number of emails sent when a report is delivered.....	109
Configuring the default view for the content page.....	110
Disabling the default cleanup of labels in data modules .....	110
Dispatcher routing.....	111
Creating server groups for advanced dispatcher routing.....	111
Setting routing rules for dispatchers.....	112
<b>Chapter 6. Schedules and activities.....</b>	<b>115</b>
Scheduling a report.....	115
Taking ownership of a schedule.....	126
Changing the entry run priority.....	126
Managing upcoming activities for a specific day.....	127
Managing past activities from the Manage tool.....	128
Managing current activities.....	129
<b>Chapter 7. Tenant administration.....</b>	<b>131</b>
Containment rules for multitenancy.....	131
Creating tenants.....	131
Assigning tenant IDs to existing content.....	132
Setting a tenant ID for a public object.....	133
Delegated tenant administration.....	133
Setting up the Tenant Administrators role.....	133
Setting up virtual tenants to enable content sharing among tenants .....	134
Customizing tenants.....	135
Defining regional settings for tenants .....	136
Setting up notifications for tenants.....	136
Terminating active user sessions for tenants .....	137
Disabling and enabling tenants.....	137
Deleting tenants.....	138
<b>Chapter 8. Managing access.....</b>	<b>139</b>
Access permissions for an entry.....	139
Setting access permissions for an entry.....	144
Security settings after installation.....	146
Securing System Administrators and standard roles.....	147
Securing the Cognos namespace.....	147
Setting access for <b>Team content</b> .....	148
User capabilities.....	148
Setting access to user capabilities.....	158
Initial access permissions for capabilities.....	159
Removing capabilities from users.....	190
Object capabilities.....	190

Setting access to object capabilities.....	194
Denying capabilities on an object.....	195
Managing user licenses.....	195
License roles.....	197
Default permissions based on license roles.....	197
Assigning capabilities based on license roles.....	206
Upgrade scenario: If your customized roles have the same names as the newer Cognos license roles.....	209
<b>Chapter 9. Customizing Cognos Analytics across all roles.....</b>	<b>211</b>
Customization samples.....	212
Creating themes.....	212
Sample themes.....	213
Example: Applying the IBM_Blue_Green sample theme.....	214
Creating extensions.....	220
Sample extensions.....	221
Adding a button or a menu item.....	226
Adding a menu.....	231
Removing a user interface element.....	231
Adding dashboard shapes.....	232
Uploading custom images.....	233
Adding a dashboard widget.....	236
compatibleProductVersion.....	237
Perspective.....	239
Creating views.....	239
Sample views.....	240
Creating a view (other than a sign-in view).....	242
Creating a sign-in view.....	244
Creating a sign-in view with a namespace prompt.....	247
Applying themes, extensions, and views.....	247
Running Cognos Analytics with customized extensions and views disabled.....	248
spec . json description.....	249
Creating a global color palette.....	254
Managing User Profiles.....	256
Edit the default user profile.....	256
Viewing or changing a user profile .....	257
Deleting a user profile.....	257
Copying user profiles.....	258
Setting global parameters.....	259
Setting the _as_of_date global parameter.....	260
<b>Chapter 10. Managing cloud storage.....</b>	<b>261</b>
Creating a connection with a Cloud Object Storage provider.....	261
Creating an IBM storage connection.....	262
Creating an Amazon storage connection.....	263
Creating a MinIO storage connection.....	264
Creating a Google Cloud Platform storage connection.....	264
Creating a storage connection in Cognos Analytics.....	266
Determining the access key ID and the secret access key.....	267
Determining the service endpoint (MinIO only).....	268
Managing the connection list.....	268
Adding a location to a connection.....	270
Testing saved outputs to cloud.....	273
Saving output to cloud.....	273
Confirming that output was saved to cloud.....	274
Troubleshooting cloud storage.....	275
Error accessing cloud storage connection.....	275

Test failed.....	275
Cannot upload file to cloud.....	276
S3 headers not specified in connection.....	276
<b>Chapter 11. Cognos Analytics on Cloud On-Demand.....</b>	<b>277</b>
Migrating to Cognos Analytics on Cloud On-Demand.....	278
Managing your On-Demand subscription (for Subscription administrators).....	282
Accepting an invitation to join a Cognos Analytics on Cloud on-Demand subscription.....	282
Logging in to My IBM dashboard.....	284
On-Demand subscription roles.....	285
Adding users to your On-Demand subscription.....	286
Removing a user from the subscription.....	289
Upgrading your trial subscription.....	291
Securing your content (for On-Demand License users).....	292
IBM Secure Gateway (On-Demand only).....	293
Creating a Secure Gateway instance.....	294
Installing and configuring the Secure Gateway Client.....	296
Adding a destination.....	304
Connecting to an on-premises destination database.....	306
<b>Index.....</b>	<b>311</b>

---

# Chapter 1. Managing people

In IBM® Cognos® Analytics with Watson, you can manage user authentication and access to content and product features.

The administrator that configures your Cognos Analytics application does the initial security setup. This setup includes configuring authentication providers to take advantage of the existing security infrastructure in your organization. Each authentication provider that is configured for use with Cognos Analytics is referred to as a namespace or an external namespace.

In addition to namespaces that represent the external authentication providers, IBM Cognos Analytics has a built-in, internal namespace that is named **Cognos**. The **Cognos** namespace simplifies the process of managing access permissions and deploying content. Finally, if the **Easy install** option was used to install IBM Cognos Analytics, you can create users in the **Cognos Users** namespace.

Cognos Analytics can also be configured for anonymous access where users are not required to provide user ID and password to access the application. For information about enabling anonymous access, see the *IBM Cognos Analytics with Watson Installation and Configuration Guide*.

**Important:** Your environment might have a large number of users. As a best practice, the users should be grouped into folders, and each folder should contain a maximum of 1000 users.

The **Users, Groups, and Roles** administration capability is required to manage accounts. For more information, see [“User capabilities”](#) on page 148.

---

## The Cognos namespace and the Cognos Users namespace

The **Cognos** namespace includes predefined objects to help you quickly set up initial security. The **Cognos Users** namespace allows you to create and manage users who are not part of an authenticated external namespace.

You use the predefined objects and other features of the Cognos namespace for ongoing security management.

The **Cognos** namespace can contain groups and roles. A group is a collection of users. Users can either be members of an authenticated external namespace or of the **Cognos Users** namespace, if the **Easy install** option was used to install IBM Cognos Analytics. Members of groups can be users and other groups. A role is a collection of capabilities that identify the tasks that a user can perform. Members of roles can be users, groups, and other roles. A user can belong to several groups or roles. When a user is a member of more than one group, access permissions are merged.

The following diagram shows the structure of groups and roles in the **Cognos** namespace.

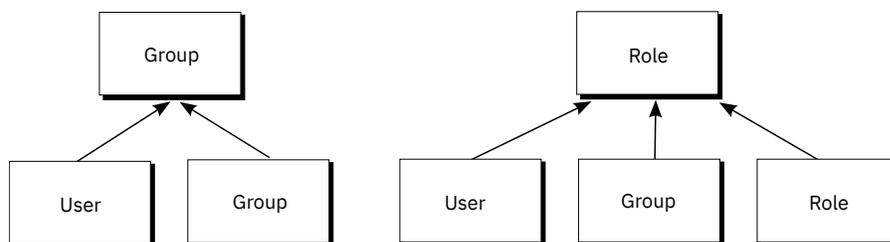


Figure 1. Structure of groups and roles

You can create groups and roles in the **Cognos** namespace. The **Cognos Users** namespace is available only if the **Easy install** option was used to install IBM Cognos Analytics with Watson. If available, you can create users in the **Cognos Users** namespace.

## Predefined and built-in objects in the Cognos namespace

Initial access permissions are applied to all predefined objects. You can modify the permissions from the object properties.

### Anonymous

This user is for the initial configuration where anonymous access is enabled and users are not prompted to provide credentials. When anonymous access is disabled in Cognos Configuration, a user logs in using their own credentials.

### 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.

### 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.

### Analysis Users

Members of this role have the same access permissions as Consumers. They can also use the IBM Cognos Analysis Studio.

### Analytics Administrators

Members have the same access permissions as Analytics Explorers. They can also access:

- **Manage > Data Server Connections**
- **Data source connections** in the Administration Console
- IBM Cognos Software Development Kit.

This role is available only after a custom installation.

### Analytics Explorers

Members have the same access permissions as Analytics Users. They can also access Planning Analytics For Microsoft Excel, Cognos Framework Manager, Cognos Cube Designer and Dynamic Query Analyzer, Transformer, and TM1 Writeback to bundled FLBI TM1 server.

This role is available only after a custom installation.

### Analytics Users

Members have the same access permissions as the Analytics Viewer members. They can create new reports, dashboards, stories, new jobs, data server connections, or data modules. They can execute reports, respond to prompts, upload files. They can also access Cognos for Microsoft Office, Cognos Workspace, Cognos Insight, Cognos Event Studio, Cognos Query Studio, and Cognos Analysis Studio

This role is available only after a custom installation.

### Authors

Members of this role 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 of this role can read and execute public content, such as reports.

### Directory Administrators

Members of this role can administer the contents of namespaces. In the Cognos namespace, they administer groups, accounts, contacts, distribution lists, data sources, and printers.

## **Analytics Viewers**

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, dashboards, and stories.

This role is available only after a custom installation.

## **Library Administrators**

Members of this role can access, import, and administer the contents of the **Library** tab in IBM Cognos Administration.

## **Mobile Administrators**

Members of this role can administer IBM Cognos Analytics Mobile Reports.

## **Mobile Users**

Members of this role can access IBM Cognos content, such as reports, through IBM Cognos Analytics Mobile Reports.

## **Modelers**

Members of this role have access to the web-based modeling capabilities.

## **Portal Administrators**

Members of this role can administer the Cognos portlets and other portlets. This includes customizing portlets, defining portlet styles, and setting access permissions for portlets.

## **PowerPlay Administrators**

Members of this role can administer the public content, for which they have full access. They can also administer and use IBM Cognos PowerPlay.

## **PowerPlay Users**

Members of this role have the same access permissions as Consumers. They can also use IBM Cognos PowerPlay.

## **Query Users**

Members of this role have the same access permissions as Consumers. They can also use the IBM Cognos Query Studio.

## **Readers**

Members of this role have read-only access to IBM Cognos software. They can navigate some portions of the content store, view saved report outputs in the portal, and use some report option such as drill-through.

## **Report Administrators**

Members of this role can administer the public content, for which they have full access. They can also use IBM Cognos Analysis Reporting and IBM Cognos Query Studio.

## **Server Administrators**

Members of this role can administer servers, dispatchers, and jobs.

## **System Administrators**

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 initial configuration for this role includes the Everyone group. You must modify the initial security settings for this role and remove the group Everyone from its membership. If you do not change the initial configuration, all users have unrestricted access to the content store.

## **Tenant Administrators**

Members of this role can perform tenant administration tasks. This role is used in a multitenant IBM Cognos environment. In the initial configuration, this role has no members and capabilities. Only System Administrators can add members and assign access permissions and capabilities for this role.

## 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 with Watson.

### References:

- For a list of default capabilities assigned to each standard role, see [“Initial access permissions for capabilities”](#) on page 159.
- To modify the membership of standard roles, see [“Securing System Administrators and standard roles”](#) on page 147.
- Another type of role is a license role. Based on license entitlements, these are the available license roles: **Analytics Administrator**; **Analytics Explorer**; **Analytics User**; **Analytics Viewer**; and **Analytics for Mobile User**. For more information, see [“License roles”](#) on page 197.

Standard role	Description
Analysis Users	Members have the same access permissions as Consumers. They can also use the IBM Cognos Analysis Studio.
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 <b>Library</b> 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.
Mobile Analytics Users	Members can access Cognos Analytics for Mobile.
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.

Table 1. Predefined Cognos standard roles (continued)

Standard role	Description
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.

## Creating and managing groups and roles

You can create new groups and roles in the **Cognos** namespace. These roles are not dependent on the authentication providers and can be managed only in IBM Cognos Analytics.

You can add users, groups, or roles from multiple external namespaces and from the **Cognos Users** namespace, if available, as members of the Cognos groups and roles.

### Before you begin

When you plan to add entries from multiple namespaces as members of the Cognos groups and roles, log on to each namespace before you start this task.

### About this task

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.

You need the **Users, Groups, and Roles** administration capability to manage accounts. For more information, see [“User capabilities”](#) on page 148.

#### 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. Click **Manage > People > Accounts**.
2. Click the **Cognos** namespace to open it.
3. Click the new group  or new role  icon, type a unique name for it in the space that is provided, and press the enter key. The group or role is added to the list of entries in the Cognos namespace.

**Tip:** You can also create groups and roles within folders. Click the new folder  icon to create a new folder.

4. Add members individually to the new group or role in the following ways:
  - a) Locate the new group or role in the Cognos namespace. To quickly find the entry:
    - 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 Type  icon to narrow the view of entries.
  - b) From the group or role More  menu, click **View members**, and click **+ Select**.
  - c) In the **Add members** panel, click the required namespace and locate the user, group, or role that you want to add. You can add members from any namespace or multiple namespaces that you are logged in to. If necessary, use the search and filter functions to find the user, group, or role to add.
  - d) Select the required users, groups, or roles. You can control-select multiple entries. Click **OK**. The selected entries are displayed on the **Members** tab.
5. To perform a bulk import of multiple members to the members tab, follow these steps:
  - a) Click  **Import**.
  - b) In the **Bulk import users** panel, enter one or more member names, separated by semicolons (;).  
Use the format *namespace/[account | group | role]*

**Tip:** To specify *account*, enter the user's given name that appears in the **Name** column after you select **People > Accounts > namespace\_name**.
  - c) Click  **Import**.
  - d) Click **Done**.
6. To remove a member, point to its name, and click the remove  icon.  
The group or role now includes members. It can also be added to another group or role.

## What to do next

The group or role More  menus provide options to manage these entries. In **Properties**, on the **Permissions** tab, you can set access permissions for the groups and roles. The **View members** option allows you to add or remove members of a group or role, and the **Add to** option allows you to add the entry to another group or role, or to a folder. With the **Copy or move** option, you can copy or move the entry to another location in the namespace. To delete the group or role, use the **Delete** option.

## Creating and managing users

You can create users in the **Cognos Users** namespace if the **Easy install** option was used to install IBM Cognos Analytics.

### Procedure

1. Click **Manage > People > Accounts**.
2. Click the **Cognos** namespace to open it.
3. Click the new user  icon, and in the **New user** dialog box, type the required information, including the user ID and password. Click **OK**.

The user name is added to the list of entries in the **Cognos Users** namespace. You can now add the user to a folder, group, or role. The user can log on to IBM Cognos Analytics with the user ID and password that you assigned for him or her.

## What to do next

A user's More  menu provides options to manage the user entry. In **Properties**, on the **General** tab in the **Advanced** properties section, you can change the user password. Also in **Properties**, on the **Permissions** tab, you can set access permissions for the user. The **Add to** option allows you to add the user to a group, role, or folder. To delete the user, use the **Delete** option.

## Customizing roles

If you are using the roles that are predefined in the Cognos namespace, you can customize themes, home pages, and report parameters that are unique to each Cognos role.

**Note:** Only Cognos roles are customizable. You cannot customize a role unless it belongs to the Cognos namespace - as either a predefined Cognos role, or one that you created yourself. For more information about Cognos roles, see the *IBM Cognos Analytics with Watson Administration and Security Guide*.

You can specify that a customized home page, or a particular report or dashboard, be displayed when a user with a particular Cognos role opens IBM Cognos Analytics with Watson. You may want to remove default user interface features for roles. In addition, you can customize parameters that can be used across reports and tailor them for each user role.

Before setting customized themes and home pages (other than a dashboard or report) you must have created and uploaded custom themes or home pages. For more information, see [Chapter 9, “Customizing Cognos Analytics across all roles,” on page 211](#).

To customize individual roles, from **Manage > People > Accounts**, click a namespace to view the list of roles for the namespace. If you click a role's More  menu and select **Properties**, the slide-out panel for that role has a **Customization** tab.

**Note:** If you want to set customizations across all roles, you use the **Managing > Customization** slide-out panel. For more information, see [“Applying themes, extensions, and views” on page 247](#).

## Setting a default home page

Click  next to the default home page. You can now browse for a dashboard or report to be the default home page, or you can select a view in the list of views to be the default home page for all users in this role.

## Hiding menu options for a feature

You can hide some menu options for a feature from users in specified roles. Click  next to **Features**. A list of views is displayed. This list includes both the built-in views and any custom views that have been uploaded. Click a view to see a high-level grouping of features for the view. Click  next to a grouping to drill-down to a lower level of features. You can deselect or select any feature in this list, or drill-down to another set of features to choose from. Click **Apply** to save your changes. You can revert your changes by clicking **Reset to defaults**.

**Important:** When you hide a menu item for a feature via customization, you do not change any user's *capability* to perform or not perform the action of the menu item. In some cases, a user can access the same functionality from a different location in the user interface. In other words, hiding a menu item does not apply security rules to a feature. To apply role-based security, you must assign capabilities. For more information, see [“User capabilities” on page 148](#).

To customize the navigation menu in reporting, expand **Reporting > Collections > Report**.

For more information, see [“Examples: Hiding menu options for a feature” on page 8](#).

## Setting a default theme

Click  next to the default theme. You can select a theme in the list of themes to be the default theme for all users in this role.

## Creating a custom folder

Click  next to **Custom folder** to set a custom content folder for users who have this role. When a user with this role logs in, the custom folder is displayed on the navigation bar below **Team content**.

## Setting the default location for uploaded files

Click  next to **Default upload location** to specify a folder in **Team content** as the default location for uploaded files for users who have this role.

## Setting the default data source to be used by the Assistant

Click  next to **Default source** to specify an asset in **Team content** that the Assistant can use as a default data source for the selected role.

## Setting default parameters for roles

Click **Settings** next to **Parameters**. A list appears of parameters that you customized. Choose the parameters that you want to configure for the role. Then select the default values that you want to appear for all users in this role. Click **Apply** then **OK** when you are done.

For more information, see "Using customized parameters" in the *IBM Cognos Analytics with Watson Reporting Guide*.

## Resolving conflicts when a user has multiple roles

A user may have multiple roles which can have different default themes or home pages. To resolve this issue, when setting customizations for a role, click **Advanced** and set a priority for the role ranging from 0 to 10. In the case of a conflict the customizations for the role with the highest priority are used. The **System Administrators** role has a hard-coded priority of 1000.

## Examples: Hiding menu options for a feature

You can hide some menu options for a feature from users in specified roles.

**Important:** When you hide a menu item for a feature via customization, you do not change any user's *capability* to perform or not perform the action of the menu item. In some cases, a user can access the same functionality from a different location in the user interface. In other words, hiding a menu item does not apply security rules to a feature. To apply role-based security, you must assign capabilities. For more information, see ["User capabilities" on page 148](#).

## Procedure

1. Log on as an administrator.
2. Go to **Manage > People > Accounts**, and click the **Cognos** namespace.
3. Click the More button  next to the role for which you want to hide menu items.
4. Click  **Properties**.
5. Click the **Customization** tab.
6. Click the chevron button  after **Features**.

The **Features** panel appears.

7. Complete the steps in one of the following examples:

### ***Disabling the greeting on the Home page***

You can remove the introductory text on the Home page for a selected role.

#### **Procedure**

1. Complete the [initial steps to remove a feature](#).
2. Click the chevron buttons  for **Home > Collections > com.ibm.bi.commonHome.sections**.
3. Deselect the check box next to **Greeting**.
4. Click **Apply**.

#### **Results**

The Home page greeting no longer appears for users in the role that you customized.

**Note:** Affected users must log out and then log back in before the change is reflected in their view of the product.

### ***Hiding the Watch video button in the Home page***

You can control which users have access to the **Watch video** button in the Home page.

For more information, see "Welcome page" in the *IBM Cognos Analytics Getting Started Guide*.

#### **Procedure**

1. Complete the [initial steps to remove a feature](#).
2. Click the chevron button  for **Home > Collections > Home page links**.
3. Clear the **Watch video button** checkbox.
4. Click **Apply**.

#### **Results**

When you log in as a user of the role for which this customization was implemented, the **Watch video** button is no longer available in the Cognos Analytics home page.

**Note:** Affected users must log out and then log back in before the change is reflected in their view of the product.

### ***Removing the Export to PDF feature from the Analysis Users role***

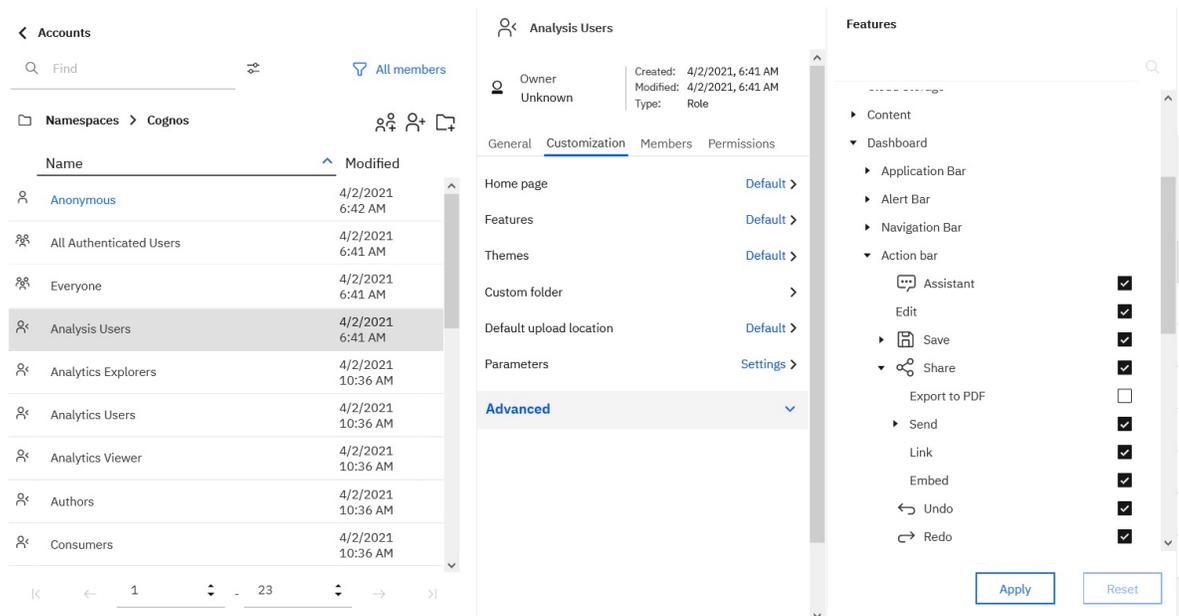
In this example, the administrator removes the **Export to PDF** option in the application bar from Analysis users who want to share dashboard content.

#### **Procedure**

1. Check the default behavior.
  - a) Log on as an Analysis user and open a dashboard.
  - b) Click the Share button  in the Action bar.  
The **Share** window appears.
  - c) Click the **Export** tab.  
The **Export to PDF** options appear.
2. Remove the Export to PDF feature for Analysis users.
  - a) Complete the [initial steps to remove a feature](#).
  - b) Click the chevron button  before **Dashboard** to expand the list.

- c) Click the chevron button  before **Action bar** to expand the list.
- d) Click the chevron button  before  **Share** to expand the list.
- e) Deselect the **Export to PDF** check box.

The Cognos Analytics window appears as follows:



- f) Click **Apply**.
3. Confirm that the feature was removed.
- a) Log on as an Analysis user and open the same dashboard.
  - b) Click the Share button  in the Action bar.
- The **Share** window appears with no **Export** tab.

## Results

The feature that you selected was removed for the role that you specified.

**Note:** Affected users must log out and then log back in before the change is reflected in their view of the product.

## Restricting users from viewing the on-demand toolbar

You can disable the on-demand toolbar from selected users, groups, or roles.

## About this task

For information about hiding the on-demand toolbar for a specific report, regardless of who is viewing it, see "Disabling the on-demand toolbar" in the *IBM Cognos Analytics Reporting Guide*.

**Important:** Turning off the on-demand toolbar will cause certain aspects of certain reports to become unavailable in HTML view. For example, if a report has both drill-through and drill-down enabled, *only* drill-through will be available to anyone looking at the report who has their on-demand toolbar disabled by either

- the following administration procedure
- the procedure to disable the toolbar for a specific report

## Procedure

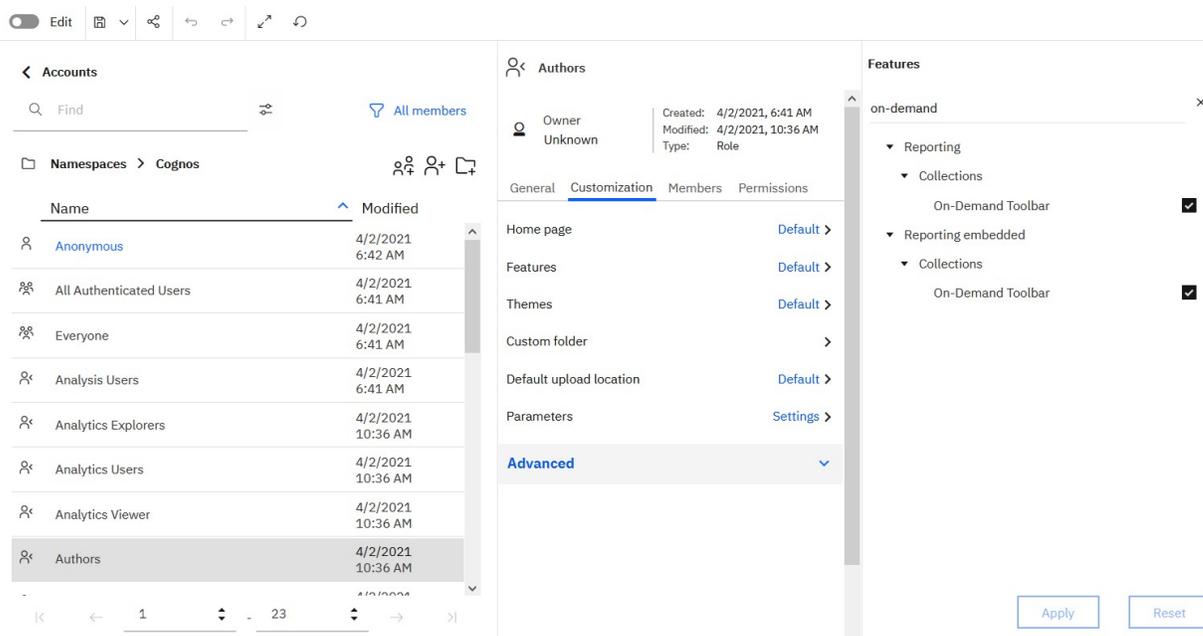
1. Complete the [initial steps to remove a feature](#).

The **Features** panel appears. However, you're not sure where in the Features tree to find the on-demand toolbar.

**Tip:** You can use the Search field to find the feature that you want to enable or disable.

2. In the Search field , type on-demand.

The search results show that you can control the on-demand toolbar appearance in reports and/or dashboards.



The screenshot shows the Cognos Analytics user interface. On the left, a list of accounts is displayed, with 'Authors' selected. The main area shows the 'Authors' role configuration, with the 'Customization' tab active. The 'Features' section is expanded, showing a search for 'on-demand'. Under 'Reporting > Collections', the 'On-Demand Toolbar' feature is checked. The 'Apply' button is visible at the bottom right.

3. Deselect the check box next to **Reporting > Collections > On-Demand Toolbar**.
4. Click **Apply**.

## Results

The on-demand toolbar does not appear for Reporting users who belong to the Authors role.

**Note:** Affected users must log out and then log back in before the change is reflected in their view of the product.

### ***Disabling a modeling feature for a role***

You can choose to make certain modeling features unavailable to selected roles.

For information about all Cognos Analytics modeling features, see "Data modeling in Cognos Analytics" in the *IBM Cognos Analytics Data Modeling Guide*.

In the following example, you do not want modelers to use newly uploaded files that reside on their local computers. You can prevent them from uploading local files to Cognos Analytics. As a result, any modeling that they perform on uploaded files will use only files that were previously uploaded to Cognos Analytics.

## Procedure

1. Complete the [initial steps to remove a feature](#).
2. Click the chevron buttons  for **Data module > Application Bar > Open menu**.
3. Deselect the check box next to **Upload files**.
4. Click **Apply**.

## Results

The **Upload files** option is no longer available in the **Open** menu  for users who belong to the Modelers role.

**Note:** Affected users must log out and then log back in before the change is reflected in their view of the product.

### ***Disabling the Run all at once option in jobs***

You can prevent users from creating a job in which every report is run at once.

For information about jobs, see "Creating a job to schedule multiple entries" in the *IBM Cognos Analytics Getting Started Guide*.

### **Example**

In this example, you want to prevent reports in a job from running simultaneously to improve your server performance. You decide to disable the **Run all at once option** in jobs created by people in the **Analytics Explorers** role.

## Procedure

1. Complete the [initial steps to remove a feature](#).
2. Click the chevron buttons  for **Jobs > Collections**.
3. Deselect the check box next to **Run all at once**.
4. Click **Apply**.

## Results

The **Run all at once** option is no longer available in the **Run options** panel of jobs created by users in the **Analytics Explorers** role.

**Note:** Affected users must log out and then log back in before the change is reflected in their view of the product.

### ***Hiding the Properties pane in reports***

You can control which users have access to the **Properties** pane in reports.

For more information, see "Properties pane" in the *IBM Cognos Analytics Reporting Guide*.

## Procedure

1. Complete the [initial steps to remove a feature](#).
2. Click the chevron buttons  for **Reporting > Collections > Toolbar**.
3. Deselect the check box next to **Propertes**.
4. Click the chevron buttons  for **Data sets > Collections > Toolbar**.
5. Deselect the check box next to **Properties**.
6. Click **Apply**.

## Results

In Cognos Analytics Reporting, the **Properties** pane is no longer available in both the Data sets and Authoring perspectives to users in the role that you customized.

**Note:** Affected users must log out and then log back in before the change is reflected in their view of the product.

### ***Hiding the More button in reports***

You can control which users have access to the **More** button  in the top-level toolbar in reports.

## Procedure

1. Complete the [initial steps to remove a feature](#).
2. Click the chevron buttons  for **Reporting > Collections > Toolbar**.
3. Deselect the check box next to **More**.
4. Click the chevron buttons  for **Data sets > Collections > Toolbar**.
5. Deselect the check box next to **More**.
6. Click **Apply**.

## Results

In Cognos Analytics Reporting, the **More** button is no longer available in both the Data sets and Authoring perspectives to users in the role that you customized.

**Note:** Affected users must log out and then log back in before the change is reflected in their view of the product.

## Authentication providers

---

User authentication in IBM Cognos Analytics with Watson is managed through authentication providers. Authentication providers define users, groups, and roles that are used for authentication. User names, IDs, passwords, regional settings, personal preferences are some examples of information stored in the providers.

In the Cognos Analytics user interface, authentication providers are represented by namespaces .

Cognos Analytics supports the following types of authentication providers:

- Active Directory
- OpenID Connect
- Custom Java Provider
- OpenID Connect Authentication Proxy
- IBM Cognos Series 7
- LDAP
- SAP
- SiteMinder

Authentication providers are configured in IBM Cognos Configuration, under the **Security > Authentication** category. After the provider namespace is added there, and the **IBM Cognos** service is restarted, the namespace name is displayed in **Manage > People > Accounts**, and users can log on to Cognos Analytics using that namespace. For more information about configuring authentication providers, see the *IBM Cognos Analytics with Watson Installation and Configuration Guide*.

You cannot create users, groups, or roles in authentication providers' namespaces from Cognos Analytics. However, you can add users, groups, and roles from these namespaces to groups and roles in the **Cognos** namespace.

## Multiple namespaces

If multiple namespaces are configured for Cognos Analytics, at the start of a session you must select one namespace. 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 that 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 to do that, 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 Cognos Configuration to enable anonymous access.

## Managing OpenID Connect namespaces

Use the **OpenID Connect** namespace type to implement OpenID Connect authentication for IBM Cognos Analytics with Watson.

Cognos Analytics supports the following OpenID Connect identity providers. This list may expand over time:

- ADFS (Active Directory Federation Services)
- Azure AD (Active Directory)
- Generic
- Google
- IBM Cloud Identity
- IBMid (IBM identity provider)
- MS Identity
- OKTA
- Ping
- Salesforce
- SiteMinder

IBMid is the IBM Identity Service, a cloud-based identity access and management solution that provides identity and single sign-on services for IBM applications.

After an OpenID Connect namespace is configured in IBM Cognos Configuration, all OpenID Connect users have access to Cognos Analytics. When the users log on, their names are automatically shown in the namespace.

**Note:** To set up an OpenID Connect namespace successfully, ensure that the Content Manager computer can access the OIDC IDP (Identity Provider). In some cases, if there is a proxy between the Content Manager and the IDP, Content Manager will not be able to connect.

As a system administrator, you might need to restrict the number of users who can access the product based on the number of licenses or other factors. To do that, perform the following optional steps:

- Add a limited number of users to the **OpenID Connect** namespace.

See step [“3”](#) on page 15 below.

- Add groups to the **OpenID Connect** namespace.

See step [“4”](#) on page 15 below.

- Add the **OpenID Connect** users to groups or roles in the **Cognos** namespace.

By using the **Cognos** groups and roles, you can quickly assign the required access permissions for different users.

- In IBM Cognos Configuration, under **Security > Authentication**, set the **Restrict access to members of the built-in namespace** property to true.

Only members of the built-in **Cognos** namespace can now access Cognos Analytics.

## Procedure

1. Log on to IBM Cognos Analytics with Watson as a system administrator.
2. Log on to the **OpenID Connect** namespace.
3. To add user accounts to the **OpenID Connect** namespace:
  - a) Navigate to **Manage > People > Accounts**, and open the **OpenID Connect** namespace.
  - b) To add an individual user account, follow these steps:
    - Click the New user icon .
    - The **Add users** panel appears.
    - Enter a unique name in the **Unique identifier** field.  
For example, enter the user's email address.
    - In the **Preferred Name** field, enter the name that you want to appear in the namespace list.
    - Click **Add**.The **Preferred Name** value appears in the namespace list.
  - c) To add multiple user accounts at once, you can import a .csv file specially formatted with account information:
    - Ensure that you created the .csv file that contains your user information.  
For more information, see [“Creating a .csv file containing user account information” on page 16](#).
    - Click the Import icon  and then select **Import users**.
    - Double click the .csv file that has the user information.  
The file is uploaded and the defaultName values from the .csv file are listed in the OpenId Connect namespace.  
The same .csv file can be imported many times. If a defaultName value already exists in the namespace, the user account is updated. You can also repeat the import if previously imported entries look incorrect.  
Repeat this step for other files, if you have multiple files.
4. To add groups to the **OpenID Connect** namespace:
  - a) Navigate to **Manage > People > Accounts**, and open the **OpenID Connect** namespace.
  - b) To add individual groups, follow these steps:
    - Click the New group icon .
    - Enter the name of the new group.  
The group name is listed in the namespace.
  - c) To add multiple groups at once, you can import a .csv file specially formatted with group information:
    - Ensure that you created the .csv file that contains your group information.  
For more information, see [“Creating a .csv file containing group information” on page 17](#).
    - Click the Import icon  and then select **Import groups**.
    - Double click the .csv file that has the group information.  
The file is uploaded and the defaultName values from the .csv file are listed in the OpenId Connect namespace. The same .csv file can be imported many times. If a group already exists in the namespace, the group is updated. You can also repeat the import if previously imported entries look incorrect.

Repeat this step for other files, if you have multiple files.

5. Add the **OpenID Connect** users to groups or roles in the **Cognos** namespace.
  - a) Open the **Cognos** namespace, and find the group or role to which you would like to add users from the **OpenID Connect** namespace.
  - b) From the group or role context menu , select **View members**.
  - c) Click  **Select**.
  - d) In the **Add members** panel, select your **OpenID Connect** namespace, and then select the appropriate users. You can select multiple users at once.
  - e) Click **Add**. The selected users are displayed on the **Members** tab.
  - f) Repeat the steps to add the **OpenID Connect** users to other **Cognos** groups or roles.
  - g) To import users from a .csv file, click **Import**, and select the file. For more information, see [“Creating a .csv file containing user account information” on page 16](#).

The same .csv file can be imported many times. If a user account already exists in the namespace, the account is updated. You can also repeat the import if previously imported entries look incorrect.

Repeat this step for other files, if you have multiple files.

6. Delete an entry by clicking **Delete** in the context menu  next to the specific group, role, or folder.

## Results

Users who use the **OpenID Connect** namespace to log on to Cognos Analytics are redirected to an external logon page where they can type their credentials. If the credentials are accepted, the users can access Cognos Analytics.

## Creating a .csv file containing user account information

The .csv file that contains the list of users to be imported into the OpenID Connect namespace must be properly formatted for the import to be successful.

The first row in the file is the header. This row must contain the `camIdentity` column, and can contain the following, optional columns: `defaultName`, `businessPhone`, `faxPhone`, `givenName`, `homePhone`, `mobilePhone`, `pagerPhone`, `postalAddress`, `surname`, `userName`.

**Tip:** All of the column names are properties of the account class in IBM Cognos Analytics. The names are case sensitive, and must be typed exactly as specified in this document.

All other rows in the file contain values corresponding to the columns specified in the first row.

Here is an example of a .csv file with two users:

- Row 1: `camIdentity,defaultName,givenName,surname`
- Row 2: `Andy.Bergin@ca.ibm.com,Andy Bergin,Andy,Bergin`
- Row 3: `Kirsten.Vaughan@ca.ibm.com,Kirsten Vaughan,Kirsten,Vaughan`

You can add all your users to one .csv file, or you can create multiple files with fewer names in each file.

After the file is imported, the `defaultName` for the user is set in the following way:

- If `defaultName` is specified in the .csv file, the name is used.
- If `defaultName` is not specified in the .csv file, but `givenName` and `surname` are specified, the default name is set as `givenName surname`.
- If `defaultName`, `givenName`, and `surname` are not specified, the `camIdentity` is used as the default name.

Multiple users can have the same first and last names. To avoid potential conflicts, specify a different `defaultName` for the users, or do not specify `surname` and `givenName` for them. You can also modify the `surname` by adding a unique character or number to it, such as `Simpson1` or `Simpson2`.

**Note:** Properties are automatically updated from the namespace provider when the user logs in. Therefore, if the namespace supports properties such as `timeZone` or `localePreference`, they are saved in the account proxy when the user logs in.

## Creating a .csv file containing group information

A group .csv file contains the list of groups to be imported into the OpenID Connect namespace. This file must be properly formatted for the import to be successful.

The first row in the group .csv file is the header. This row must contain both the `type` and `defaultName` columns. The header row can also contain the following, optional column: `tenantID`.

**Tip:** All of the column names are properties of the group class in IBM Cognos Analytics. The names are case sensitive, and must be typed exactly as specified in this document.

All other rows in the file contain values corresponding to the columns specified in the first row.

Here is an example of a .csv file with two groups:

- Row 1: `type,defaultName`
- Row 2: `group,Reviewers`
- Row 3: `group,Data-Scientists`

You can add all your groups to one .csv file, or you can create multiple files with fewer groups in each file.

## Finding users, groups, and roles

---

As an administrator, you often need to locate the users, groups, or roles in the namespace that you manage.

In the **Namespaces** view in **Manage > People > Accounts**, you see all the namespaces  that are configured for use with IBM Cognos Analytics with Watson, the **Cognos** namespace, and the **Cognos Users** namespace, if applicable. You can navigate only the namespaces that you are logged in to, and the **Cognos** and **Cognos Users** namespaces.

### Searching for entries

A namespace might contain thousands of users and numerous groups, roles, and folders, and the only way to find these entries is by using the search capability in **Accounts**. You must search for entries in one namespace at a time so you need to select the namespace first, and then type text in the  **Find** field.

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. The search is also used when you add members of groups and roles, specify access permissions, and so on.

### Filtering entries

You can filter on users, groups, and roles to narrow your view of entries. When using with search, specify the filter criteria for faster response. Click the filter  icon and select or clear the filter options.

### Sorting entries

Click **Name** to sort entries by name, ascending alphabetically. Click **Name** again to sort entries by name, descending alphabetically. Click **Modified** to sort entries by newest to oldest. Click **Modified** to sort the entries by oldest to newest.

## Paging

If your namespaces have many entries, and you [enabled](#) account entries to be loaded by pages, you can navigate more quickly between pages to find the [entries](#) you want.

## Creating contacts, distribution lists, and folders

---

Create contacts and distribution lists for people who can be recipients when reports are delivered by email.

Use distribution lists if you want to send a report to more than one recipient at a time. Distribution lists contain a collection of users, groups, roles, contacts, or other distribution lists.

If a recipient is not part of the IBM Cognos security system, you can create a contact for this person. The contacts you create can also be assigned as contacts for reports. You can create folders to organize your entries in a logical way.

Note that if you choose the email recipient from a list, such as a group, role, or distribution list, you must have read access to both the list and the recipient's email account. Otherwise, the report delivery fails.

### Creating contacts

If a recipient is not part of the IBM® Cognos® security system, you can create a contact for this person.

#### Procedure

1. Click **Manage > People > Contacts**.
2. Click the New icon , and then click **Contact** .
3. Enter the name and email address of the person.
4. Click **Create**.

The contact name appears in the **Contacts** panel.

#### What to do next

As you would with a user name in the **Cognos Users** namespace, you can click a contact's More icon , click **Properties**, and then have these options:

- On the **General** tab under **Advanced**, you can disable or hide the contact.
- On the **Preferences** tab, you can specify the contact's default format, their time zone, and the language of their Cognos Analytics content.
- On the **Permissions** tab, you can set access permissions for the contact. For more information, see [“Setting access to user capabilities” on page 158](#).

You can also [add the contact to a distribution list](#).

### Creating distribution lists

Use distribution lists if you want to send a report to more than one recipient at a time.

Distribution lists can contain a combination of users, groups, roles, contacts, or other distribution lists.

#### Procedure

1. Click **Manage > People > Contacts**.
2. Click the New icon , and then click **Distribution list** .
3. Enter a name for the distribution list.
4. Click **Create**.

The distribution list name appears in the **Contacts** panel.

5. To add users, groups, roles, contacts, or other distribution lists to the distribution list, follow these steps:

a) Click the distribution list name.

b) Click the **Members** tab.

c) Click the Add icon .

d) Locate the entry in the **Cognos** or **Cognos Users** namespace. To quickly find the entry:

- Type text in the  **Search** 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.

- Click the Sort icon . You can then specify that search results are sorted by name, by date modified, or by type. You can also choose whether the results appear in ascending or descending order.

**Tip:** As search results appear, you can change your options for search method, filtering, and sorting. The results update dynamically with each change that you make.

e) Select the entries. You can control-select multiple entries.

**Tip:** You can add members from any namespace or multiple namespaces that you are logged in to.

f) Click **Add**.

The selected entries are displayed on the **Members** tab.

g) To remove a member, point to its name, and click the Remove  icon.

## What to do next

If you click a contact's More  menu, and then click **Properties**, you have these options:

- On the **General** tab under **Advanced**, you can disable or hide the distribution list.
- On the **Members** tab, you can edit the list of members.
- On the **Permissions** tab, you can set access permissions for the distribution list. For more information, see [“Setting access to user capabilities” on page 158](#).



---

## Chapter 2. Managing content

The most common reasons for you to backup and restore content are when you want to move content from a test environment to a production environment as part of the application development process, or to prepare to upgrade to a new version of the product.

The **Configure and manage the system** administration capability is required to manage content.

### Deployment planning

The process of backing up and restoring content is called a deployment. For security settings to work when you deploy content, the source environment and the target environment must use the same namespaces for policies, users, roles, and groups to work correctly. The Cognos namespace is included when you create a backup. Ensure that the other required namespaces are configured in the target environment before restoring the content.

If the deployment is part of an upgrade, before you create a backup you can run a consistency check to find and fix inconsistencies within the content store or between the content store and external namespaces. You run a consistency check from the **Administration console > Configuration > Content administration > New consistency check**.

### Backing up content

To protect sensitive information, all backups are encrypted. When you restore the content, you must provide the password set when the backup was created.

The backup is saved as an archive file (.zip) in the **Deployment files location** specified in Cognos Configuration. The default location is *install\_location\deployment*. To deploy the content store in a different instance of IBM Cognos Analytics with Watson, such as the computer used for the production environment, copy the archive file to the deployment files location on the target computer to make the file available to restore.

A backup includes the following content.

- public folders
- packages
- reports
- data sources
- distribution lists and contacts
- printer configuration
- access permission settings
- the Cognos namespace
- deployment specifications

Personal entries for each user, such as reports and folders from the user's **My Content**, are not included in the backup.

### Restoring content

To restore content, the backup file you want to use must be in the **Deployment files location** specified in Cognos Configuration. The default location is *install\_location\deployment*. You must provide the password that was set when the backup was created.

When you restore content, the contents of the target content store are removed and replaced by the contents of the source content store.



---

## Chapter 3. Configuring content sharing

You can configure Cognos Analytics so that users can send their content in Slack, in Microsoft Teams, or by Email.

**Tip:** You can also customize this feature to restrict how people in selected roles are able to send content. For more information, see [“Example: Selectively disabling content sharing by email”](#) on page 28.

For information, see "Sharing content" in the *IBM Cognos Analytics Getting Started Guide*.

---

### Integrating with a collaboration platform

If your company uses Slack\* or Microsoft Teams, you can integrate your preferred collaboration tool with Cognos Analytics. Cognos Analytics users can then connect to Slack or Microsoft Teams to share messages and Cognos Analytics content with other users.

For information about the initial access permissions that are granted for administering collaboration, see "Collaboration Administration" in the "Initial access permissions for capabilities" section of the *IBM Cognos Analytics Administration and Security Guide*.

For information about how users can share their content, see the *IBM Cognos Analytics Getting Started Guide*.

**Note:** Collaboration platforms in IBM Cognos Analytics are not created by, affiliated with, or supported by either Slack Technologies or Microsoft.

### Creating a Slack application

In Slack, create an application so that you can connect to Slack from within Cognos Analytics.

#### Before you begin

Your company must have a registered Slack account.

#### Procedure

1. Go to <https://api.slack.com/apps>
2. Sign into the slack account for your company.
3. Click **Create New App**.
4. In the **Create a Slack App** dialog, enter a name for your application, for example, type Cognos Analytics, and select **Development Slack Workspace**.
5. Select the workspace that you signed in to.
6. Click **Create App**.  
The Slack application is created
7. On the **Slack API** page, click the **Basic information** tab and scroll down to the **App Credentials** section.
8. Make a note of both the **Client ID** and the **Client Secret** values. You will need them when configuring Slack in Cognos Analytics.  
**Tip:** Click the **Show** button in each field to see the values.
9. In the **Features** section, click **OAuth & Permissions**.
10. In the **Redirect URLs** section, add the following Redirect URL:

`https://ca_servername:port/bi/v1/collaboration/auth/slack`

where `ca_servername:port` is the fully qualified name and port number of your Cognos Analytics server.

**Tip:** You must specify `https` at the start of the URL, as Slack does not permit the `http` protocol. You can configure multiple redirect URLs. This allows you to use the same Slack application in multiple Cognos Analytics environments, for example, "Dev", "Test", and "Prod".

11. Click **Add**.
12. Click **Save URLs**.
13. If you don't have administration access to your Slack workspace, follow these steps:
  - a) Go to the **Scopes** section and, in the **Select Permission Scopes** field, select **Access your workspace's profile information users:read**.
  - b) Click **Save changes**.
  - c) Scroll up to the **OAuth Tokens & Redirect URLs** section and click on **Request approval**.

After your request is approved by the Slack admin, you receive a message from slackbot indicating that your request was approved. The **Install app to workspace button** appears in the **OAuth & Permissions** section of your app.

- d) Click **Install app to workspace**.
14. Confirm that your Slack workspace is working.
  - a) If not done already, install Slack on your computer.
  - b) Sign into your Slack app using the email account and password that you used to create the Slack app.
  - c) Test your Slack workspace.

**Tip:** For information about setting up and using Slack, see the documentation available at [www.slack.com](http://www.slack.com).

## What to do next

You are now ready to “[Adding a collaboration platform in Cognos Analytics](#)” on page 25.

## Creating a Microsoft Teams application

In Microsoft Teams, create an application so that you can connect to Microsoft Teams from within Cognos Analytics.

### Before you begin

Your company must be using the Microsoft 365 developer program with an E5 subscription (<https://developer.microsoft.com/en-us/microsoft-365/dev-program>).

**Note:** An E5 subscription is required because Cognos Analytics requires access to Graph API.

### Procedure

1. Create an Azure service named Azure Active Directory.

For more information, see [Manage Azure Active Directory](https://portal.azure.com/?quickstart=True#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~~/Overview) ([https://portal.azure.com/?quickstart=True#view/Microsoft\\_AAD\\_IAM/ActiveDirectoryMenuBlade/~~/Overview](https://portal.azure.com/?quickstart=True#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~~/Overview)).
2. Sign in to the Azure portal using an account with administrator permission.

**Note:** You must use an account in the same Microsoft 365 subscription (tenant) as the one in which you are registering the MS Teams application. You can also access the Azure portal through the Microsoft 365 Admin center by expanding the **Admin center** item in the left navigation pane and selecting **Azure Active Directory**.
3. In the Azure portal, select **Azure Active Directory** in the left pane, select **App registrations**, and click **New registration**.
4. In the **Register an application** page, enter your application's registration information:
  - a) In the **Name** section, enter a meaningful application name that will be displayed to the users.
  - b) Select **Accounts in any organizational directory** in the **Supported account types** section.

c) In the **Redirect URI** field, type the following:

`https://host_name:port_number/bi/v1/collaboration/auth/msteams`

or

`https://web_server_name:443/virtual_directory/bi/v1/collaboration/auth/msteams`

d) Click **Register** to create the application.

5. On the app **Overview** page, hover over the **Application (client) ID** value and click the **Copy to clipboard** icon to copy the value.

**Note:** You will need to specify this value in your application's authentication code or `app.config` file, where appropriate.

6. Click the **Manifest** tab.

7. In the Manifest Editor, set the `allowPublicClient*` property to `true`, and then click **Save**.

8. Click the **API permissions** tab.

9. Click **Add a permission**, and then set permissions according to the following table:

**Note:** The permissions in the table must be granted by the administrator.

Permission name	Description	Admin consent request
user.read.all	Read all users' full profiles	Yes
directory.read.all	Read directory data	Yes
channelMessage.send	Send channel messages	No
channelSettings.read.all	Read the names, descriptions, and settings of channels	Yes
group.read.all	Read all groups	Yes
groupMember.read.all	Read group memberships	Yes
chat.readBasic	Read names and members of user chat threads	No
chatMember.read	Read the members of chats	Yes
chatMessage.Send	Send user chat messages	No
chat.create	Create a chat with single or multi	No

10. Search for and choose **Dataverse** in the **APIs my organization uses** tab. If Dataverse is not found, search for "Common Data Service".

11. Click **Delegated permissions**, check the options, and then click **Add permissions**.

12. Go to **Certificates & secrets** and click **New client secret** to create an application secret key.

## What to do next

You are now ready to [“Adding a collaboration platform in Cognos Analytics”](#) on page 25.

## Adding a collaboration platform in Cognos Analytics

You can connect Cognos Analytics to a third party collaboration platform, such as Slack or Microsoft Teams. This allows Cognos Analytics users to share Cognos Analytics content with each other.

### Before you begin

Before you configure collaboration in Cognos Analytics, you must do one of the following:

- [Create a Microsoft Teams application](#).

- [Create an application in Slack](#).

## Procedure

1. Ensure that you have been assigned the Collaboration Administration capability.
2. Log on to Cognos Analytics.
3. In the **Manage > Collaboration** slide-out panel, click the **Add collaboration platform** icon **+**.
4. Enter a name for the collaboration platform, for example, Cognos Analytics collaboration.
5. In the **Settings** tab, enter the following collaboration platform details:
  - Client ID  
Enter the Client ID that you noted when you created the [Slack](#) or [Microsoft Teams](#) application.
  - Client Secret  
Enter the Client Secret that you noted when you created the [Slack](#) or [Microsoft Teams](#) application.
  - Workspace URL (Slack only)  
If you are adding a Slack collaboration platform, enter the workspace URL that [you registered with Slack](#), except for the `.slack.com` at the end.
  - Tenant ID (Microsoft Teams only)  
If you are adding a Microsoft Teams collaboration platform, enter the tenant ID that you used when you created and [registered the app in Azure](#).
6. Click the **Add workspace** icon **+**.
7. Click **Test**.
8. If you are not authenticated already by the Slack or Microsoft Teams workspace, a message may appear asking you to sign in. Use your Slack or Microsoft Teams credentials to sign in.
9. Click **Save**.

## Results

The collaboration platform is created. The platform name appears in the **Manage > Collaboration** slide-out panel. To see its associated workspaces or to add additional ones, click the platform name and scroll down in the slideout panel.

## What to do next

If you want to disable your Collaboration platform for Cognos Analytics users, click the **General** tab and then select the **Disable this entry** check box. Users will still see the **Collaboration** icon in the toolbar. However, the platform name will be inactive and grayed out.

If you want to hide your Collaboration platform from Cognos Analytics users, click the **General** tab and then select the **Hide this entry** check box.

**Note:** If users selected the **Show hidden entries** check box under **My preferences > General** tab, they will see the collaboration platform name in grayed out text. If they did not select **Show hidden entries**, they will not see the name.

If you click the name of the collaboration platform and then click the **Permissions** tab, you can control the access that different users, roles, and groups have to the collaboration platform. You can assign one of three values:

- **Full** - allows administrative access to the collaboration platform
- **Read** - allows users to send Microsoft Teams or Slack messages via the collaboration platform
- **Deny** - hides the collaboration platform from the selected user, group, or role, preventing them from using it to send messages

## Microsoft Teams not available when sharing content

When you try to share content via Microsoft Teams, the Teams *collaboration\_platform\_name* does not appear in the **Share** window, even though you previously configured it.

This issue can occur if the following events occurred, in the order shown:

1. You were running a version of Cognos Analytics that was earlier than 11.2.3.
2. You manually updated the value of the advanced property `Collaboration.supportedPlatforms`.
3. You upgraded to version 11.2.3 (or later).

In this case, the property value that you had set was preserved after the upgrade, even though Microsoft Teams was introduced in 11.2.3 as a valid collaboration platform.

### Solution

To resolve this issue, manually update the `Collaboration.supportedPlatforms` property again:

1. Log in to Cognos Analytics as a System Administrator.
2. Click **Manage > Configuration > System**, and then select **Advanced Settings**.
3. Type `Collaboration.supportedPlatforms` in the **Key** field.
4. Confirm that the value in the **Value** field does not include the `msteams` option.
5. In the **Value** field, type the following:  
`slack, email, msteams`
6. Click **Apply**.
7. Refresh the page.

The next time a user shares content, the **Microsoft Teams** option will appear in the **Share** panel.

## Enabling content sharing by email

---

Configure a mail server to allow users to share Cognos Analytics content in an email.

### Procedure

1. In the location where Content Manager is installed, start IBM Cognos Configuration.
2. In the **Explorer** window, under **Data Access**, click **Notification**.
3. In the **Properties** window, for the **SMTP mail server** property, type the host name and port of your SMTP (outgoing) email server.

To be able to open content that is sent by email, you must change the host name portion of the **Gateway URI** from `localhost` to either the IP address of the computer or the computer name. Otherwise the URL in the email will contain `localhost`, and remote users will not be able to open the content.

To be able to open content that is sent as links, ensure that the **Gateway URI** on report servers and notification servers specifies an accessible web server hosting IBM Cognos content. If you have mobile users accessing links remotely, consider using an external URI.

4. Click the **Value** box next to the **Account and password** property, and click the edit button when it appears.
5. Type the values in the **Value - Account and password** dialog box, and click **OK**.

If logon credentials are not required for the SMTP server, remove the default information for the **Account and password** property. When you are prompted for confirmation to leave this property blank, click **OK**. Ensure that the default user name is removed. Otherwise, the default account is used and notifications do not work properly.

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

7. In the **Explorer** window, right-click **Notification**, and click **Test**.

IBM Cognos Analytics with Watson tests the email server connection.

## Results

Users can now select **Email** as a collaboration platform when they share their Cognos Analytics content.

## Example: Selectively disabling content sharing by email

You can control precisely which scenarios allow Cognos Analytics content to be sent by email by customizing **1.** specific roles or **2.** all roles.

In this example, you have enabled content sharing by email for all users. However, you now want to prevent only people in the Analytics Users role from sending Cognos Analytics report or dashboard content.

**Tip:** If you wanted to disable the sharing of content by email for everyone, you could customize the feature for all roles.

## Procedure

1. Log on as an administrator.
2. Go to **Manage > People > Accounts**, and click the **Cognos** namespace.
3. Click the More icon  next to the **Analytics Users** role.
4. Click  **Properties**.
5. Click the **Customization** tab.
6. Disable email content sharing for both dashboard content and report content.
  - a) Click the chevron button  after **Features**.
  - b) Click the chevron button  before **Reporting** to expand the list.
  - c) Click the chevron button  before **Collections** to expand the list.
  - d) Click the chevron button  before **Toolbar** to expand the list.
  - e) Click the chevron button  before  **Share** to expand the list.
  - f) Click the chevron button  before **Send** to expand the list.
  - g) Deselect the **Email** check box.

**Tip:** This action also deselects the **Email** check box for **Dashboards**, because email sharing is a feature common to both dashboards and reports.

- h) Click **Apply**.

---

## Chapter 4. Managing data access

IBM Cognos Analytics with Watson supports data servers, data modules, packages, data sets, and uploaded files as sources of data.

### Data servers

---

A data server defines the physical connection to a database or a cube.

A data server connection specifies the parameters that are needed to connect to the database or cube, such as the location of the database and the timeout duration. Authentication information can also be included in the connection.

IBM Cognos Analytics with Watson supports multiple relational and OLAP data servers. The list of supported data server types might change from release to release. For information about the currently supported data server types, follow these steps:

1. Go to the [IBM Cognos Analytics on Premises 11.2.x: Supported Software Environments](https://www.ibm.com/support/pages/node/6440667) website (<https://www.ibm.com/support/pages/node/6440667>).
2. Scroll to the 11.2.x release you want.
3. Under **Requirements by type**, click **Software**.
4. Select the **Supported Software** tab.
5. Click **Data Sources**.

A table appears showing details of all the supported data sources for the Cognos Analytics release that you selected.

If you include database authentication information, such as the Cognos Analytics credentials or a signon, for the connection, users need not enter database authentication information each time the connection is used. The signon that is produced when you create a data server connection is by default available to the **Everyone** group. You can modify the signon permissions from the properties of the data server connection.

#### Data server versus data source

In the legacy **IBM Cognos Administration** user interface, the equivalent of **Data server** is **Data source** that has the JDBC connection specified.

Data sources do not appear in **Manage > Data server connections** until you enable web-based modeling for the data source connections. To do that, go to **Manage > Administration console > Configuration > Data source connections**, and select the **Allow web-based modeling** check box on the connections. Only data sources with JDBC connections have this check box.

### Creating a data server connection

A data server connection specifies the parameters that are needed to connect to the database or the cube that the connection represents.

Each data server can have one or more connections. The connection names must be unique.

#### Before you begin

Most data server connections require a database vendor-supplied JDBC driver. Use a version of the JDBC driver that is compatible with Java™ Runtime Environment version 8. Copy the driver to the Cognos Analytics *installation\_location*\drivers directory, and restart the query service. Restarting the full **IBM Cognos** service is not necessary.

To create data server connections, you need the **Data Source Connections** administration capability. Certain roles, such as **Analytics Explorers** and **Analytics Users**, have this capability by default. For more information, see [“Setting access to user capabilities”](#) on page 158.

**Note:** If you want to connect to a data server using an SSL certificate that is located on the cloud, see [“Securing your data server connection using a cloud-based certificate”](#) on page 31.

## Procedure

1. Click **Manage > Data server connections**.
2. On the **Data server connections** page, click **Add data server**.
3. Define the data server type.
  - a) Add a name and description (optional) for the connection.
  - b) In the **Connection type** field, select a data server type or start typing to quickly find the connection type that you want.
  - c) If you are a System Administrator, you can select a tenant.
  - d) Click **Next**.
4. Enter the connection details.

For most connections, you must specify the JDBC URL. You can view the syntax and example URL under connection details. You might need to ask the database administrator for more details, or check the database vendor documentation.

In the **Connection properties** box, type the supported property name. For information about the supported JDBC properties, see [“Cognos-specific connection parameters”](#) on page 61.

For **IBM Planning Analytics** connections, specify the TM1 database host and HTTP port number. To use an SSL connection, select the **Use SSL** check box.

If you are connecting to a data server using an SSL certificate in a Cloud Object Storage location, read about how to [specify S3 header information](#).

- a) Select an isolation level from the list.
- b) Under **Authentication method**, specify how to access the data server.  
You can select one of the following options.

### **Connect anonymously or Integrated security**

Choose the **Connect anonymously** option when anonymous access to the data server is allowed.

Choose the **Integrated security** option when the TM1 database is configured for Integrated Security mode 4 or 5. This option is applicable for **IBM Planning Analytics** connections only.

### **Prompt for the user ID and password**

Choose this option when the user must be prompted for database credentials with each use.

### **Use an external namespace**

Choose this option to secure the connection against a namespace that is configured for Cognos Analytics. Use the drop-down menu to select one of the available namespaces.

Cognos Analytics logs on to the data server with the credentials that are used to authenticate to the selected namespace. The namespace must be active, users must be logged on prior to accessing the data server connection, and the authentication credentials that are used for the namespace must be relevant for the data server authentication.

Typically, this authentication method is used in the following situations:

- You want Cognos Analytics to pass through to the database the user ID and password that is presented to the portal during authentication.
- You want Cognos Analytics to use Kerberos authentication.

- You want Cognos Analytics to use JSON Web Token (JWT) authentication.

The query server determines the credential information that is provided by the external namespace, and chooses which connection method to attempt.

### Use the following signon

Choose this option to assign a signon for the connection.

Select the signon from the drop-down list, or create a new signon by clicking the add icon **+**. In the **New data server connection** window on the **Credentials** tab, type a user ID and password.

To restrict the signon to particular users, roles, or groups, on the **Permissions** tab, click the add icon **+**, and specify the access permissions for the signon.

- c) Click **Test connection** to verify that the data server connection works.

**Tip:** If the test fails, click **View result**. You can copy the error details to the clipboard to help you troubleshoot the cause.

- d) Click **Next**.

The **Commands** page appears.

5. If you want, you can select commands that you want the database to execute. For more information, see [Command blocks](#).
6. Click **Create**.

## Results

The new connection name is displayed on the **Data server connections** page. To edit the data server connection, including adding or modifying its signon, click the connection name.

**Note:** The following message may appear:

MSR-GEN-0026 The schema "*schema\_name*" is either empty, or not accessible using the current signon

This message could mean, as stated, that the schema is empty (has no objects) or that the user does not have access to it. However, the message could also mean that the schema simply has no TABLE objects, such as TABLE, VIEW, or a SYNONYM to a TABLE/VIEW object, yet still contains other object types. In this scenario, the produced message is incorrect.

## What to do next

To use a data server as a source for reports, dashboards, explorations, and other Cognos Analytics content, create data modules that are based on the connection.

For relational data server connections, you must preload the schema metadata to make the schema available to create data modules in the modeling component. For more information, see [“Loading metadata”](#) on page 69.

For **IBM Planning Analytics** connections, you can create data modules directly from the connection user interface. For more information, see [“Creating data modules from Planning Analytics cubes”](#) on page 78.

## Securing your data server connection using a cloud-based certificate

If you want to create a connection to a data source that is secured with SSL encryption, you must specify a valid SSL certificate. This certificate may be stored externally in a Cloud Object Storage (COS) location.

Using an SSL certificate that is stored externally provides these benefits:

- Your Cognos Analytics environment does not have to be accessed by the certificate.
- You don't need to import certificates into different keystores, as they do when imported to a local environment.
- You don't need to import certificates to multiple Cognos Analytics servers.

If your database vendor supports the inclusion of a certificate's location in the jdbc URL, you can use this feature. See your database vendor's documentation for the following information:

- a list of supported certificate types
- samples of jdbc URLs

### Step 1: Create a COS location

Follow the steps in [“Creating a connection with a Cloud Object Storage provider”](#) on page 261.

**Remember:** Make a note of the **Connection name** and **Location** that you create.

### Step 2: Upload the certificate to the COS location you created

First, ensure that your certificate meets the format criteria.

To upload your certificate, follow the instructions of your Cloud Object Storage provider:

- If you are using IBM Cloud Object Storage, see [Upload data](https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-upload) (https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-upload).
- If you are using Amazon Simple Storage Service (S3), see [Upload an object to your bucket](https://docs.aws.amazon.com/AmazonS3/latest/userguide/uploading-an-object-bucket.html) (https://docs.aws.amazon.com/AmazonS3/latest/userguide/uploading-an-object-bucket.html).
- If you are using Google Cloud Platform (GCP) storage, see [Uploading objects](https://cloud.google.com/storage/docs/uploading-objects) (https://cloud.google.com/storage/docs/uploading-objects).

### Step 3: Connect to the COS location from Cognos Analytics

Follow the steps in [“Creating a storage connection in Cognos Analytics”](#) on page 266.

**Remember:** Make a note of the **Connection name** and **Location** that you created.

### Step 4: Specify S3 header information

You can point your data server connection to a database that is configured for SSL certificates. In your connection, you specify S3 header information that references a certificate stored in a Cloud Object Store location.

#### External certificate retrieval via JDBC:

Connections to a data source via JDBC may be required to use TLS. In turn, Cognos Application tier servers may need to be provisioned with certificates required by TLS. When a data source connection is defined, optionally it may refer to a file which is dynamically retrieved from external storage. The associated JDBC driver must provide a name-value pair via which the location of certificate is provided.

The location of the certificate will be referenced using a session variable called \$certificatePath\$. For example, if a vendor provides the name SSLCert the URL or connection for a data source would include SSLCert=\$certificatePath\$. If a certificate cannot be retrieved from external storage, for example it was deleted or renamed, an error will be displayed. A JDBC driver may reject a certificate if it has expired or cannot be read.

For more information, see the applicable vendor documentation for further details about which name-value pairs a JDBC driver may support for TLS.

1. Ensure that you have [uploaded the certificate to a Cloud object Storage location](#).
2. Follow steps “1” on [page 30](#) - “4” on [page 30](#) of [creating a data server connection](#), ensuring that the data server type supports SSL certificates .
3. Click the chevron icon  to expand the **Cloud certificate details** field.
4. Enter the **Connection name** that you specified when you [created the COS location](#).
5. Select from the list the COS **Location** to which you uploaded the certificate.
6. Select from the list the certificate.

7. In the **Connection properties** field, enter the values that are required for your specific driver.

**Important:** For details, see the vendor documentation for your driver.

For example, for a DB2 connection, enter the following:

```
sslConnection=true;sslCertLocation=$certificatePath$/certFile.arm
```

8. Click **Test** to ensure that the connection works

9. Click **Save**.

## Data server types - connection details

Some data server types require unique parameters when you configure their connections.

This section describes connection details for some of those data server types.

### Connections that support JWT authentication

You can create data server connections using JSON Web Token (JWT) authentication for the following products.

To use this functionality with a data server connection, you must configure Cognos Analytics to use an OpenID Connect authentication provider. To provide the token, the connection settings must specify the OpenID Connect namespace that was configured. The identity provider namespace must be capable of returning claims in the JWT that the vendor requires.

Following is a list of data server types for which Cognos Analytics supports JWT authentication:

- **Amazon Redshift**

Use the Amazon JDBC driver. The URL must include the plugging name-value pair `plugin_name=com.amazon.redshift.plugin.BasicJwtCredentialsProvider`. Amazon Redshift JDBC driver version 2.1.0.4 or higher is required.

**Note:** When you use Azure Active Directory and Amazon Redshift, you must include additional scope details by specifying the following name-value pair: `ibmcognos.oidc.scope=https://database.windows.net/.default`. For more information, see "ibmcognos.oidc.scope" in the *Cognos Analytics Managing Guide*.

- **Azure SQL and Synapse**

Use the Microsoft SQL Server JDBC driver. The connection automatically passes the token via the SQL Server driver `accessToken` property.

**Note:** When you use Azure Active Directory and Azure SQL or Azure Synapse, you must include additional scope details by specifying the following name-value pair: `ibmcognos.oidc.scope=https://database.windows.net/.default`. For more information, see "ibmcognos.oidc.scope" in the *Cognos Analytics Managing Guide*.

- **Db2 and BigSQL**

For more information, see "Support for JWT authentication with Db2 and BigSQL data server connections" in the *Cognos Analytics What's New Guide*.

- **Denodo**

Use the Denodo JDBC driver. A connection must include the Denodo name-value pair `useOAuth2=true`.

- **Exasol**

Use the Exasol JDBC driver. A connection must include the Exasol name-value pair `authmethod=accessToken`. Exasol JDBC driver version 7.1.2 or higher is required.

- **Google Bigquery**

Use the Bigquery JDBC driver. A connection must include the Bigquery name value pair `OAuthType=2`.

- **Progress DataDirect Autonomous REST**

Use the Autonomous REST JDBC driver. A connection must include the Autonomous REST name-value pair `AuthenticationMethod=OAuth2`.

- **SAP Hana**

Use the SAP Hana JDBC driver.

- **Snowflake**

For more information, see [Snowflake connections](#).

- **Teradata**

Use the Teradata JDBC driver. The URL must include the Teradata `LOGMECH=JWT` name-value pair. Teradata JDBC driver version 17.10.00.14 or higher is required.

- **Trino**

Use the Trino JDBC driver. A connection must include the Trino name-value pair `SSL=true`.

- **Dremio**

Use the Dremio JDBC driver. A connection must include the Dremio name-value pair `SSL=true;token_typ=jwt;`.

## IBM Planning Analytics data server connections

If you plan to connect to an IBM Planning Analytics data server, you can optimize how Cognos Analytics manages the data by performing the tasks in this section.

### ***Connecting to Planning Analytics data servers from CA on Demand***

From an IBM Cognos Analytics on Demand environment, you can connect to a TM1 data server that is in a Planning Analytics on Cloud environment.

**Note:** There are two types of Planning Analytics on Cloud: Hosted and On Demand. Only the Hosted Planning Analytics on Cloud environment is supported if you are connecting from Cognos Analytics on Demand.

To do so, [create a data server connection](#), selecting **IBM Planning Analytics** as the data server type.

**Important:** This topic describes how to set the authentication method in Cognos Analytics to match the authentication method used in the TM1 data server. However, the TM1 database administrator must also secure the TM1 server using the dedicated Cognos Analytics instance that is associated with the users' Planning Analytics tenant. Contact the TM1 database administrator to determine the URL of the TM1 database server.

Users and groups are separately managed and configured in Cognos Analytics on Demand and Planning Analytics on Cloud. Therefore, security groups in Cognos Analytics on Demand cannot be used in Planning Analytics on Cloud.

The Cognos Analytics on Demand user ID must be included in the Planning Analytics on Cloud subscription.

For more information, see "Planning Analytics security overview" in the *IBM Planning Analytics TM1 Operations Guide*.

## Procedure

1. Click **Manage > Data server connections**.
2. In the **Data server connections** pane, click the **Add data server** icon .
3. Select **IBM Planning Analytics** from the list of supported types.
4. In the field **New data server connection**, type a unique name for the connection.

5. Under **Authentication method**, select **Integrated security**, where the TM1 database is configured for Integrated Security mode 4 or 5.
6. Beside **Connections details**, click **Edit** and enter the connection details:
  - a. In the **TM1 database host** field, enter the URL of the TM1 database server, for example:
 

```
https://prodsupport.planning-analytics.ibmcloud.com/api/v0/tm1/G0_New_Stores
```
  - b. In the **HTTP port number** field, enter -2
  - c. Leave the **Use SSL** check box unchecked.
7. Click **Test**  to ensure the connection is valid.
8. Click **Save**.

### ***Ensuring that root members in a Planning Analytics data source match those in the TM1 client***

If you import a TM1 data source into Cognos Analytics and select the data source type as **IBM Planning Analytics**, the list of root members in the metadata tree may look different than the list that appears in TM1 client.

### **Solution**

You can enable the REST API `tm1.RootMembers()`. This REST API returns root members from the Planning Analytics data source that match the root members returned from the TM1 Client.

**Important:** You must be using a Planning Analytics server version of 2.0.6 or later.

Follow these steps:

1. Stop the IBM Cognos Analytics service.
2. Go to `installation_location\configuration`
3. If the file `xqe.config.custom.xml` does not yet exist, copy the file `xqe.config.xml` and rename it `xqe.config.custom.xml`
4. Edit `xqe.config.custom.xml`:
  - a. Immediately after the `<queryExecution>` line, add the following line:

```
<paUseRootMembers enabled="true"/>
```

- b. Save `xqe.config.custom.xml`.
5. Start the IBM Cognos Analytics service.

### ***Disabling filler members in a Planning Analytics package***

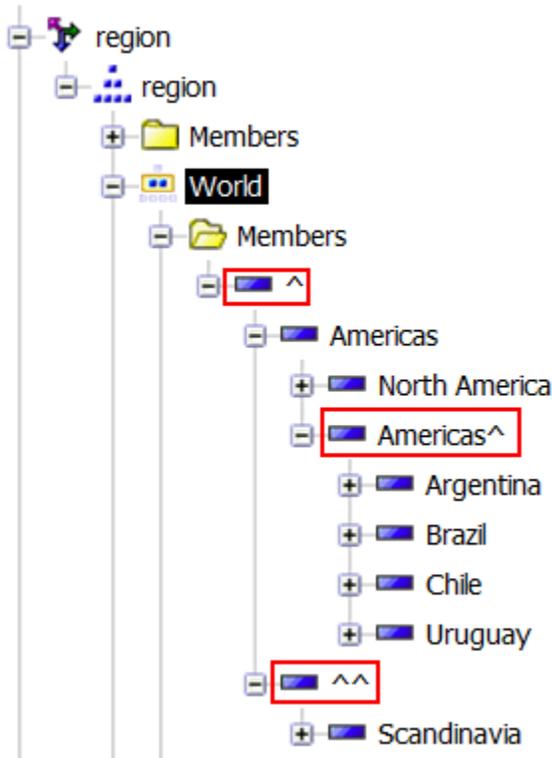
You can disable automatic generation of filler members so that a Planning Analytics package imported to Cognos Analytics shows the same characteristics as it does in the TM1 client.

In Cognos Analytics, by default, filler members are generated to fill gaps due to restricted access from the root of the hierarchy down to members whose data are visible to the user. In IBM Cognos TM1 however, the default behavior is that filler members are not generated.

### **Example 1: Filler members enabled**

When filler members are enabled, the caption of a filler member in the data tree is the caption of the parent member with a caret character (^) appended. If access to a root member is not granted to the user, the root member's caption is a caret character (^) only.

A metadata tree with filler members enabled is shown in the following image:



A chart for the same cube appears as follows:

Budget	1 Quarter	2 Quarter	3 Quarter	4 Quarter
Americas^				
North America	825517.05	846801.29	830379.17	868830.05
Total(children(Am))	825517.05	846801.29	830379.17	868830.05

## Example 2: Filler members disabled

**Note:** Since access to the root member is restricted for the cube in example 1, if filler members are disabled, the user cannot see any members at all in the data tree.

A chart from the same cube appears as follows:

Budget	1 Quarter	2 Quarter	3 Quarter	4 Quarter
North America	825517.05	846801.29	830379.17	868830.05
Total(children(Am))	825517.05	846801.29	830379.17	868830.05

## Procedure

To ensure that a data source displays the same characteristics in both TM1 client and Planning Analytics, follow these steps:

1. Stop the IBM Cognos Analytics service.
2. Go to *installation\_location*\configuration

3. If the file `xqe.config.custom.xml` does not yet exist, copy the file `xqe.config.xml` and rename it `xqe.config.custom.xml`
4. Edit `xqe.config.custom.xml`:
  - a. Immediately after the `<queryExecution>` line, add the following line:

```
<!-- Set the paUseFillerMember enabled attribute value to false to turn the Filler Member OFF -->
<paUseFillerMember enabled="false"/>
```

- b. Save `xqe.config.custom.xml`.
5. Start the IBM Cognos Analytics service.

### Localizing hierarchies in Planning Analytics data sources

You can see localized hierarchy captions from a Planning Analytics data source in your reports and dashboards in the language that you want.

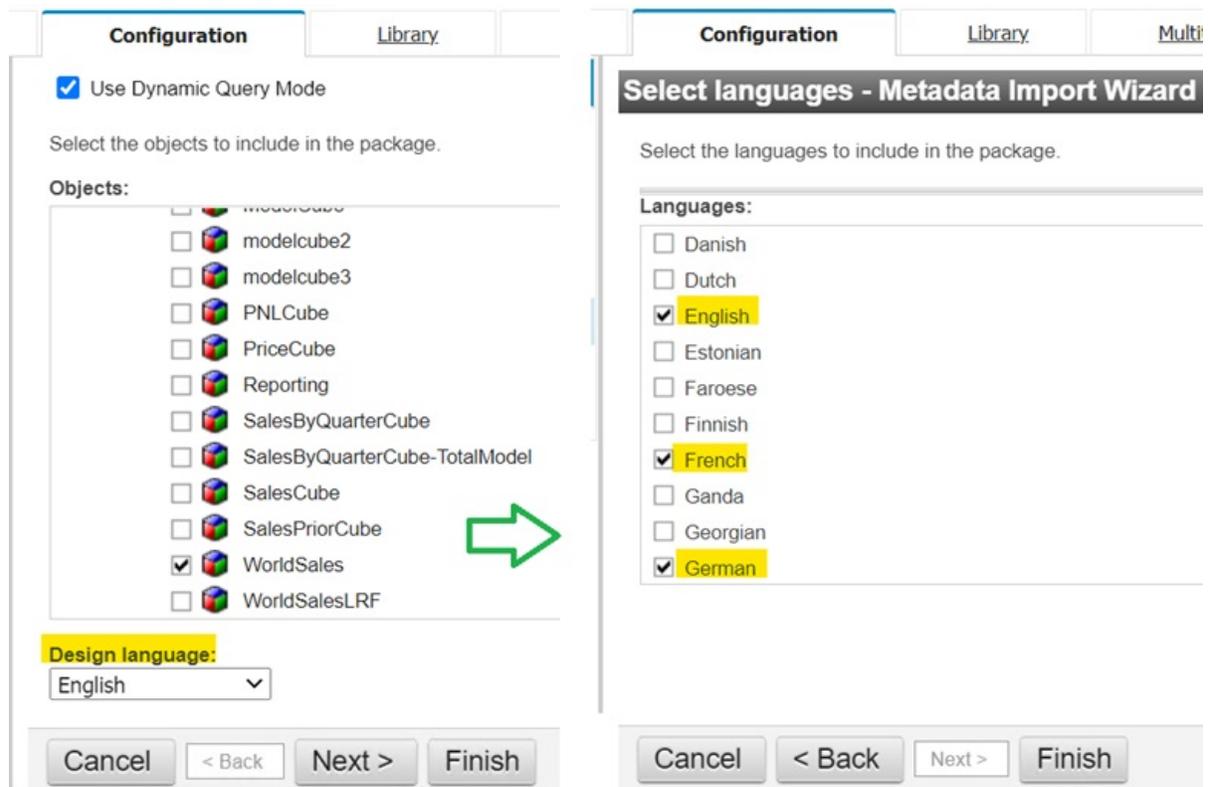
To proceed, do the following:

1. Create the a Planning Analytics package, while ensuring that you define the languages to be localized.
2. Set your [Cognos Analytics content language](#).

### Creating the Planning Analytics package

Create a Planning Analytics package from a Planning Analytics data source as follows:

1. Select the **Use Dynamic Query Mode** check box.
2. Select the objects to include in the package.
3. Select the languages that you want defined in the package.



### Setting your Cognos Analytics content language

Follow these steps:

1. Click the **Personal menu** icon  in the application bar, and then click the **Profile and settings** link below your user name.
2. Click the **Settings** tab.
3. In the **Content language** field, select the language you want displayed with your Cognos Analytics content.

## Result 1: Localized hierarchy names in the metadata tree

Select the Planning Analytics package that you created and view the metadata tree. The hierarchy names appear in the language that you chose:



## Result 2: Localized hierarchy names in a dashboard visualization

Create a dashboard visualization from the metadata tree. The hierarchy names appear in the language that you chose:



For more information, see "Creating multilingual dashboards" in the *IBM Cognos Analytics with Watson Dashboards and Stories Guide*.

## Disabling hierarchy localization

You may decide that you only want to enable hierarchy localization when you are creating Planning Analytics packages.

Planning Analytics hierarchy localization is enabled by default. Follow these steps to disable it:

1. Stop the IBM Cognos Analytics service.
2. Go to `installation_location\configuration`
3. If the file `xqe.config.custom.xml` does not yet exist, copy the file `xqe.config.xml` and rename it `xqe.config.custom.xml`
4. Edit `xqe.config.custom.xml`:
  - a. In the `<queryExecution>` section, set the `paEnableHierarchyLocalization` parameter to `false` as follows:

```
<!--Disable the PA Hierarchy Localization (enabled by default). -->  
<paEnableHierarchyLocalization enabled="false"/>
```

- b. Save `xqe.config.custom.xml`.
5. Start the IBM Cognos Analytics service.

### ***Problems derived from duplicate (ambiguous) names in Planning Analytics cubes***

When a Planning Analytics server has elements of a different type, such as a member, level, or subset, that share a name, the Cognos Analytics query service is not able to handle these elements properly. The queries become ambiguous.

The following queries can become ambiguous.

- The query includes a name that is shared by a subset, a member, or a level.

Most likely, the response to this query doesn't contain the requested object. If the query response is not what is expected, the query service detects the problem, and produces an internal error that starts with the following message: XQE-GEN-0010 Found an internal error: '!mapSuccess - reportName=

- The query references a name that is shared by a member and a level in a cube.

The query response corresponds to the member, not the level. However, a report or dashboard author querying for the ambiguously named level sees instead a single member that has the same name as the requested level.

The solution to this type of problems is to give unique names to all members, levels, and subsets within the cube dimension.

## Salesforce connection editor

The Salesforce connection editor is available from both **Manage > Data server connections** and from the Administration console.

The following diagram shows the Edit Salesforce connection pane:

## Edit Salesforce connection

JDBC URL:

```
jdbc:sfdc://https://login.salesforce.com/services/Soap/u/49.0;  
[property=value[;...]];
```

Driver class name:

```
com.ibm.cognos.jdbc.sfdc.SFDCDriver
```

Restore

✓ Example URL

Connection properties: ?

Close

When you create a new connection, the default URL includes the default instance name `login.salesforce.com` and the API Version `49.0`.

For example:

```
jdbc:sfdc://https://login.salesforce.com/services/Soap/u/49.0;
```

Optional name and value pairs can be specified in the URL or as part of the Connection properties.

For example:

```
jdbc:sfdc://https://login.salesforce.com/services/Soap/u/49.0;QUERYBATCHSIZE=1000;
```

Names are case insensitive. If a duplicate name occurs, the last once parsed from the URL or Connection properties is used. Unrecognized names or invalid values result in an error message.

### Salesforce connection properties

The following table describes the properties that you can append to the connection string.

Connection property	Description
CONNECTION_TIMEOUT	<p>If a connection has not completed in the specified amount of time, it will automatically time out.</p> <p>The default value is 60 seconds.</p> <p>A value must be an integer value in the range of 0 (zero) to 2147483647.</p> <p>Incorrect values will result in an error.</p>
MAX_RETRIES	<p>If a network error is returned when a connection is attempted, it will be retried up to the maximum value specified.</p> <p>The default value is 1 (one).</p> <p>A value must be an integer value in the range of 0 (zero) to 2147483647.</p> <p>Incorrect values will result in an error.</p>
WAIT_BETWEEN_RETRIES	<p>If a connection is retried, the system will pause for the specified number of seconds between each retry.</p> <p>The default value is 0 (zero).</p> <p>A value must be an integer value in the range of 0 (zero) to 2147483647.</p> <p>Incorrect values will result in an error.</p>
PROXY_ENABLED	<p>If a proxy server will be used between Cognos Analytics and Salesforce</p> <p>The default value is false</p> <p>A value must be either false or true.</p> <p>Incorrect values will result in an error.</p>
PROXY_HOST	<p>The hostname of the proxy server that will be used when PROXYENABLED is true.</p> <p>A valid hostname which can be accessed that hosts the proxy server.</p> <p>Incorrect values will result in an error.</p>
PROXY_PORT	<p>The port number the proxy server that will be used when PROXYENABLED is true.</p> <p>The default value is 80.</p> <p>A valid port number.</p> <p>Incorrect values will result in an error.</p>
PROXY_USERNAME	<p>Specifies a username used with the proxy server that will be used when PROXYENABLED is true.</p> <p>Incorrect values will result in an error.</p>
PROXY_PASSWORD	<p>Specifies a password used with the proxy server that will be used when PROXYENABLED is true.</p>

Connection property	Description
	Incorrect values will result in an error.
QUERY_BATCH_SIZE	Specifies the batch size used by the Salesforce query API. The default value is 500. A value must be an integer value in the range 200 to 2000.
CONCURRENT_CALLS_LIMIT	Specifies the maximum number of concurrent requests. The default value is 25. A value must be an integer value in the range 1 (one) to 2147483647.
USER_CONCURRENT_CALLS_LIMIT	Specifies the maximum number of concurrent requests for a user. The default value is 10. A value must be an integer value in the range 200 to 2000.

**Note:** Previous versions of Cognos Analytics provided a connection editor that is only available from the Administration console. These connections can only be used Framework Manager packages. While connections using this editor will continue to work, this connection editor will be deprecated in a future release of Cognos Analytics. Applications should migrate to using the new connection editor.

Metadata described by these connections would include non-groupable columns, while the new editor will exclude them by default.

## Progress DataDirect Autonomous REST connections

The Progress DataDirect Autonomous REST connection queries JSON responses from API endpoints that are accessed via the HTTP protocol. The connection generates a configuration file that translates the endpoint's JSON content into database tables (schemas) in Cognos Analytics. You can create dashboards and reports that use this REST API endpoint data as their data source.

To create or edit a connection to a Progress DataDirect data server, go to **Manage > Data server connections**. Your connection can access either a single URL or multiple endpoint URLs.

**For details about how to configure a connection and the supported options:** See the *Progress® DataDirect® Autonomous REST Connector for JDBC™ User's Guide for Partners*.

The connection string that you enter must include either a 'Sample=REST\_API\_endpoint' or 'Config=configuration\_file' name-value pair that specifies the endpoints to be queried. You may also need to specify an API key in your connection. If you do, ensure that the permissions to the data server connection apply only to the people who require access using this API key.

- The Sample method allows you to easily obtain data from a single endpoint URL. However, if you are working with large amounts of data in a complex schema, this method can slow performance. The reason for this is that the driver must build the endpoint-to-schema mapping on its own.

For more information, see "Sample" on page 99 of the *Progress® DataDirect® Autonomous REST Connector for JDBC™ User's Guide for Partners*.

- The Config method allows you to define the endpoint to schema mapping at configuration time and provides these advantages:
  - It greatly reduces the work performed by the driver at runtime, returning results more quickly.
  - It can issue multiple REST API endpoint requests in a single connection.
  - It tailors the REST API results for schema mapping. This allows for customized table names, column names, and data type mapping.

For more information, see "Config" on page 73 of the *Progress® DataDirect® Autonomous REST Connector for JDBC™ User's Guide for Partners*.

**Before you begin:** Read the topic "Setting up the driver" on page 10 of the *Progress® DataDirect® Autonomous REST Connector for JDBC™ User's Guide for Partners*.

### Sample parameter

Specify the `Sample` parameter in the JDBC URL of a REST API connection. The REST response is a tabular schema that you can import to Cognos Analytics as a data module.

The **JDBC URL** field appears when you [create a data server connection](#) and select **Progress Data Direct Autonomous REST connection** as the connection type.

**For more details:** Read the topic "Using the Sample property method" on page 19 of the *Progress® DataDirect® Autonomous REST Connector for JDBC™ User's Guide for Partners*

### Syntax

```
jdbc:ibmcognos:autorest:Sample='endpoint_URL'
```

### The endpoint URL

The endpoint URL is a REST API location that returns data that you can use in Cognos Analytics. It can contain many optional connection properties to accommodate various types of API responses and authentication. For example, its properties support many OAuth 2.0 authentication flows which vary based on the security needs of each web service.

### Example URLs

The following connection performs an HTTP GET on the URL `http://worldtimeapi.org/api/timezone/America/Toronto`. The JSON response returned from the endpoint is represented as a table with columns that correspond to the fields in the response.

```
jdbc:ibmcognos:autorest:Sample=http://worldtimeapi.org/api/timezone/America/Toronto
```

When a URL includes characters that are used by the driver, you must enclose it in single quotes. The following URL includes a query string in which the name-value pair includes an equal sign (=).

```
jdbc:ibmcognos:autorest:Sample='http://myWebSite/resources?type=dog'
```

**Note:** For additional examples, see [“Examples using the Sample parameter method”](#) on page 46.

### Config parameter

Specify the `Config` parameter in the JDBC URL of a REST API connection. Unlike the `Sample` method, the `Config` method creates a connection that references a local configuration file. You can customize this `.json` configuration file so that the schema translation is preconfigured. This allows you to achieve high performance when you retrieve large amounts of data.

The **JDBC URL** field appears when you [create a data server connection](#) and select **Progress Data Direct Autonomous REST connection** as the connection type.

**For more details:** Read the topic "Using the input REST file method" on page 20 of the *Progress® DataDirect® Autonomous REST Connector for JDBC™ User's Guide for Partners*

### Syntax

```
jdbc:ibmcognos:autorest:Config="path_to_local_configuration_file";ServerName=Endpoint_URL
```

where:

- *path\_to\_local\_configuration\_file* is the path, enclosed in double quotes, to a central location to which you uploaded the configuration file.

For more information, see “Store .json files in a central location” on page 46.

- *Endpoint\_URL* is a REST API location that returns data that you can use in Cognos Analytics. It can contain many optional connection properties to accommodate various types of API responses and authentication. For example, its properties support many OAuth 2.0 authentication flows which vary based on the security needs of each web service.

**For more details:** See the topic "Input REST file syntax" on page 117 of the *Progress® DataDirect® Autonomous REST Connector for JDBC™ User's Guide for Partners*.

### **API key**

If the Data Direct data server you are connecting to uses OAuth 2.0 authentication, you must specify values for the key and secret key in the connection string.

An endpoint may require an API key before it can accept requests. A site may use a process to generate a token that must be part of the HTTP request header. The driver provides name-value pairs that can be used to set header variables. The key can be specified several ways:

- in the URL or connection properties
- in the optional Key field
- via a Cognos Analytics session variable

For example, if a site generates an API key that is to be passed as a bearer token and you prefer to keep the key hidden, use the optional Key field. If the key is a bearer token, enter the value `Bearer`, followed by a space, followed by the API key from the site.

**For more details:** See the topics "ClientId" and "ClientSecret" on pages 71 and 72 respectively of the *Progress® DataDirect® Autonomous REST Connector for JDBC™ User's Guide for Partners*.

### **Tips for creating REST API connections**

This section provides tips to help you save time when you create a DataDirect Autonomous REST connection.

### **Research the API that you want to connect to**

Before you define a connection to a particular API endpoint, review the documentation of the API to find answers to these questions:

- What is the format of the URL and query string?
- What is the format of the JSON responses returned?
- What limits may an endpoint impose in terms of requests in a period?
- What methods are used to authenticate requests, such as via an API key?
- Does the connection provide endpoints that are designed for analytical applications?
- What is the endpoint response time?
- How are the responses mapped by the driver?

### **Try these tools**

You can research the endpoints' behavior using the following tools:

- Curl
- Postman
- a web browser

## Is the endpoint appropriate?

A candidate endpoint may *not* be appropriate for a connection from Cognos Analytics if the connection exhibits any of these behaviors:

- It does not use HTTP for the protocol.
- It does not return JSON responses.
- It uses a proprietary query specification language expressed in the body/query string.
- Its JSON representation cannot be transposed into a schema used by the driver.
- Its endpoints may not have been designed with analytical applications in mind.

For example, a business user may intend to build a dashboard which summarizes information about multiple locations over several business days. If the URL was designed to return information for a single location and day, it may need to be enhanced.

## Map Boolean values to type VarChar or Integer

Cognos Analytics does not support returned Boolean values, for example, true or false values. As a result, if your JSON output contains Boolean values, you cannot use the `Sample` method. Instead, use the `Config` method to map Boolean values to either text (for example, `VarChar`) or `Integer`.

For information about the data types that are supported by Cognos Analytics, see "Supported SQL data types" in the Cognos Analytics *Data Modeling Guide*.

## Indicate nested data objects in the name of the top-level table

Some API calls return data objects that are nested under a top-level table. You can adopt a naming convention for the top-level table that indicates the following:

- the data is nested
- the name of the nested object whose data you want to use in Cognos Analytics

For example, a top-level table might contain call-level attributes such as `success`, `return code`, `error message`, and also an array (or object) called `data`. In this example, `data` contains the data that you are interested in. You name the top-level table `ObjectResults` and name the nested array `Object`. This way, when you create a data module, you can ignore the `ObjectResults` tables and bring in to your module only the various `Object` tables.

**For more details:** Read the topic "Columns with nested objects" on page 143 of the *Progress® DataDirect® Autonomous REST Connector for JDBC™ User's Guide for Partners*

## Add comments

You can add comments to Progress DataDirect REST API configuration files. To do so, type `//` at the beginning of each comment line. Use comments to document the content of your configuration file as well as any nuances of the APIs that you call.

For example, you want to retrieve two subsets of data from the same API. However, when you try to retrieve all the data in one call, the API times out because there is too much data. To solve this issue, you decide to make two separate calls to the API, each one retrieving a different subset. You add a comment that explains why your schema makes two calls instead of one.

## Use column name overrides

You can change the column names of your JSON output to something that makes more sense to your end users and analysts. To override a column name, edit your configuration file and insert your new name, enclosed in angle brackets. That is, change "`old-column-name`" to "`old-column-name<new-column-name>`".

For example, you typically use underscores in your schemas. However, the API that you call returns concatenated names. You decide to rename them to use underscores. You edit the configuration file and change this text:

```
"fieldNumberOne": "VarChar(64)"
```

to this:

```
"fieldNumberOne<field_number_1>": "VarChar(64)"
```

## Relink associated data modules after any connection update

When you save a new version of your DataDirect Autonomous REST connection, you are updating a schema. As with any schema change, you must relink any data module that uses that data server connection.

For more information, see "Relinking sources" in the Cognos Analytics *Data Modeling Guide*.

## Store .json files in a central location

Ensure that you store your .json files in a central location available to everyone in your Cognos Environment. Following are some examples of storage locations, depending on which [Cognos Analytics offering](#) you are using:

### If you are using Cognos Analytics on Cloud Hosted:

Your administrator can give you access to an SSH File Transfer Protocol (SFTP) dropbox in the root file system.

### If you are using Cognos Analytics for Cloud Pak for Data or Cognos Analytics On Demand:

You can host your configuration file on a public URL or in a Cloud Object Store location. For more information, see [Chapter 10, "Managing cloud storage,"](#) on page 261.

### If you are using Cognos Analytics on Premises or Cognos Analytics on Cloud Hosted:

Your configuration file can be stored

- in a Cloud Object Store (COS) location
- in a file system location on each Cognos Analytics application tier server
- on a network drive location that is accessible to each Cognos Analytics application tier server

## Examples using the Sample parameter method

This topic contains an example of using the Sample parameter to create a REST API connection.

## Example that uses a fictional API provider

In this example, you create a REST API data server connection to an API provider using the Sample parameter. Your connection retrieves a Panel data object. The Panel object contains List tables that contain Card tables. You will use your new connection to create a data module in Cognos Analytics that references the **Panel** schema.

1. You go to the web site of the API provider and research its API requirements. You make a note of the required inputs to the API, including the URL syntax and authentication parameters.

You discover that:

- The API uses OAuth1 authentication.

**For more details:** See the topic "Authentication" on page 42 of the *Progress® DataDirect® Autonomous REST Connector for JDBC™ User's Guide for Partners*.

- You would like to access the Panel API.
- You will use the SAMPLE method to query the API.

2. You register with the company's API service and obtain unique information that you will use in your Panel API call.
  - You obtain a panel id that identifies the schema instance that will be returned to you.
  - You obtain your own security key and security token.
3. In Cognos Analytics, you build a data server connection to the API.
  - a. You follow the steps in [Creating a data server connection](#), specifying values as follows:
    - In the **Select a type** pane, you click **Progress Data Direct Autonomous REST connection**.
    - In the **JDBC URL** field, you type the following:

```
jdbc:ibmcognos:autorest:sample='HTTP://company_api_url/panel_id?fields=all&key=your_security_key&token=your_security_token'
```

**where:**

- The sample method uses single quotes around its entire value.
  - The *panel\_id* is sent to you when you registered with its API service.
  - `fields=all` specifies that all fields in the data are to be returned.
  - `key=` and `token=` are prefixes to the security key and security token values that you were assigned when you registered with the API service
  - The **Driver class name** field is auto-filled with this text:  
`com.ibm.cognos.jdbc.autorest.AutoRESTDrive`
  - Under **Authentication method**, you select **Connect anonymously**.
- b. You save the new connection.
4. You verify that the metadata was loaded.
    - a. Hover over the connection to see the connection context menu , and click **Assets**.  
In the **Assets** page, the **AUTOREST** schema appears in the list, confirming that all of the tables from the API service were loaded into Cognos Analytics.
    - b. You click the context menu  for the **AUTOREST** schema.  
The names of the tables appear. You can use these tables to create a data module.
    - c. If you need to refresh the data, you click **Load metadata**.
  5. You create a data module, based on the connector that you built.
    - a. In the Cognos Analytics Welcome page, you click **New > Data module**.
    - b. In the **Select sources** dialog box, you select the Data servers and schemas icon .
    - c. You select the connector that you just built.  
You are prompted to select a connection.
    - d. You select **Panel Info** and then click **OK**.
    - e. You select the **AutoREST** schema that was returned by your connection.  
Auto-generated table names appear.  
**Tip:** The last table in the list is named **Configuration**. To create a connection that uses the Config parameter, you can copy data from any similar **Configuration** table into a customized configuration file. For more information, see [“Example using the Config parameter method”](#) on page 48.
    - f. You select all the tables in the list, and then click **OK**.  
A **Grid** view appears of the tables that you imported. You notice that one of the tables contains the Panel info. This name was auto-generated from the JDBC URL value that you entered when you created the API connection.
    - g. You examine the data module and modify it, if required.

- h. You click **Save** to save the data module.

The data module  is created in the location that you chose.

### **Example using the Config parameter method**

In this example, you create a REST API connection to a fictional API provider using the `Config` parameter. This connection method references a configuration file that calls several endpoints and maps the results into a custom database schema. You then edit the configuration file to optimize future data retrieval via the connection.

**Tip:** Step “4” on page 48 of this example describes modifying the configuration file used in the connection. You can also use the Cognos Analytics modeling tool to make changes to objects, for example, to modify label names.

### **Procedure**

1. You use a configuration file, for example, `my_config.json`, to specify the data you want returned by the REST API service.
2. You store the file `my_config.json` in a central location available to everyone in your Cognos Analytics environment.

For more information, see “Store .json files in a central location” on page 46.

3. You create a connection using the `Config` parameter:

- a) You follow the steps in “Creating a data server connection” on page 29, specifying these values:

- In the **Select a type** pane, you click **Progress Data Direct Autonomous REST connection**.
- In the **JDBC URL** field, type the following:

```
jdbc:ibmcognos:autoREST:config="path_to_my_config.json";ServerName=url_endpoint
```

**where:**

- `path_to_my_config.json` is the path to your configuration file, which is stored in a central location.
  - The path to your configuration file is enclosed in double quotes.
  - You determine the `url_endpoint` by visiting the web site of the API provider.
  - The `panel_id`, security key, and security token are not explicitly included in the API call. Instead, they are defined in the configuration file, which is encrypted.
  - The **Driver class name** field is auto-filled with this text:  
`com.ibm.cognos.jdbc.autoREST.AutoRESTDriver`
- Under **Authentication method**, you select **Connect anonymously**.
- b) You save the new connection.
4. You examine `my_config.json` in a text editor and modify the file, if required:
    - You can rename the schema name and panel name to be more intuitive.
    - You may notice that multiple API calls are made when using this configuration file.
    - If you want to ignore some members or rows in a table, you can comment them out using double slashes (`//`).
    - For each main table object, you replace *actual* values with a corresponding *data type*.
    - You may notice nested tables within the configuration file. For example, each nested table may appear as an array, denoted by a pair of square brackets (`[]`), under its parent table.
    - You might want to rename an original table name. For example, you want to rename `labels` to `cardLabels`. Using the configuration file syntax, you replace the code `labels` with `labels<cardLabels>`.

**For details about how to modify a configuration file:** Read the topic "Modifying the relational view" on page 21 of the *Progress® DataDirect® Autonomous REST Connector for JDBC™ User's Guide for Partners*.

5. You create a data module based on the connection.

**Tip:** See step "5" on page 47 in "Example that uses a fictional API provider".

6. In the data module, you select the **Relationships** view.

The table relationships are shown graphically. These relationships were generated in Cognos Analytics from the corresponding information in the configuration file.

## What to do next

You can use this data module as the data source when you create, for example, a or .

## Microsoft Azure Analysis Services

The Microsoft Azure Analysis Services data server connection is supported on IBM Cognos Analytics with Watson on premises on Microsoft Windows only. Follow these guidelines when you create the data server connection.

- Specify **Prompt for the user ID and password** or **Use the following signon** for the authentication method.
- Specify the server name shown in the Microsoft Azure portal for the **Server name**. Do not use the management server name.
- Specify the **Language** field in the following format: ll or ll-cc, where ll is the ISO language code and cc is the ISO region or country code.

For more information about Microsoft requirements, see [Client libraries for connecting to Azure Analysis Services](https://docs.microsoft.com/en-us/azure/analysis-services/analysis-services-data-providers) (<https://docs.microsoft.com/en-us/azure/analysis-services/analysis-services-data-providers>).

### Notes:

- Driver version must be Microsoft Analysis Services OLE DB Provider (MSOLAP) 15.1 or higher
- Compatibility level must be 1400 or higher
- Framework Manager does not support Microsoft Azure Analysis Services data server connections

## Microsoft Analysis Services and Microsoft Azure Analysis Services - Language code

Use the following format in the **Language** field for the Microsoft Analysis Services or Microsoft Azure Analysis Services data server connection:

ll or ll-cc, where ll is the ISO language code and cc is the ISO region or country code. The region or country code is optional.

## Snowflake connections

You can configure a connection to Snowflake using the Snowflake JDBC driver so that it passes a JSON Web Token (JWT) when authenticating to the database.

To enable a Snowflake connection, complete these tasks:

1. Choose an identity provider namespace that can return claims in the JWT that Snowflake requires.
2. Configure Cognos Analytics to use the OpenID Connect authentication provider.

For more information, see "OpenID Connect authentication provider" in the *IBM Cognos Analytics with Watson Installation and Configuration Guide*.

3. Specify the connection settings:

- a. Select the OpenID Connect namespace that you configured as an identity provider.

**Tip:** This allows the JWT token to be passed.

- b. Select **Use an external namespace** as the authentication method.
- c. Include the Snowflake name-value pair `authenticator=oauth` in the connection URL.

For more information, see [“Creating a data server connection” on page 29](#).

For information about Snowflake JWT authentication, see the Snowflake documentation.

## SingleStoreDB

A connection to SingleStoreDB supports using the SingleStoreDB driver. In previous Cognos Analytic releases, connections required the MariaDB Connector/J JDBC driver or the MySQL Connector/J JDBC driver.

**Note:** "SingleStore" is the rebranded name of the company formerly known as "memSQL".

To change existing connections that use the MariaDB Connector/J or MySQL Connector/J JDBC driver, update the URL to the format supported by SingleStore and alter the driver class name to refer to the SingleStoreDB driver class name.

SingleStore recommends that their customers use their SingleStoreDB JDBC driver instead of MySQL or MariaDB drivers.

## Data catalogs

IBM Cognos Analytics can be connected to a catalog such as Watson Knowledge Catalog (WKC).

Watson Knowledge Catalog is an extension to IBM Cloud Pak for Data that provides self-service access to data assets for knowledge workers who need to use those data assets to gain insights.

For more information, see these topics:

- [What is IBM Watson Knowledge Catalog?](https://www.ibm.com/cloud/Watson-knowledge-catalog) (<https://www.ibm.com/cloud/Watson-knowledge-catalog>)
- [Watson Knowledge Catalog overview](https://www.ibm.com/support/knowledgecenter/SSBRA9_addon/wsj/catalog/overview-wkc.HTML) ([https://www.ibm.com/support/knowledgecenter/SSBRA9\\_addon/wsj/catalog/overview-wkc.HTML](https://www.ibm.com/support/knowledgecenter/SSBRA9_addon/wsj/catalog/overview-wkc.HTML))

A Catalog in WKC can reference one or more connected assets that refer to data sources. Cognos Analytics can import and re-use the connection details. Currently, only details for connected assets that correspond to databases supported by Cognos Analytics are imported.

## Notes about WKC connections in Cognos Analytics

- Cognos Analytics displays WKC schemas and tables the same way that it displays data for other types of data server connections. After you [load metadata](#) and view the **Assets** page, a concatenation of *catalog name/connection name/schema name* appears.

Here are some examples:

**Default Catalog/GSDB/gosalesdw**

**My WKC Catalog/Foodmart/FOODMART**

**Platform assets catalog/Great Outdoors Warehouse/gosales**

- Cognos Analytics administrators do not manage the connection details of a connected WKC asset. Connection details are managed by the database administrator in WKC.
- You can create Cognos Analytics connections to multiple catalogs.
- Cognos Analytics also displays schemas and tables from the Platform assets catalog (Platform Connections). For more information, see [Connecting to data sources at the platform level](https://www.ibm.com/support/producthub/icpdata/docs/content/SSQNUZ_latest/cpd/access/connect-data-sources.html#connect-data-sources__platform) ([https://www.ibm.com/support/producthub/icpdata/docs/content/SSQNUZ\\_latest/cpd/access/connect-data-sources.html#connect-data-sources\\_\\_platform](https://www.ibm.com/support/producthub/icpdata/docs/content/SSQNUZ_latest/cpd/access/connect-data-sources.html#connect-data-sources__platform)).

## Before you begin

To connect to a Watson Knowledge Catalog, you must first add the WKC certificate to your Cognos server. To do so:

- Follow the steps in "Import the CA certificates into IBM Cognos components" in the *IBM Cognos Analytics with Watson Installation and Configuration Guide*.

**Important:** Self-signed certificates are not supported for CA/WKC integration in 11.1.7 and later. The CPD/WKC certificate that is imported into Cognos Analytics must be signed by a trusted root authority. To confirm that your certificate is signed by a trusted root authority, enter the WKC URL into a browser and verify that there is a padlock to the left of the URL.



If you import a self-signed certificate and try to create an External Catalog connection to WKC, the following message may appear:

MSR-WKC-2404 Invalid connection string, user name or password

If your certificate is self-signed, replace it with a trusted TLS certificate by following the steps in [Using a custom TLS certificate for HTTPS connections](https://www.ibm.com/support/producthub/icpdata/docs/content/SSQNUZ_latest/cpd/install/https-config-openshift.html) ([https://www.ibm.com/support/producthub/icpdata/docs/content/SSQNUZ\\_latest/cpd/install/https-config-openshift.html](https://www.ibm.com/support/producthub/icpdata/docs/content/SSQNUZ_latest/cpd/install/https-config-openshift.html)).

- Restart your IBM Cognos services.

## Connecting to a Watson Knowledge Catalog

1. Click **Manage** > **Data server connections**.

2. In the **Data server connections** pane, click the **Add data server** icon .

3. Select **External Catalog** as the type.

4. In the **Edit External Catalog connection** panel, enter the following text in the **Server URL** field:

```
jdbc:wkc:url_for_wkc_server
```

where *url\_for\_wkc\_server* is the URL to the IBM Cloud Pak for Data main landing page for the CPD instance with WKC installed.

For example, if your CPD URL is `https://wkc-cpd.test.cloud.ibm.com`, then the **Server URL** value would be:

```
jdbc:wkc:https://wkc-cpd.test.cloud.ibm.com
```

**Tip:** Leave the **Connection properties** field blank.

5. In the **Authentication method** section, select **Use the following signon**.

**Tip:** This is the only valid authentication method for an External Catalog connection type.

6. Click the plus sign icon .

7. On the **Credentials** tab, enter a valid Watson Knowledge Catalog user ID and password.

**Tip:** Specify a username and password that you want to connect to WKC with. The user credentials are the credentials that are defined in the CPD instance. You can choose to use the CPD admin userid or another CPD userid with access to WKC.

8. Click **Test** to ensure that the connection works.

9. Click **Save** to save the connection in Cognos Analytics.

## 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 sections list the isolation levels in increasing order of isolation. Each section contains a description of the isolation level and information about equivalent isolation levels in different databases.

## Read Uncommitted

### Description

Changes made by other transactions are immediately available to a transaction.

### Equivalent isolation level for different databases

The following table lists, for example databases, isolation levels that are equivalent to **Read Uncommitted**.

**Tip:** To find out isolation levels equivalent to **Read Uncommitted** for databases not listed in the table, see the database vendor's JDBC driver and server documentation.

<i>Table 2. Read Uncommitted databases and equivalent isolation levels</i>	
<b>Database</b>	<b>Equivalent isolation level</b>
Oracle	Not applicable
Db2	Uncommitted read
Microsoft SQL Server	Read uncommitted
Sybase Adaptive Server Enterprise	Read uncommitted
Informix®	Dirty read

## Read Committed

### Description

A transaction can access only rows committed by other transactions.

### Equivalent isolation level for different databases

The following table lists, for example databases, isolation levels that are equivalent to **Read Committed**.

**Tip:** To find out isolation levels equivalent to **Read Committed** for databases not listed in the table, see the database vendor's JDBC driver and server documentation.

<i>Table 3. Read committed databases and equivalent isolation levels</i>	
<b>Database</b>	<b>Equivalent isolation level</b>
Oracle	Read committed
Db2	Cursor stability
Microsoft SQL Server	Read committed
Sybase Adaptive Server Enterprise	Read committed
Informix	Committed read

## Cursor Stability

### Description

Other transactions cannot update the row in which a transaction is positioned.

### Equivalent isolation level for different databases

The following table lists, for example databases, isolation levels that are equivalent to **Cursor Stability**.

**Tip:** To find out isolation levels equivalent to **Cursor Stability** for databases not listed in the table, see the database vendor's JDBC driver and server documentation.

<i>Table 4. Cursor stability databases and equivalent isolation levels</i>	
<b>Database</b>	<b>Equivalent isolation level</b>
Oracle	Not applicable
Db2	Not applicable
Microsoft SQL Server	Not applicable
Sybase Adaptive Server Enterprise	Not applicable
Informix	Cursor stability

## Reproducible Read

### Description

Rows selected or updated by a transaction cannot be changed by another transaction until the transaction is complete.

### Equivalent isolation level for different databases

The following table lists, for example databases, isolation levels that are equivalent to **Reproducible Read**.

**Tip:** To find out isolation levels equivalent to **Reproducible Read** for databases not listed in the table, see the database vendor's JDBC driver and server documentation.

<i>Table 5. Reproducible read databases and equivalent isolation levels</i>	
<b>Database</b>	<b>Equivalent isolation level</b>
Oracle	Not applicable
Db2	Read stability
Microsoft SQL Server	Repeatable read
Sybase Adaptive Server Enterprise	Repeatable read
Informix	Repeatable read

## Phantom Protection

### Description

A transaction cannot access rows inserted or deleted since the start of the transaction.

### Equivalent isolation level for different databases

The following table lists, for example databases, isolation levels that are equivalent to **Phantom Protection**.

**Tip:** To find out isolation levels equivalent to **Phantom Protection** for databases not listed in the table, see the database vendor's JDBC driver and server documentation.

<i>Table 6. Phantom protection databases and equivalent isolation levels</i>	
<b>Database</b>	<b>Equivalent isolation level</b>
Oracle	Not applicable
Db2	Not applicable
Microsoft SQL Server	Not applicable
Sybase Adaptive Server Enterprise	Not applicable
Informix	Not applicable

## Serializable

### Description

A set of transactions executed concurrently produces the same result as if they were performed sequentially.

### Equivalent isolation level for different databases

The following table lists, for example databases, isolation levels that are equivalent to **Serializable**.

**Tip:** To find out isolation levels equivalent to **Serializable** for databases not listed in the table, see the database vendor's JDBC driver and server documentation.

<i>Table 7. Serializable databases and equivalent isolation levels</i>	
<b>Database</b>	<b>Equivalent isolation level</b>
Oracle	Serializable

<i>Table 7. Serializable databases and equivalent isolation levels (continued)</i>	
<b>Database</b>	<b>Equivalent isolation level</b>
Db2	Repeated read
Microsoft SQL Server	Serializable
Sybase Adaptive Server Enterprise	Serializable
Informix	Not applicable

## 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

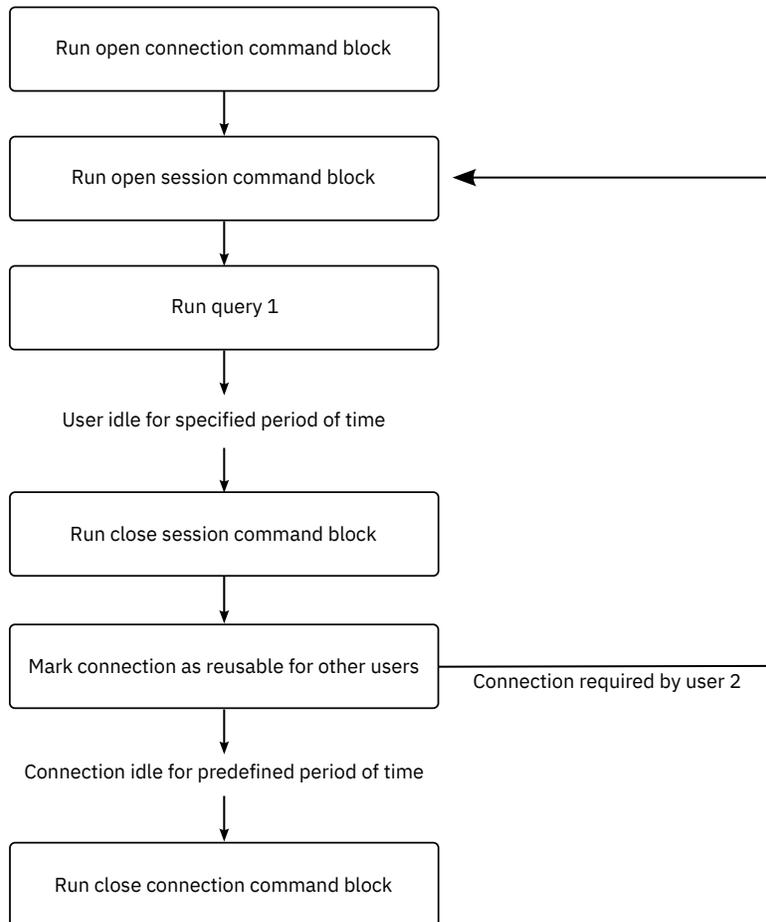


Figure 2. Example of interaction between command blocks

## 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>
```

```
</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>
    </sessionStartCommand>
  </commands>
</commandBlock>
```

```

    </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 "Schema for Data Source Commands" in the *IBM Cognos Analytics Administration and Security Guide*.

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**.

## 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>
```

```
</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 59.

## 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.

## 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.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.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.fetchBufferSize**

This parameter is used to set the JDBC driver fetch size for data source connections in IBM Cognos Analytics with Watson.

When the query service in IBM Cognos Analytics with Watson 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.import**

The `ibmcognos.import` property allows you to configure a data server connection that imports metadata. For example, you can integrate Cognos Analytics with Egeria by importing Egeria metadata.

## **Requirements**

To integrate Cognos Analytics with Egeria, you must have the following:

- a Cognos Analytics 11.2.0 environment or later installed, configured, and running
- an Egeria environment with the analytics-modeling OMAS running Version: 2.5 or later.

For more information, see [Analytics Modeling Open Metadata Access Service \(OMAS\) \(https://egeria.odpi.org/open-metadata-implementation/access-services/analytics-modeling/\)](https://egeria.odpi.org/open-metadata-implementation/access-services/analytics-modeling/)

- an Egeria catalog populated with at least one `DeployedDatabaseSchema`

### **Note:**

If connecting via `https`, you must import the SSL certificates to the Cognos Analytics keystore. For instructions see: [Importing certificate from an SSL enabled website to Cognos Analytics \(https://www.ibm.com/support/pages/importing-certificate-ssl-enabled-website-cognos-analytics\)](https://www.ibm.com/support/pages/importing-certificate-ssl-enabled-website-cognos-analytics)

## **JSON Configuration**

Integration of Cognos Analytics with Egeria is configured via a JSON document. This document describes the REST calls to make to the `analytics-modeling OMAS`.

**To view the example egeria.json document:** Download and extract the egeria.zip file.

The egeria.json document is divided into three sections, each section describing a REST call Cognos Analytics will make to Egeria's analytics-modeling OMAS:

1. schemas

- Called when listing available schemas for a Data Source Connection

2. tables

- Called when listing available tables for a Data Source Connection schema

3. modules

- Called when loading metadata for a Data Source Connection schema

**Note:** You must review each section and ensure that they match the Egeria environment being called.

**Updating attributes**

In the egeria.json file, update the attributes shown in the following table:

Attribute	Value
<code>(schemas tables modules).[0].url.scheme</code>	Optional, adjust to http if not using https
Lines: 6, 38, 70	
<code>(schemas tables modules).[0].url.host</code>	Adjust to match the hostname of ING's Egeria server
Lines: 7, 39, 71	
<code>(schemas tables modules).[0].url.port</code>	Adjust to match the port number of ING's Egeria server
Lines: 8, 40 72	
<code>(schemas tables modules).[0].url.path</code>	Adjust relative URL path to match ING's Egeria server and username. These are represented as CST and system in the template relative URL path
Lines: 9, 41, 73	
<code>(schemas tables modules).[0].url.params.[0].value</code>	Adjust with a DeployedDatabaseSchema GUID from ING's Egeria server. For more information, see <a href="#">Finding a DeployedDatabaseSchema GUID</a>
Lines: 13, 45, 77	

For example, here are the highlighted fields to change in the schemas section. Other sections follow the same pattern:

```

"schemas": [
  {
    "url": {
      "scheme": "https",
      "host": "vott-egeriaubuntu1.fyre.ibm.com",
      "port": 8080,
      "path": "/servers/CST/open-metadata/access-services/analytics-modeling/users/system/$1/schemas",
      "params": [
        {
          "pattern": "$1",
          "value": "database@149975b8-c073-4673-bc37-bda0691c7146:b1c497ce.6e83759b.2r5n1ifi1.b61hs80.8j60ak.ku3oo19c4k8862o3nns8b"
        },
        {
          "key": "startFrom",
          "value": "0"
        },
        {
          "key": "pageSize",
          "value": "0"
        }
      ]
    },
    "sslVerificationOff": true,
    "method": "GET",
    "onSuccess": [
      200
    ],
    "onError": [
      "FAIL"
    ]
  }
]

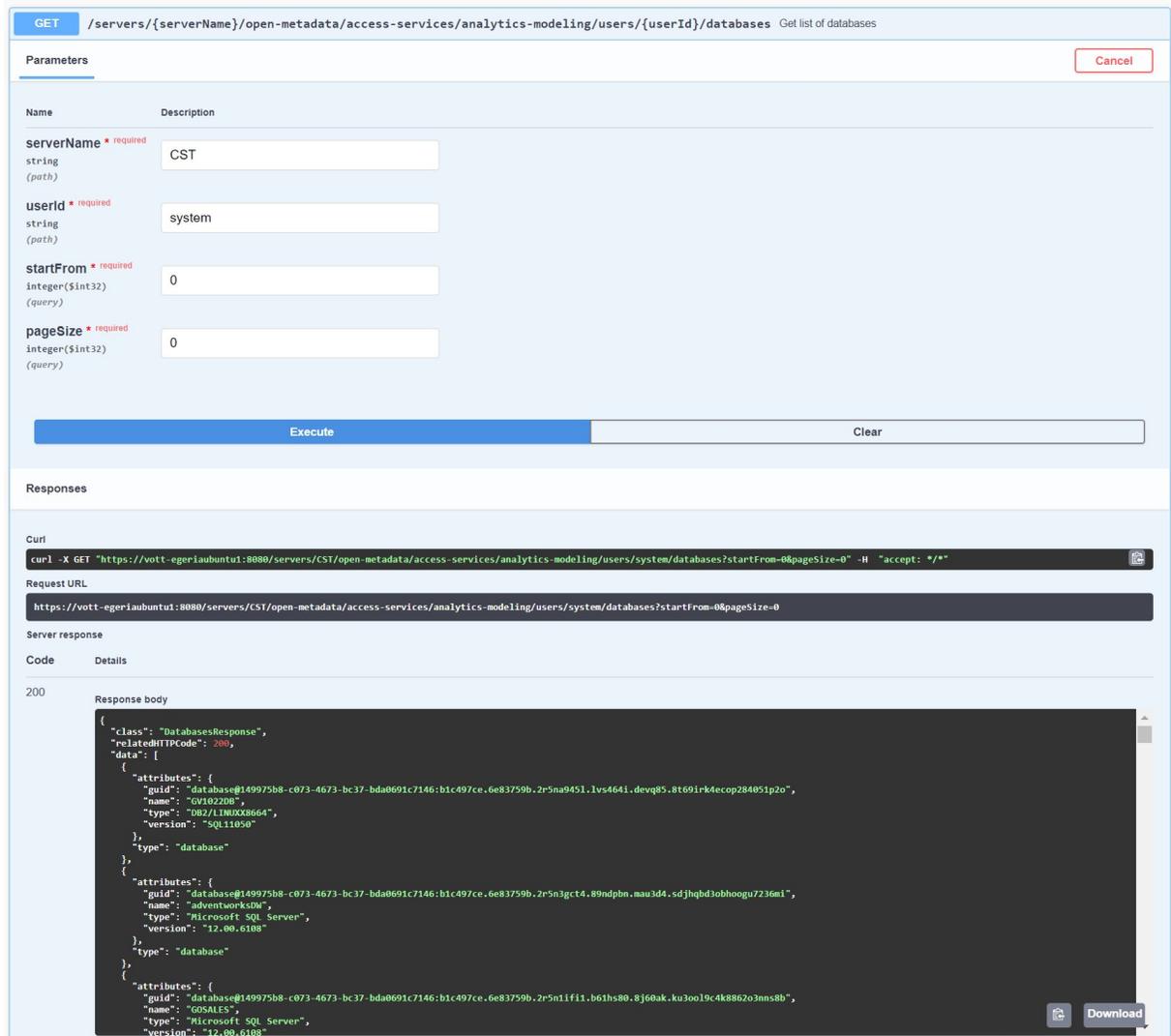
```

**Note:** The attribute name `sslVerificationOff` forcefully disables SSL certificate verification.

### Finding a DeployedDatabaseSchema GUID

The analytics-modeling OMAS provides an endpoint to quickly find all available `DeployedDatabaseSchema` instances and their GUIDs. This endpoint can be executed from the swagger-ui or via a REST call to the OMAS.

Here is an example:



## Hosting the configuration file

For Cognos Analytics to use a JSON configuration file successfully, the file must either be:

- hosted on an http server  
For example, with the URL `http://hostname:3000/egeria.json`  
OR
- copied to a location that is common to all Cognos Analytics reporting nodes  
For example, with the URL `file:///D:/config/egeria.json`

## Creating a data server connection that imports metadata from Egeria

Follow these steps:

1. Click **Manage > Data server connections**.
2. In the **Data server connections** pane, click the **Add data server** icon **+**.
3. Select the data server type from the list of supported types.  
For example, select **Microsoft SQL Server**.
4. In the field **New data server connection**, type a unique name for the connection.  
For example, type `MSSQL_GOSALES1`

5. Beside **Connections details**, click **Edit** and enter the connection details for the type of connection that you are creating.
  - a. Fill in the **JDBC URL** field.  
 For example, type `jdbc:sqlserver://server:12345;databaseName=GOSALES`
  - b. In the **Connection Properties** field, enter the following:  
`ibmcognos.import=URL_of_JSON_file`  
 Here are two example URLs:
    - `ibmcognos.import=file:///D:/egeria/config.json`
    - `ibmcognos.import=http://myserver:3000/config.json`
6. Under **Authentication method** > **Use the following signon**, select the signon from the drop-down list, or create a new signon by clicking the add icon **+**. In the **New data server connection** window on the **Credentials** tab, type a user ID and password.
7. Click **Test** to verify that the connection works.
8. Click **Save** to save the new data server connection.

## Modeling with Egeria metadata

You are now ready to navigate to the **Assets** page to preview and load metadata as usual. Metadata is retrieved from Egeria via JDBC calls.

After you load a schema, you can see the results by creating a new data module using the schema as the source.

For more information, see "Creating a data module" in the *IBM Cognos Analytics with Watson Data Modules Guide*.

## 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:

Database	Default VARCHAR precision
Db2 iSeries	32739
Db2 ZSeries	4096
Db2 LUW	8168
Exasol	2000000
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.maxRowsRetrieved

The `ibmcognos.maxRowsRetrieved` property on a data server connection can be used to set the maximum number of rows that are returned in an SQL query.

This property is applicable for the dynamic query mode (DQM) only, and can be used to prevent users from executing queries which retrieve large numbers of rows from the database server.

Use the following syntax to specify this property, where *N* represents the maximum number of rows to return:

```
ibmcognos.maxRowsRetrieved=N
```

The *N* value must be an integer greater than 0 and less or equal to 2147483647.

An exception is thrown if an invalid value is detected. By default, no limit is applied to the number of rows that are returned.

Not setting this property, or setting it to 0, means that there is no limit.

**Note:** If the queried database offers workload management features, use these features instead of this property.

## **ibmcognos.oidc.scope**

When this parameter is specified, the value will be used when a token is obtained from the identity provider.

Cognos Analytics supports passing tokens to several data sources, where a connection is associated to a namespace configured to use OpenID Connect. In many cases, the scope in the namespace specification used with Cognos Analytics is sufficient to obtain a token that is accepted by a data source.

When alternate scope details must be specified to obtain a token, specify **ibmcognos.oidc.scope**. The following example shows when an alternate scope detail must be specified.

When using Azure Active Directory and Azure SQL or Azure Synapse, specify **ibmcognos.oidc.scope=https://database.windows.net/.default**.

## **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 with Watson.

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.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.

## **UDA.CONVERT\_TIMESTAMP\_LITERAL\_TO\_DATE\_LITERAL**

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.

Because the Oracle `DATE` column contains the date and time parts, UDA reports the Oracle `DATE` datatype as `TIMESTAMP`.

Cognos Analytics 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.

#### Syntax

UDA.CONVERT\_TIMESTAMP\_LITERAL\_TO\_DATE\_LITERAL= "*database\_name: boolean\_value*"

#### Data type

Boolean

#### Default

False

## Loading metadata

After a data server connection is created, you need to load the metadata from the database schemas or catalogs. Only schemas where metadata was loaded can be used to create data modules. The loaded metadata is saved to the content store.

When you load metadata, IBM Cognos Analytics with Watson examines the data servers for information, such as primary and foreign keys, approximate number of rows in each table, or distinct values in certain columns. Based on this information, data is prepared for use in data modules. For example, relationships between tables are inferred automatically, and intelligent default settings are assigned for **Aggregation** and **Usage** properties. This process is also referred to as smart data preparation.

### About this task

Loading metadata doesn't take long for some data server schemas, but it can take a while for schemas with thousands of tables. If the schema contains tables that don't have any analytical value, exclude them so that no time is wasted retrieving their metadata.

When specifying the load options, you can include a sample of statistical data that is retrieved from the underlying data server. This data is used by the Cognos Analytics AI to do better automation, and make better visualization suggestions.

**Tip:** The term schema in the Cognos Analytics user interface also represents the term catalog. Both terms denote a logical classification of database objects.

### Procedure

1. Click **Manage > Data server connections**.
2. In the **Data server connections** page, click a data server name.

The data server connections are displayed. A data server can have multiple connections.

**Tip:** Ensure that the connection represents a relational database.

3. Hover over a connection to see the connection context menu , and click **Assets**.

The list of database schemas is displayed. The **Status** column indicates the load status of the schema tables. If no tables are loaded, the **Load** link is available.

The **Tables loaded** column indicates how many tables are loaded. If the schema is not loaded, this information is not available.

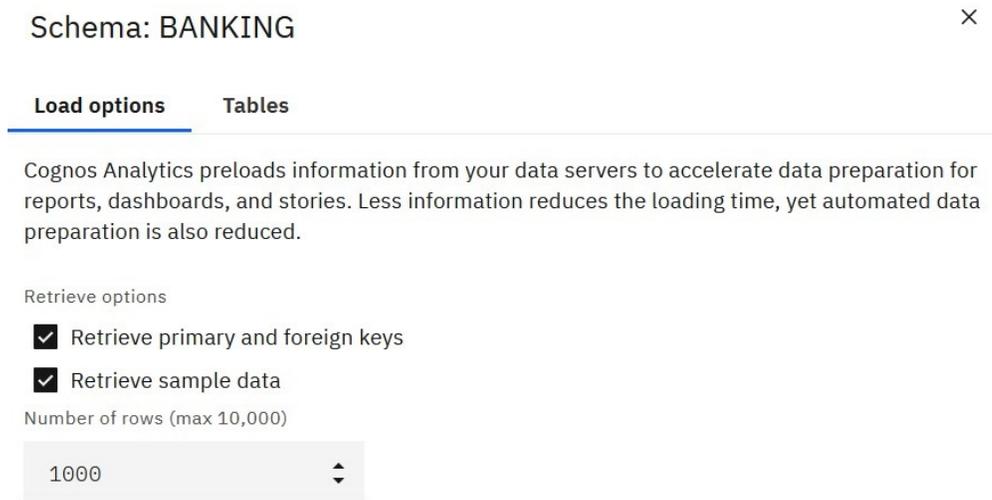
By default, the list doesn't include the system and administration schemas for several types of data servers. These types of schemas are not loaded by default. For example, the PUBLIC schema in ORACLE is not displayed. To view the system and administration schemas for a data server connection, select the **Load system assets** checkbox.

**Tip:** The set of system and administration schemas that are not displayed for specific (not all) vendors is defined in the `install_location\configuration\moser\import.xml` file.

4. Hover over a schema to see the context menu , and click one of the following options:

- **Load options**

Use these options to specify which load options to select, and which schema tables to load.



– On the **Load options** tab, select or clear the following checkboxes (these checkboxes are selected by default):

**Retrieve primary and foreign keys**

Select this checkbox to facilitate automatic detection of relationships between tables.

Clearing this checkbox reduces the time and memory usage by the system when the data is loaded. However, fewer joins might be created.

**Retrieve sample data**

Select this checkbox to retrieve a statistical sample of data from each selected table.

By default, 1000 rows of the data per table is retrieved. You can modify this value, and specify up to 10000 rows. Too many rows might have negative impact on the system performance; too few rows might not gather enough information.

Clearing this checkbox reduces the time and memory usage by the system when the data is loaded, and might be the right choice in some situations.

For more information, see [“Data sampling” on page 71](#).

– On the **Tables** tab, select or deselect the tables to load.

Use the **Exclude tables** option to exclude tables that aren’t used in your dashboards or explorations, which reduces the time and memory usage when queries run. You can also exclude tables that cause errors, or those that you cannot access.

Use the **Include tables** option to select a fixed set of tables for metadata loading. This option is helpful if you want to refresh the loaded metadata, but do not want to automatically include any newly defined tables.

- **Load metadata.**

This option loads all tables in the schema by using the default load options.

- **Delete metadata**

This option is available only if the schema metadata was loaded before. Use this option to remove the previously loaded metadata from the content store. However, this option should be used with caution because it can break reports, dashboards, or explorations that are based on data modules that use the schema, and delete security filters from the data modules.

## Results

When loading is finished, the **Status** column indicates that the schema is loaded. The **Tables loaded** column indicates how many tables are loaded.

## What to do next

If the schema was loaded for the first time, it can now be used to create data modules. If this is a subsequent reload of the schema metadata, the data in the associated data modules is refreshed.

## Data sampling

Data sampling is a way for the IBM Cognos Analytics with Watson artificial intelligence (AI) to learn about the data in the underlying data server. This data is used by the AI to do better automation, and make better visualization suggestions.

Without the sample data, some Cognos Analytics features don't work. For example, the relationships diagram in **Explore** is displayed only if the sample data is available. Otherwise, it's not displayed.

When loading the schema metadata or enriching a package, a sample of statistical data can be retrieved from the underlying data server. To enable this functionality, select the **Retrieve sample data** checkbox in the related dialog box.

By default, 1000 rows of a statistical sample of the data per table (query subject for packages) is retrieved from the underlying data server. This sample data is used by the Cognos Analytics AI to infer characteristics, or "advanced metadata", that help the AI in its automation choices and visualization suggestions.

An example of a characteristic that can be inferred from the sample data is the approximate number of unique values in each field. This information helps the AI make visualization type recommendations. For example, a bar chart is recommended only if there are not too many unique values to display as bars. A bubble chart is more appropriate for data fields that have hundreds of unique values.

The type and amount of data that is retrieved with the data sample is not always the same, and is influenced by the following factors:

- User's permissions to query specific tables or columns in the table.
- Data security that constraints the rows that the user can see.
- Data masking that might change the data that the user can see.
- Expressions might be dynamic because of macros.
- Data server connections might be dynamic because of macros or security on the connections.

## Disabling data sampling

To disable data sampling for all tables in the data server, clear the **Retrieve sample data** checkbox in the metadata loading or package enrichment user interface.

If data sampling is disabled, the Cognos Analytics AI doesn't know as many characteristics about the data. It still knows some characteristics by looking at the data server metadata, but not as many as it would know if it had access to the sample data. Using the example above, without sampling, a bar chart might be recommended even for data fields that have too many unique values to be appropriate for this visualization type. In summary, the visualization recommender works without the characteristics inferred from the sample data, but it doesn't work as well.

Here is a list of features that are negatively affected when data sampling is disabled:

- Forecasting
- Assistant
- Relationship diagram
- Decision tree visualization

- Spiral visualization
- Driver analysis visualization
- Sunburst visualization
- Natural language details
- Insights in visualizations
- Correlated insights
- Recommended visualizations in Explore
- Related visualizations
- Recommended visualizations in dashboards

For more information, see the *IBM Cognos Analytics with Watson Exploration* and *Dashboards and Stories* guides.

Disabling data sampling is justified in the following situations:

- Errors occur when the sample data is retrieved.
- The negative performance impact on the system is too significant.

Instead of disabling data sampling entirely, you can keep the **Retrieve sample data** checkbox selected, but exclude some tables from the process. Both the metadata loading and package enrichment user interfaces include options to deselect tables. For example, you could exclude tables that generate errors. You can also reduce the number of sample rows that are retrieved.

## Reference and troubleshooting

When creating and maintaining data server connections in IBM Cognos Analytics with Watson, you might encounter issues with JDBC drivers, data server version support, authentication, and so on.

The connection information is different for each type of data server. For more information, see the database vendor documentation.

### Managing multiple connections to the same data source

When a data source with multiple connections is queried, an ambiguous connection condition can result. You can ensure that ambiguous connection conditions do not occur.

#### About this task

You can [create](#) more than one connection to the same data source. The data source is then associated with more than one connection definition. When a Cognos Analytics user queries a data source, the query engine must connect to it. The query engine obtains information about the data source from the content service. However, if the response includes information about two or more connections, the result is an ambiguous connection condition.

When an ambiguous connection condition occurs, the user is prompted to select the connection that the query engine will use.

As administrator, you can prevent ambiguous connection conditions from occurring. This ensures that a user won't be prompted during a query operation. You can achieve this in two ways:

- by modifying who can use the data source connection
- by modifying the status of the data source connection

**Note:** After you modify a data source connection using one of these methods, it can take several minutes for the Dynamic Query server to apply your changes. Applications that use the Compatible Query engine apply your changes immediately.

## Example: Modifying user access to a connection

The data source `dsone` includes the connections `connone` and `conntwo`. The user `userone` runs a report on the data source `dsone`. While the report is running, `userone` is prompted to choose which connection they want to use.

To ensure that `userone` does not encounter this ambiguous connection condition again, you edit the `userone`'s access to the `connone` connection:

1. Click **Manage > Data server connections**.
2. In the connection list, click `connone`.
3. Click the **Permissions** tab.
4. Select **Override parent permissions**.
5. Click the add icon , and specify access for a group or role to which `userone` does not belong.
6. Remove access for roles and groups that include `userone` by clicking the Remove selected item icon .
7. Click **Apply**.

The next time `userone` runs the report, the query engine again requests information about the data source `dsone`. However, now the response returns only the connection `conntwo`, as this is the only connection that `userone` can access.

## Example: Modifying a connection's status

The data source `dsone` includes the connections `connone` and `conntwo`. The user `usertwo` runs a report on the data source `dsone`. While the report is running, `usertwo` is prompted to choose which connection they want to use.

To ensure that *any* user, including `usertwo`, does not encounter this ambiguous connection condition again, you decide to disable the `connone` connection:

1. Click **Manage > Data server connections**.
2. In the connection list, click `connone`.
3. Click **Advanced**.
4. Select the **Disable this entry** check box.

The next time any user runs the report, the query engine again requests information about the data source `dsone`. However, now the response returns only the connection `conntwo`, as this is the only connection that any user can access.

## Query service warnings related to unknown data types

When the query service encounters the Unknown data type while processing queries, it might return a warning.

The query service allows expressions to reference in-database functions whose signature (input and output types) is unknown to IBM Cognos Analytics with Watson. As queries are validated and planned, the query service checks the data type information. If the data type is Unknown, a warning might be returned.

A known issue exists with the IBM JCC (JDBC) driver and Db2 where the expected response from JDBC `DatabaseMetadata.getFunctionColumns` method is not returned. Consequentially, the return type of the function is unknown to the query service from the model, which results in a warning.

To work around this issue, you can enclose the in-database function in another function that is known to the query service, such as `CAST`. For example, `CAST( myUDF ( . . . ) , integer )`. Then, the query service uses the data type information that is returned by that function.

**Note:** It's not mandatory to import a function into a Framework Manager model before a function can be referenced in an expression. By importing a function, the metadata, including the data type, about the function is made available to the query service.

## Cloudera Impala JDBC drivers

IBM Cognos Analytics with Watson supports connections to Cloudera Impala data servers that use JDBC drivers version 2.5.34 and later. JDBC drivers earlier than 2.5.34 are not supported.

When attempting to connect to Cloudera Impala, the query engine checks the version of the JDBC driver. If the version is earlier than 2.5.34, an error message is returned.

To avoid potential issues, replace older versions of JDBC drivers for Impala in the Cognos Analytics environment with newer versions. The driver can be downloaded from the [Cloudera website](http://www.cloudera.com/downloads/connectors/impala/jdbc/2-5-34.html) (www.cloudera.com/downloads/connectors/impala/jdbc/2-5-34.html). For more information, see Cloudera documentation.

## Stalled queries in the Pivotal HDB engine

Queries might become stalled in the Pivotal HDB engine because of a defect in the Pivotal optimizer.

To resolve the problem, the Pivotal administrator can change the server defaults, or add the following command block for the connection in IBM Cognos Administration.

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql>select disable_xform('CXformExpandNAryJoinDP')</sql>
    </sqlCommand>
  </commands>
</commandBlock>
```

If a table was created in HDB with partitioning, the Pivotal JDBC driver returns metadata for each partition of the table. Currently, there is no means in the Pivotal software to prevent it from returning the extra metadata. A modeler in IBM Cognos Analytics with Watson does not need to include that additional metadata for queries to work.

## Denodo 5.5 and 6.0 data servers

The Denodo 5.5 and 6.0 data server types are supported through the Denodo JDBC driver.

The minimum supported version of Denodo 5.5 is update 20160322 that must have Denodo hot fix #26682 applied. Previous versions of Denodo 5.5 are not supported.

The initial release of Denodo 6.0 GA requires Denodo hot fix #26681 to be applied.

Denodo requires a 6.0 JDBC driver when accessing a 6.0 server, and a 5.5 JDBC driver when accessing a 5.5 server.

Denodo 5.5 JDBC drivers do not prevent connections against a 6.0 server. If this situation occurs, the 6.0 server might throw exceptions while running queries or attempting to import metadata.

## Data servers no longer supported in Cognos Analytics

The list of supported data servers is continuously evaluated. New data servers are added, and some of the previously supported data servers are removed.

All data server connections that were defined in previous releases of Cognos Analytics remain in the content store until they are manually deleted or changed to a supported type where applicable. These connections are visible in the product administration interfaces. When such connections are opened in IBM Cognos Administration, they appear in the connection editor of type **Other type**. This connection editor provides a limited interface to view or edit the connections, and to access the associated signons.

Each data server connection in the content store is represented by a string with various custom names and values. This string is visible in the connection editors in Cognos Analytics. For example, when testing a connection, a string such as the following one is displayed:

```
^User ID: ^?Password: ; LOCAL ; PG ; DSN=MyDataSourceName ;
UID=%s ; PWD=%s ; MyODBCDSN@ASYNC=0@0/0@COLSEQ=
```

The connection type in the string is shown after the value LOCAL. In the above example, the connection type is PG.

If your current version of Cognos Analytics is using connections to data servers that are no longer supported, in some cases you can change the connections to the supported types.

### **Cognos Analytics 11.1.3**

Pivotal HDB data server is no longer supported in Cognos Analytics.

The associated data server type in the administration interfaces, **Pivotal Greenplum and HDB**, is changed to **Pivotal Greenplum**.

### **Cognos Analytics 11.0.8**

The following data servers are not supported as of the 11.0.8 release:

- Hitachi Advanced Data Binder Platform (JDBC)
- IBM Domino (JDBC)
- MongoDB Connector for BI version 1

Update any version 1 connections to use MongoDB Connector for BI version 2.2.1. Also, update existing Cognos models while connected to version 2.2.1. This will ensure that the model metadata reflects differences in data types and scale that were introduced in MongoDB Connector for BI 2.2.1.

### **Cognos Analytics 11.0.6**

The following data servers are not supported as of the 11.0.6 release:

- Actian Matrix (ODBC and JDBC)

Generic ODBC connection types can be used to refer to an ODBC DSN that uses an ODBC driver on Microsoft Windows operating systems to access an Actian Matrix server. You will not be able to use an existing JDBC connection.

- Actian Vector (ODBC)

Generic ODBC connection types can be used to refer to an ODBC DSN that uses an ODBC driver on Microsoft Windows operating systems to access an Actian Vector server.

- IBM® IMS™ (JDBC)

### **Cognos Analytics 11.0.3**

The following data servers are not supported as of the 11.0.3 release:

- IBM Cognos Finance - connection type CL
- Microsoft SQL Server Analysis Services 2005 and 2008 (ODBO) - connection types YK and M8

Applications on Windows operating systems should use the ODBO client that is released with the supported Microsoft Analysis Services version. Applications on non-Windows platforms can use an XMLA (connection type X8) connection. The ODBO clients releases with SQL Server Analysis Services 2005, 2008 and 2008 R2 are no longer supported. Connections for versions 2012 (connection type M12) and 2014 (connection type M14) are both supported. New connections that reference the 2012 or 2014 clients should only be used for version 2012 and 2014 of the corresponding SQL Server Analysis Services servers.

As of Cognos Analytics 11.0.0, only dynamic query mode servers support SQL Server Analysis Services. The compatible query mode does not support SQL Server Analysis Services.

- Microsoft SQL Server 2005 and 2008 Native Clients, and OLE DB (connection type OL and Provider=SQLNCLI or SQLNCLI10)

Older versions of the Microsoft SQL Server client libraries are no longer supported (<https://msdn.microsoft.com/en-us/library/cc280510.aspx>). For applications that must access SQL Server via OLE DB, you can use Native Client connections that include the `Provider=SQLNCLI11`. These connections are parallel to the current SQL Server Native Client version 11 that is supported with SQL Server 2016, 2014, and 2012. Alternatively, connections that use the Microsoft ODBC driver for SQL Server can be used.

- SAP ECC

## Cognos Analytics 11.0.2

The following data servers are not supported as of the 11.0.2 release:

- Composite (ODBC)

Composite (connection type CS): Generic ODBC (OD) connection types can be used to refer to an ODBC DSN which may be using an ODBC driver on Window operation systems to access Siebel servers. Dynamic query mode supports several technologies, including Cisco Information Server and Denodo via JDBC that could potentially be used to provide federated access to Siebel systems.

- IBM Cognos Now! - Real-time Monitoring Cube (connection type LA)

There is no alternative connection type.

- IBM Cognos Planning - Series 7 (connection type CR)

There is no alternative connection type.

- IBM Cognos Virtual View Manager (ODBC)
- IBM Red Brick® (ODBC)
- Progress OpenEdge (ODBC)
- Siebel
- Sybase Adaptive Server Enterprise (CT-Lib)

## Errors related to mismatched SQL and Java data types

A table column might use a vendor data type which the JDBC driver does not directly support and attempts to return as another data type such as VARCHAR.

For example, a table includes a column of type ARRAY and a column of type STRUCT which the JDBC driver describes as a VARCHAR. Effectively, to IBM Cognos Analytics with Watson, those columns and VARCHAR data types and any operation the vendor supports involving a VARCHAR are supported. Cognos Analytics may generate a SQL statement including operations, such as COUNT, DISTINCT or ORDER BY referencing those columns. The statement may not execute if the vendor does not support those operations on the data type of the column (for example, ARRAY).

These types of errors might occur when both of these conditions are true:

- You import schema metadata from a database, for example, to create data modules,
- The options to retrieve sample data are turned on.

For more information, see [“Loading metadata” on page 69](#). Similar errors might occur when you create and test model query subjects in Framework Manager.

To avoid errors that are related to mismatched data types, try these solutions:

- Read the related database vendor documentation to find out how a JDBC driver defines the SQL data types that are supported by the database.
- Define in-database views or expressions that convert the mismatched data types into types that are recognized by Cognos Analytics.

For more information, see "Unknown types" in the *IBM Cognos Analytics with Watson Data Modeling* guide.

## Updates by release

Cognos Analytics supports many different data servers. In different releases, data servers are added, changed, or removed.

To view an up-to-date list of data servers that are supported for specific versions of Cognos Analytics 11.2, go to the [IBM Cognos Analytics on Premises 11.2.x: Supported Software Environments](https://www.ibm.com/support/pages/node/6440667) website (https://www.ibm.com/support/pages/node/6440667). In the release section, for example 11.2.0, click one of the following links to view a detailed report about supported data sources:

- Under **Requirements by type**, click the **Software** link. On the **Supported Software** tab, go to the **Data Sources** section. All supported data sources are listed in the table.
- Under **Requirements by platform**, click the operating system name, such as **Linux**. On the **Supported Software** tab, go to the **Data Sources** section. All data sources that are supported for the chosen operating system are listed in the table.

**Note:** If you want to view the data server updates by release for Cognos Analytics 11.1 and 11.0, see [Updates by release for 11.1 and 11.0](#).

## Cognos Analytics 11.2.0 - new and changed features

Following are data server-related updates for Cognos Analytics 11.2.0.

### Vendor-supported driver versions tested with 11.2.0

IBM Cognos Analytics with Watson 11.2.0 supports an updated list of client driver versions.

For more information, see *Vendor-supported client driver versions that were tested with Cognos Analytics on Premises 11.2.0* [Relational] [OLAP] (https://www.ibm.com/support/pages/node/1106607#11.2.0r).

### Default driver class name changed for Cloudera Impala

The Cloudera Impala driver 2.6.15.1017 and higher now supports `com.cloudera.impala.jdbc.Driver` as the driver class name. As a result, the default driver class name has changed from `com.cloudera.impala.jdbc4.Driver` to `com.cloudera.impala.jdbc.Driver`.

If you prefer to use the older driver than 2.6.15.1017, you must manually change the driver class name back to `com.cloudera.impala.jdbc4.Driver` or `com.cloudera.impala.jdbc41.Driver` depending on the level of the JDBC driver API.

For more information, see *Vendor-supported client driver versions that were tested with Cognos Analytics on Premises 11.2.0* [Relational] [OLAP] (https://www.ibm.com/support/pages/node/1106607#11.2.0r).

## Data modules

---

Data modules contain data from data servers, uploaded files, data sets, other data modules, and from relational, dynamic query mode packages.

Data modules are created in the web modeling component in IBM Cognos Analytics with Watson, and saved in **Team content** or **My content**. You can use multiple input sources for a single data module.

**Tip:** If you create a data module using data from an uploaded file and you want the data to be available to other users, store both the data module and the file in **Team content**. This ensures that another user can run a report that references the data. This restriction applies to report authors and consumers. Administrators can run reports that use data from any user's **My content** folder.

Data modules can be used as sources for reports, dashboards, stories, explorations, notebooks, data sets, and other data modules.

For more information, see the *IBM Cognos Analytics with Watson Data Modules Guide*.

Data modules that are sourced from IBM Planning Analytics cubes are created in the administration component. For more information, see [“Creating data modules from Planning Analytics cubes”](#) on page 78.

## Creating data modules from Planning Analytics cubes

After successfully establishing a connection to an IBM Planning Analytics TM1 database server, you can browse its cubes and use them to create data modules.

Data modules that contain Planning Analytics cubes can be used to create reports, dashboards, stories, and other Cognos Analytics content in the same way as packages that contain Planning Analytics cubes are used.

**Note:** You cannot create data modules that combine Planning Analytics cubes and other types of data sources.

### Before you begin

A successful connection of type **IBM Planning Analytics** to the TM1 database server must already be created. For more information, see [“Creating a data server connection”](#) on page 29.

### About this task

The following restrictions apply when you create a data module from a Planning Analytics cube:

- Only hierarchy member subsets are supported
- The following Planning Analytics subsets are not supported:

- Multi-hierarchy member sets

**Tip:** You can modify a Planning Analytics data source that has multiple measure hierarchies so that reporting results are valid. See [“Example: Modifying a PA data source to have only one measure hierarchy”](#) on page 79.

- Control subsets with "}" in the first position in the subset name
- Rollup subsets created in Planning Analytics views. These subsets are tuple sets, not member sets.
- Subsets with an invalid MDX expression or an empty member set

### Procedure

1. In **Manage > Data server connections**, locate an existing **IBM Planning Analytics** data server connection.
2. Click the data server to open its properties.
3. On the **Connections** tab, click the connection to access its properties.
4. Click the **Cubes** tab.

The list of cubes that the connection includes is displayed.

5. From a cube context menu , click **Create data module**.
6. Type the module name, and save it to a location in **Team content** or **My content**.

**Tip:** In **Team content**, you must save items inside folders.

A message at the top of the application page confirms that the data module was successfully created.

7. If the database contains more cubes, repeat steps 5 to 6 to create a data module for any of the remaining cubes.

### Results

The data modules are created in the location that you specified.

## What to do next

Use the data modules to create dashboards, explorations, and other Cognos Analytics content against Planning Analytics cubes.

### Example: Modifying a PA data source to have only one measure hierarchy

This example begins with a report on a Planning Analytics data source with multiple measure hierarchies that originally yields invalid results. To resolve the issue, you remove the additional measure hierarchies so that only one hierarchy remains.

#### Problem

In Cognos Analytics, you run a report on a Planning Analytics data source that uses multiple measure hierarchies. However, in the report output, the values in one measure are incorrectly repeated in another measure.

Here is the expected result, as obtained in Planning Analytics:

	Measure	
	Revenue	Quantity
3	99	11
4	99	11
5	99	11
8	99	11

Here is the actual result in Cognos Analytics:

	Revenue	Quantity
3	11.00	11.00
4	11.00	11.00
5	11.00	11.00
2	11.00	11.00

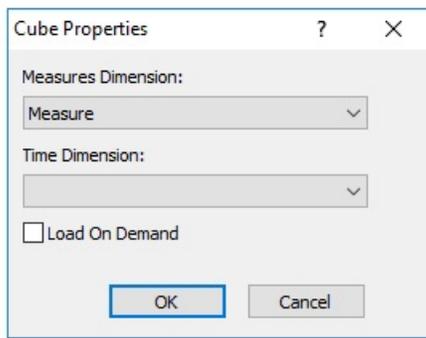
#### Cause

The measure values are repeated because Cognos Analytics does not support PA data sources that use more than one measure hierarchy.

#### Solution

To resolve this issue, remove the additional measure hierarchies so that only one hierarchy remains.

1. In Architect, locate the measure dimension by checking the properties of the cube.



2. Check the existing hierarchies of that dimension by using the `}HierarchiesProperties` Control Cube.
3. Use the `HierarchyDestroy` function in a TI process to remove all the additional hierarchies from the measure dimension.

**Tip:** Ensure that you also remove the Leaves hierarchy.

4. In Cognos Analytics, run the report again on the modified PA data source.

The report output now appears as expected.

## Packages

---

A package is a subset of a model, which can be the whole model, that is made available to the IBM Cognos Analytics with Watson application.

Relational packages are created in IBM Cognos Framework Manager, and OLAP packages in IBM Cognos Cube Designer and in IBM Cognos Administration. For more information, see the chapter on publishing packages in the *IBM Cognos Framework Manager User Guide*.

Not all types of packages can be used in all Cognos Analytics components. Only Reporting can use all types of packages traditionally supported in earlier versions of Cognos Analytics.

For dashboards and stories, the following packages are supported:

- Relational, dynamic query mode packages.
- Relational, compatible query mode packages if there is a JDBC connection defined for each data source in the package.
- Dimensional OLAP packages that are based on PowerCubes, dynamic cubes, Planning Analytics data sources, dimensionally modeled relational (DMR) data sources, and other data sources.

The modeling component supports only relational, dynamic query mode packages as sources for data modules.

For more information, see the *IBM Cognos Analytics with Watson Data Modeling Guide*.

**Note:** Cognos Analytics doesn't support Framework Manager namespaces, which are containers that organize and uniquely qualify content in a model. The namespaces are shown as folders when Framework Manager packages are viewed in data modules, dashboards, and other content.

## Enriching packages

To optimize the user experience in IBM Cognos Analytics with Watson components, such as dashboards and explorations, Framework Manager packages must be enriched.

The enrichment process associates the Cognos Analytics data characteristics, such as **Time** and **Geographic location**, to query items in the packages. The information from the enrichment process complements the information, such as the data type, column name, or **Usage** property value, that is derived from the package metadata.

An enriched package includes the data characteristics that are required for the artificial intelligence (AI) based functionality in the product, such as visualization recommendations or intelligently set default

values on column properties. For example, to display the relationships diagram in **Explore**, an enriched package must be used. Otherwise, the relationships diagram isn't displayed.

The enrichment process can be time and memory-intensive so it should be performed only when the original package has changed. Consider reenriching the package after the following changes to the package:

- Names of query subjects, query items, and namespaces are changed.
- Data types on query items are changed. For example, number changed to string.
- New query items are added.
- Filters or expressions are changed that significantly alter the values that the query subject would return.
- A deployment archive is imported into a new environment that uses different data from the source used for a previous enrichment.

When a package is republished, existing enriched metadata isn't removed or refreshed.

## Before you begin

To minimize the impact of the enrichment process on the system, consider creating smaller packages that include only a subset of purpose-specific query subjects, and enriching only the smaller packages. For example, a package used by advanced report authors might expose many query subjects where many of the query subjects aren't relevant when creating dashboards or explorations. You can create a smaller package off the original package, and include only those query subjects that you need in your dashboards and explorations. Enriching this smaller package requires less time and memory.

## About this task

You can enrich a package metadata by using the automatic or manual process. The automatic process evaluates all query items of all selected query subjects in the package, and automatically applies the data characteristics to them. To minimize the impact on the system, you can deselect namespaces or individual query subjects to exclude them from the enrichment process.

In the manual process, you explicitly apply the data characteristics to individual query items. The manual process is not applicable for dimensional data.

When enriching a package, you typically start with the automatic process. Use the manual process to enrich only a small subset of query items or to override values that were set incorrectly by the automatic option.

The automatic enrichment includes the option to retrieve sample data. When this option is selected, the Cognos Analytics query engine connects to the data source and reads a sample of its data. The enrich dialog box allows the sample size to be changed. Setting the sample size to a low value, or not sampling at all, reduces the amount of information that the enrichment can gather. The amount of sampled data also depends on the signons that are used to access the package underlying data sources. An ideal signon can access the tables, views, and columns that the query subjects are based on, and a representative number of rows and values in the queried tables and views.

To access the **Enrich package** functionality, you need write permissions for the package.

## Procedure

1. Locate the package or its shortcut in **Team content** or **My content**.
2. From the package or shortcut context menu , select **Enrich package**.

**Tip:** If a package was used as a data module source, you can enrich the package in the modeling user interface, from the **Sources** pane.

3. Select one of the following options.
  - **Enrich automatically**

Most of the time, start with this option. The status information shows you the dates when the package was last published and enriched (if it was enriched before).

- In the **Select tables** panel, you can deselect the query subjects that you don't want to be evaluated by the enrichment process. By default, all visible query subjects in the package are evaluated.

This option gives you the opportunity to exclude the query subjects that aren't used in your dashboards or explorations, and therefore reduce the time and memory usage by the system during the enrichment process.

- To enable data sampling, select the **Retrieve sample data** checkbox, and specify the number of rows of data to be retrieved.

The data sample includes some deeper data characteristics that support the product functions that are behind the optimized user experience in dashboards, explorations, and other components. Extracting too many rows might impact the system performance. No data sampling, or too few rows might not provide enough information. Clearing this checkbox reduces the time and memory usage during the enrichment process, but the expected information might not be gathered.

For more information, see [“Data sampling” on page 71](#).

- Click **Run**.

Depending on the number of query subjects involved, the enrichment process can take some time, potentially even hours. After the process is finished, an information message shows you the results of the process. Even if only a certain percentage of the query subjects were enriched, you might have enough data to support the AI-functions in your dashboards and explorations.

- Click **Close**.

- **Enrich manually**

Use this option to enrich individual query items.

- Expand the package.

Then, expand a query subject, and select one or more query items.

- From the **Define data representation** drop-down menu, select the option that you want the data in the query to represent.

Select either **Time** or **Geographic Location**, and their specific values. The **Default** value allows to propagate settings from the source.

- Click **OK**.

## Data sets

---

Data sets are customized collections of data items that you use frequently. As you make updates to the data set, the dashboards, stories, or explorations that use that data set are also updated the next time you run them.

You can create data sets from packages or data modules, and use as sources to create dashboards, stories, explorations, and data modules.

You can't create a report directly from a data set. However, to use the data from the data set in a report, create a data module from the data set, and then use the data module as a source for your report.

The data set mechanism is based on the Cognos Analytics report foundation. You add data to a data set in a similar manner as you add data to a list report. You can switch between **Page design** and **Page preview** modes. The **Query** view provides an alternative way to modify the data sets. In this view, you can copy and paste queries from existing reports, manage advanced filters and prompts, and rename queries.

Here is an example of a data set in the **Page preview** mode.

← → | Data set > Pages > Page1

**Insertable objects**

Find

- Auto group data module
  - Sales
  - Sentiment
  - Recalls
  - Dealers
  - Models

Dealer Name	City	Address	Current Quarter [Quantity Sold]
Weston Auto	Arvada	9825 W 58th Ave	307
Colfax Auto	Denver	1350 W Colfax Ave	267
Northern Auto Sales	Denver	3320 W 38th Ave	338
Suwanda's Auto	Westminster	200 W 136th Ave	213
Great Outdoors Auto	Denver	9190 E 33rd Ave	324
South Parker Auto	Aurora	6462 S Parker Rd	271
Narezney's Auto	Colorado Springs	1905 S Federal Blvd	257
North Parker Auto	Aurora	2651 Parker Rd	277
Club Auto Sales	Federal Heights	9190 N Federal Blvd	291
Broadway Auto	Littleton	6300 S Broadway	219

Summarize detailed values, suppressing duplicates, for relational data sources  
 Row suppression

## Creating data sets

Create data sets to group customized collections of data items that you use frequently.

If a data set is based on a package with multiple data server connections or signons, the connection or signon that you choose is saved with the data set. If the package connection information changes later, users might see the ambiguous connection message. To avoid this message, edit the data set choosing the new connection or signon, and save the data set using the **Save as** option. Select yes when asked whether you want to overwrite the data set. The data set is saved with the new connection or signon and its subsequent refreshes use the new information.

### Before you begin

Review the "Best practices for improving query performance on uploaded files and data sets" in the *IBM Cognos Analytics with Watson Managing Guide*.

The package or data module that you plan to use as a source for your data set must already be saved in **Team content** or **My content**.

### About this task

The list in the data set can be associated with only one query. If you want to add data items from different queries to your data set, you can create a custom query in the **Queries** view that contains data items from different queries.

When creating or editing data sets, you can reuse queries from Cognos Analytics reports. For more information, see ["Reusing report queries in data sets"](#) on page 86.

### Procedure

1. Locate the package or data module in **Team content** or **My content**.
2. From the package or data module context menu, click **Create data set**.

The data set editor is opened in the **Page design** mode.

3. Drag the data items from the **Insertable objects** pane to the work area. The items appear as columnar data in a similar fashion to a list report.

To preview data in the data set, switch from the **Page design** mode to the **Page preview** mode.

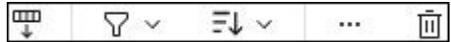
4. For relational data or for data modules, select the **Summarize detailed values, suppressing duplicates, for relational data sources** checkbox.

If you aren't sure if this checkbox must be selected, clear it and then select it again to see how the data is aggregated. Condensed data with fewer rows usually leads to better performing reports and dashboards. A reason for not aggregating the data in your data set is that you lose some details in the process, and the data from one system might not match the data from another system. This is especially true for calculations, such as an average.

5. Select **Row suppression** if you want to hide rows with no data or zeros.

Suppressing rows without data gives you a more concise view of your data set.

6. Refine the data in the data set by using the options in the on-demand toolbar



To view the toolbar, click any column.

To add filters to the columns or individual items of the data set, click the item, and then click the filter icon  in the toolbar. You can add a customized filter or use one of the predefined filters.

To sort the values, click the sort icon , and select from the available sort options.

To view the column expression, click the **More** icon , and select **Edit Query Expression**.

7. Use the **Query** view to access more data set functionality.

From the **Data set** menu, click **Queries** to open the Query Explorer.

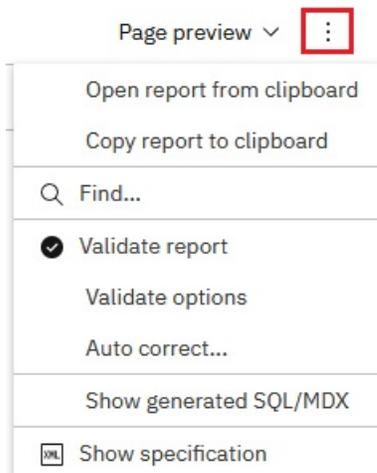
In this view, you can copy and paste queries from existing reports, manage advanced filters and prompts, or rename the queries.

Here is an example of a data set in the **Queries** view:

A screenshot of the Query Explorer interface. The top bar shows 'Data set &gt; Queries' and 'All queries'. The left pane, 'Insertable objects', lists 'Query', 'Join', 'Union', 'Intersect', 'Except', 'SQL', and 'MDX'. The main area shows a query diagram with 'Initial query', 'Report query', and 'Joined query' nodes. The right pane, 'Query', shows settings for 'DATA' (Auto group &amp; summarize: Yes), 'QUERY HINTS' (Auto-sort, Maximum rows retrieved, Use local cache, Refresh on prompt), and 'MISCELLANEOUS' (Name: Joined query).

**Note:** The query names are used as table names when the data set is used to create data modules. Use logical names that clearly describe the data when renaming the queries.

8. Click the **More** icon  to access additional functionality:



Click **Validate report** to validate the data set, or click **Show generated SQL/MDX** to view the data set SQL.

9. Click the save icon , and choose one of the following options to save the data set:
  - To save the data set for the first time or to save changes to the data set, click **Save**. This option saves the metadata, but doesn't load the data. Depending on the data set, loading data might take some time.
  - To save an updated data set as a new data set, click **Save as**. This option saves the metadata, but doesn't load the data. Depending on the data set, loading data might take some time.
  - To save the data set and load the data, click **Save and load data**. In addition to saving the new or changed metadata, this option loads data. The data is immediately available when you create a dashboard or story.

## Results

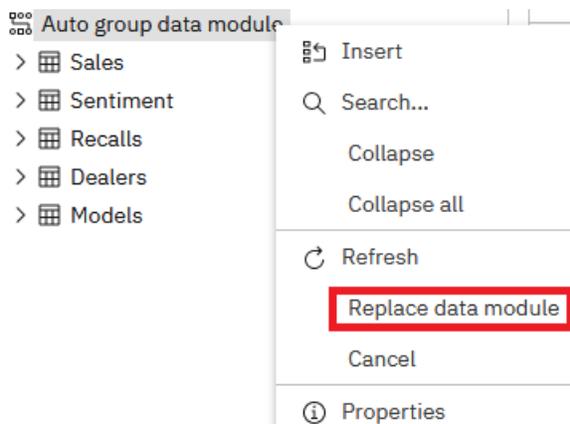
The data set object  is created in a location that you saved it to.

## What to do next

To edit the data set, open it from **Team content** or **My content**.

You can replace data items in the data set with data items from a different query. In the **Page design** or **Page preview** mode, click the **Reset** button. The previously selected data items are removed, and you can start adding new ones to the list.

You can also replace the data module or package that was used as a source for the data set. Right-click the source name in the **Insertable objects** pane, and select the **Replace data module** or **Replace package** option, as shown in the following screen capture:



## Reusing report queries in data sets

You can reuse existing queries from Cognos Analytics reports by copying either individual queries or entire report specifications into data sets.

The data set and the report from which you copy the queries must be based on the same type of data source, either a data module or a package.

When you copy an individual report query, you add the query to the data set, and can continue working with the data set.

When you copy the report specification, the data set is overwritten and you can use the query (or queries) from the report in the data set. The report layout is not copied. The data set is renamed to the default **New data set**. You can then save it as a new data set.

### Procedure

1. Create or open an existing data set.
2. From **Team content** or **My content**, open the Cognos Analytics report in the edit mode.
3. Use the following steps to copy an individual query into your data set:
  - a) In the report, from the **Report** menu, click **Queries** to open the report **Queries** view.
  - b) Right-click the query that you want to copy, and click **Copy**.
  - c) Go back to the data set, and from the **Data set** menu, click **Queries**.
  - d) Right-click anywhere in the empty space in the **Queries** view, and click **Paste**. The new query is added to the view.
  - e) Save the data set.
4. Use the following steps to copy the report specification:
  - a) From any page in the report, click the **More** icon , and select **Copy report to clipboard**.
  - b) Go back to the data set, click the **More** icon , and select **Open report from clipboard**.
  - c) Paste the report specification into the empty box that is displayed, and click **OK**.

You are back in the data set list view. The data source and the query in the data set were replaced. The data set name is shown as **New data set**, even if you started with a data set named differently.
  - d) Open the **Queries** view. All queries from the report are copied into the data set.
  - e) Save the data set using the **Save as** option.
5. From the **Data set** menu, click **Pages** > **Page1**. You are back in the data set list view.
6. Click the **Reset** button to break the list association with the previous query.

The data items are removed from the list. You can now add data items from a different query, including the copied report queries, to the list.
7. In the **Insertable objects** pane, click the **Data items** tab .

The report queries and their data items are shown in the tab.
8. Drag items from one query to the data set list.
9. Save the data set.

### Results

Here is an example of the **Queries** view after a query labeled **Report query** was copied into the data set. The report query was joined with a preexisting query labeled **Initial query**.

The screenshot shows the IBM Cognos Analytics interface. On the left, the 'Insertable objects' pane lists various query types: Query, Join, Union, Intersect, Except, SQL, and MDX. The main workspace displays a query diagram with three nodes: 'Initial query', 'Report query', and 'Joined query'. The 'Joined query' node is highlighted in grey. On the right, the 'Query' properties pane is visible, showing sections for 'DATA' (Auto group & summarize: Yes), 'QUERY HINTS' (Auto-sort, Maximum rows retrieved, Use local cache, Refresh on prompt), and 'MISCELLANEOUS' (Name: Joined query).

Later, the data items from the **Joined query** were used to populate the list in the data set.

The screenshot shows the IBM Cognos Analytics interface displaying a data table. The 'Insertable objects' pane on the left shows a tree view of the query structure: 'Initial query', 'Report query', and 'Joined query'. The 'Joined query' is expanded, showing its fields: 'City', 'Dealer Name', 'Phone number', 'Model', and 'Current Month [Quantity Sold]'. The main workspace displays a table with the following data:

City	Dealer Name	Phone number	Model	Current Month [Quantity Sold]
Arvada	Weston Auto	1 (303) 449-1354	Champlain	30
Aurora	South Parker Auto	1 (303) 449-5441	Champlain	25
Denver	Great Outdoors Auto	1 (303) 808-3333	Labrador	155
Colorado Springs	Narezney's Auto	1 (719) 874-4559	Champlain	25
Denver	Northern Auto Sales	1 (303) 449-6548	Beaufort	100
Littleton	Broadway Auto	1 (303) 326-6889	Beaufort	70
Denver	Colfax Auto	1 (303) 808-9383	Champlain	25
Aurora	North Parker Auto	1 (303) 808-3432	Champlain	25
Arvada	Weston Auto	1 (303) 449-1354	Salish	115
Denver	Colfax Auto	1 (303) 808-9383	Salish	100
Aurora	South Parker Auto	1 (303) 449-5441	Salish	105
Arvada	Weston Auto	1 (303) 449-1354	Hudson	200

Below the table, there are two toggle switches: 'Summarize detailed values, suppressing duplicates, for relational data sources' (checked) and 'Row suppression' (unchecked). A 'Reset' button is also present.

## Uploaded files

If you want to do some quick analysis and visualizations with data files, you can upload the files to IBM Cognos Analytics with Watson by yourself. Your data files must meet size and structure requirements.

The data in the files must be in a simple columnar format. Pivot tables or crosstabs aren't supported.

The size limits for uploaded files are configured by administrators in **Manage > Configuration > System > Data**. The settings that need to be modified are **Size limit per upload of data (MB)** and **Size limit of stored data per user (MB)**.

The following file size limitations apply to individual users:

- Maximum size of each individual file. The default is 100 MB.
- Maximum size of all uploaded files. The default is 500 MB.

The file types that you can upload into Cognos Analytics are specified below.

### Microsoft Excel workbook files

The supported Microsoft Excel file formats include .xls and .xlsx workbook files.

The file formats .xlsb and .xlsm aren't supported.

All worksheets in a multi-tab workbook are uploaded simultaneously. Each worksheet appears as a separate table in Cognos Analytics.

The following conditions apply to uploading Microsoft Excel files:

- .xlsx files that are saved in OpenOffice aren't supported.
- Password-protected Excel files aren't supported.
- Filters in Excel files are ignored. You can use the filtering options in data modules to reapply the filters.
- Comments before the first header row are interpreted as column headers.

Text before the first row that describes the worksheet is incorrectly read as a column header. If you need a description of the worksheet, leave an empty row at the end of your data, and add the description under the empty row.

- Totals and subtotals are treated as part of the data.

Totals can be mistaken as unsummarized data, and give misleading results. Consider removing totals and subtotals from your data before uploading the file.

- The files can contain merged cells.
- Each file can contain a maximum of 2000 columns.

However, for better query performance, avoid uploading files with hundreds of columns. Try to remove redundant columns and rows from the files before uploading the files.

For more information, see [“Best practices for improving query performance on uploaded files and data sets”](#) on page 92.

## Delimiter-separated values files

The supported delimiter symbols include commas, tabs, semi-colons, and pipes (|). The file extension can be .csv, .tsv, .tab, or .txt.

The following conditions apply to uploading delimiter-separated values files:

- Quotation mark characters escape literal values. Single quotation marks (') and double quotation marks (") are supported.
- Record separators separate rows. Newline (\n), carriage return (\r), and carriage return followed by newline (\r\n) are supported.
- If your file is encoded as Unicode, it must contain a byte order mark (BOM) as the first character.
- Each string value in a file can contain a maximum of 5000 characters. Any extra characters are truncated.
- The date and time values in the files must be in a supported format. Otherwise, the data might not be rendered properly in visualizations. Cognos Analytics supports the ISO 8601 standard formats for times.

The following date formats are supported:

- M/d/yy
- MMM d, y
- MMMM d, y
- dd-MM-yy
- dd-MMM-yy
- yyyy-MM-dd

The following time formats are supported:

- h:mm a
- h:mm:ss a
- h:mm:ss a z
- HH:mm

- HH:mm z
- HH:mm:ss
- HH:mm:ss.SS
- HH:mm:ss z
- HH:mm:ss.SS z

## Jupyter Notebook files (.ipynb)

You can upload Jupyter Notebook (.ipynb) files that were created in a Jupyter environment outside of Cognos Analytics.

For more information, see "Uploading external notebooks" in the *IBM Cognos Analytics with Watson Getting Started* guide.

## Compressed files (.zip and .gz)

The compressed file types that you can upload to Cognos Analytics are .zip and .gz files.

The .zip file can contain files with different (supported) extensions, such as .csv, .xls, .xlsx, or .txt. The .gz format can be used only with .csv files, which means that only the .csv.gz extension is supported.

When a .zip file is uploaded, all files inside the ZIP archive are treated as if they were from one Excel workbook, and a table is created for each file. If a file inside the ZIP archive contains multiple worksheets, a table is created for each worksheet. Each of those tables is named using the *FileName - SheetName* naming convention. For example, a .zip file contains the Product.csv and Geography.xlsx files, where Geography.xlsx contains two sheets, Country and Region. After the .zip file is uploaded to Cognos Analytics, the file is shown with the following 3 tables: Product, Geography - Country, and Geography - Region. Cognos Analytics tries to detect joins between all of these tables.

The files inside a ZIP archive are saved together in **Team content** or **My content**. You cannot replace a subset of files that were uploaded as a single .zip file. The whole .zip file must be replaced.

## Uploading files

You can upload supported file types that are stored in any location to which your computer has local or LAN access.

You can upload each data file individually or upload multiple files concurrently. Multiple files can also be compressed for a one-step upload.

### Before you begin

Review the "Best practices for improving query performance on uploaded files and data sets" in the *IBM Cognos Analytics with Watson Managing Guide*.

The package or data module that you plan to use as a source for your data set must already be saved in **Team content** or **My content**.

### Procedure

1. Use the following methods to upload files:

- In the Cognos Analytics welcome page, click the **Open menu** icon  in the application bar, and then click **Upload data**. Browse for the files on your local drive or on the LAN, and select one or multiple files to upload them.
- Drag one or multiple files from your local drive onto the welcome page to activate the **Quick upload** functionality. When **Quick upload** appears, drop the files into the appropriate box to immediately start building a data module, exploration, dashboard, or a notebook.

- From the **Content** view, click **Upload data**. Locate the files on your local drive or on the LAN, and select one or multiple files to upload them. The files are saved to the folder from which you initiated the upload.

**Tip:** At different upload stages, progress and error messages are shown for single-file uploads and consolidated, progress messages for multi-file uploads.

2. Optional: If the **Replace data** message is displayed, it means that a file was uploaded before, and you can either replace or append data to the file. For more information, see [“Updating data in uploaded files”](#) on page 90.

## Results

By default, the uploaded files are saved in **My content**. When the upload was initiated from a specific folder in **Team content** or **My content**, the files are saved to that folder.

If you specified a different default, shared location in **Team content** for uploaded files at the role, tenant, or global level, users can save uploaded files to this location. For more information, see [Edit the default user profile](#).

## What to do next

Use uploaded files to create dashboards, stories, explorations, data modules, or data sets.

To join two uploaded files, create a data module using them as sources.

Reporting can't use uploaded files directly. However, they can be incorporated into a data module, which can then be used as a source in Reporting.

## Updating data in uploaded files

You can replace or append data in an uploaded file with data from an external file.

### About this task

During the **Replace file** operation, you put data from an external file in the place of data in an uploaded.

During the **Append file** operation, you add rows of data from an external file at the end of data in an uploaded file.

To perform both these operations with success, the following conditions must be fulfilled:

- External file contains data, not only column names.
- The names of columns are the same in both files.
- Data types of columns in the external and uploaded files are compatible. For more information, see [Data type compatibility while replacing or appending files](#).

When you replace a file, the order of columns in the external and uploaded files can be different. Also, the external file can contain additional columns with arbitrary names.

### Procedure

1. In **Team content** or **My content**, locate the uploaded file that you want to update.
2. Click the **Action menu** icon , and choose one of the following options from the context menu:
  - **Replace file**
  - **Append file**

**Tip:** While the file is being updated, progress and error messages are displayed.

## Results

You replaced or appended data in the uploaded file with data from an external file. The name of the updated file does not change.

## Data type compatibility while replacing or appending files

Column data types in the original and incoming file must be compatible to replace or append data in uploaded files.

Otherwise, IBM Cognos Analytics with Watson might return the MSR-UPL-2128 error. This error is thrown when the column data type in the original file is incompatible with the detected data type for the same column in the incoming file. The error is returned to prevent data type changes that might cause problems in existing dashboards, reports, or other content.

To avoid this error, ensure that the data types of columns in the original file and in the file that is used to replace or append data are compatible. The following table shows compatible data types for the **Replace file** functionality:

Data type in the original file	Compatible data types in the incoming file
VARCHAR	VARCHAR, BIGINT, DOUBLE, DATE, TIME, TIMESTAMP
BIGINT	BIGINT, DOUBLE
DOUBLE	BIGINT, DOUBLE
DATE	DATE
DATETIME	TIME
TIMESTAMP	TIMESTAMP

**Note:** When replacing a file, the compatible data type replaces the data type in the original file. As a result, you might now see the MSR-UPL-2128 error for the original file. For example, a file containing DOUBLE values was replaced with a file containing BIGINT values. Now, you can no longer append the original file containing the DOUBLE values.

The following table shows compatible data types for the **Append file** functionality:

Data type in the original file	Compatible data types in the incoming file
VARCHAR	VARCHAR, BIGINT, DOUBLE, DATE, TIME, TIMESTAMP
BIGINT	BIGINT
DOUBLE	BIGINT, DOUBLE
DATE	DATE
TIME	TIME
TIMESTAMP	TIMESTAMP

**Note:** When appending a file with a compatible data type, the data type in the original file is preserved. In this case, you can see this type of error message: MSR-UPL-2128 Original column "Price" type "BIGINT" doesn't match column "Price" type "DOUBLE" at the same position.

## Best practices for improving query performance on uploaded files and data sets

IBM Cognos Analytics with Watson can process large uploaded files and data sets. However, to improve query performance and save memory, consider some best practices.

Apply the following best practices before uploading files to and then process data sets in IBM Cognos Analytics with Watson:

- Consider configuring a limit to the size of a request or an attachment. For more information, see [“Limiting the size of a request” on page 92](#).
- 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, 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.

- Summarize data to the highest level that supports the business requirements of dashboards and reports. Reducing the volume (rows and columns) of data that has to be converted to Parquet files managed via the [Content Manager](#) and queried by the Compute engine will improve performance.

For example, if the workload always summarizes to the day, week or month level. Store data summarized to the day level versus transactions at the hour or hour and minute level of detail This will reduce the volume of data which has to be read and summarized (aggregation) by queries.

For example, if the workload presents a set of categorical values (product group, country or business unit) for filters or tables in a dashboard, create a set which includes those values. This will reduce the volume of data which has to be read and summarized (grouped) by queries.

For example, if the workload attempts to compute how many distinct values occurred in a time period (visits per day), create a dataset with those computed values. This will reduce the volume of data that has to be read and summarized (distinct aggregation) by queries.

- Review how dashboard caching can be leveraged to reduce the number of queries that have to be executed by the [dynamic query mode](#) and the Compute service.

### Limiting the size of a request

Configure the CM.MULTIPARTREQUESTMAXLENGTH parameter to limit the overall size of a request or, if data is sent as a request attachment, the maximum size of each attachment.

This setting saves you from running out of disk space and having to troubleshoot this error message: [“CM-REQ-4276 The multipart length exceeds configured limit” on page 93](#).

The value of CM.MULTIPARTREQUESTMAXLENGTH is specified in bytes, with a default value of 2000000000 (release 11.2.4 and later) or 500000000 (prior to release 11.2.4).

### About this task

Data sets are managed by Content Manager, which by default stores report output and data sets in BLOB data types.

**Note:** Do not set the `CM.MULTIPARTREQUESTMAXLENGTH` value higher than 2GB, as most databases limit the size of BLOB columns used for storing large data to 2GB. The maximum size of a BLOB varies by database vendor. Here are some examples:

- Db2: 2GB
- Informix: 2GB+
- ORACLE: (4 gigabytes - 1) \* (database block size)
- SQL Server: 2GB

Content Manager can also be configured to store output into a file system, which would include data sets. The data set sizes are not limited by the database vendor limits used for other Content Manager objects.

For more information, see [“Best practices for improving query performance on uploaded files and data sets” on page 92.](#)

## Procedure

1. Click **Manage > Configuration > System**, and select **Advanced settings**.
2. Type `CM.MULTIPARTREQUESTMAXLENGTH` in the **Key** field.
3. Click in the **Value** field.

The default value, 2000000000 (release 11.2.4 and later), or 500000000 (prior to release 11.2.4) appears.

4. Delete the current value and then enter a new number in the **Value** field.
5. Click **Apply**.
6. Refresh your browser window.

## CM-REQ-4276 The multipart length exceeds configured limit

When you try to upload a large file, the following message appears:

CM-REQ-4276 The multipart length exceeds configured limit.

This message occurs because the large file that you tried to upload exceeds one or both of the size limits enforced by Content Manager and by the database used as the content store.

## Solution

To avoid this issue, first ensure that you have [set the `CM.MULTIPARTREQUESTMAXLENGTH` parameter to its maximum value.](#)

If you still cannot upload the file, consider configuring an [external object store](#).

## Data types used to store data in uploaded files and data sets

IBM Cognos Analytics with Watson applies its own data types to data in uploaded files and data sets.

The data in uploaded files and data sets is stored in the following data types:

- All integer types (smallint, 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, nclob) 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. Report server renders interval values. In previous releases, the value was stored as a string.

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. The scale of a precise value can be reduced by specifying a CAST expression with a scale smaller than 38.

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).

---

## Chapter 5. Configuring system settings

You can configure system settings that affect all users and components in your Cognos Analytics environment.

### Configuring appearance

---

Administrators can enable certain elements to appear in the Cognos Analytics user interface.

#### Procedure

1. Go to **Manage > Configuration > System**, and select **Appearance**.
2. Specify values, as required, for the following settings:

Property	Setting	Result
<b>Load content by pages in Accounts</b>	<b>Enabled</b> (default)	In <b>Manage &gt; People &gt; Accounts</b> , the list of user, group, and role entries is split into separate pages. When you manage accounts, you can navigate more quickly between pages to find entries.
	<b>Disabled</b>	The list of entries appears as one scrollable list.
<b>Items per page in Accounts</b>	<i>number</i> Default=200	If <b>Load content by pages in Accounts</b> is enabled, the number of namespace entries per page.
<b>Launch Cognos legacy UI</b>	<b>1</b>	Legacy BI components are enabled. Users can access Analysis Studio, Drill-through definitions, Event Studio, Query Studio, and Cognos Workspace by clicking <b>New +</b> and then clicking <b>Other</b> .
	<b>0</b>	The <b>Other</b> menu does not appear.

Property	Setting	Result
Enable My portal pages	Enabled	The <b>My portal pages</b> folder  appears under the <b>Team content</b> folder  . Users who had portal pages in their Cognos BI 10.x environment can migrate their content to Cognos Analytics. Their portal pages will look and operate as they did in Cognos BI 10.x.
	Disabled(default)	The <b>My portal pages</b> folder does not appear.

3. Click **OK**.

### Results

The configuration changes are saved and propagated to all dispatchers. You do not need to restart the service for the changes to take effect.

## Configuring security

Administrators can configure security settings in Cognos Analytics.

### Procedure

1. Go to **Manage > Configuration > System**, and select **Security**.
2. Specify values, as required, for the following settings:

Property	Setting	Result
<b>Allowlist for cloud object storage headers</b>	<i>list of S3</i>	Use this parameter to define a set of allowable S3 headers, separated by commas, that can be used when configuring an S3 storage connection.  For more information, see step “6” on page 266 in <a href="#">“Creating a storage connection in Cognos Analytics”</a> on page 266.
<b>HTTP Strict Transport expiration period (days)</b>	<i>number</i>	The HTTP Strict Transport Security Max Age setting in days.
<b>Login redirect URL</b>	<b>URL</b>	The url of a page that the user is redirected to when they sign in to Cognos Analytics.  <b>Tip:</b> You can use this parameter when integrating with your specific SSO environment.

Property	Setting	Result
<b>Logout redirect URL</b>	<i>URL</i>	The url of a page that the user is redirected to when they sign out from Cognos Analytics. <b>Tip:</b> You can use this parameter when integrating with your specific SSO environment.
<b>Login parameters allowed in URL</b>	<i>comma-separated list of parameter names</i>	Use this parameter to enable passing CAM namespace login parameters. <b>Example</b> Your company wants to deploy the following user login syntax: <code>http://server:port/bi/v1/dispatch?CAM_action=logonAs&amp;CAMNamespace=NamespaceName&amp;CAMUsername=UserID&amp;CAMPassword=Password</code> As Administrator, you would enter the following in the <b>Login parameters allowed in URL</b> field: CAMNamespace , CAMUsername , CAMPassword
<b>Allowlist email domains</b>	<i>list of domains</i>	Use this parameter to define a list of allowable email domains. When the parameter is set, emails can be sent only to the specified email domains. The value is a comma-separated list of domains, for example: ibm.com, domain.com, mail.com. If no value is specified, any email domain can be sent a message.
<b>Token Login Signing Secret</b>	<i>alphanumeric string</i>	Specify the signing secret for tokens generated for login.

3. Click **OK**.

## Results

The configuration changes are saved and propagated to all dispatchers. You must restart the service to ensure that all changes take effect.

## Managing data file uploads

You can control how data files are uploaded to IBM Cognos Analytics with Watson. Follow these steps to specify the encryption and size limits of data for uploaded data files.

### Tips:

- These settings apply to uploaded data files only; they do not apply to other types of data, such as data sets.
- To change the location of the directory for uploaded data files, start Cognos Configuration, click **Environment** and then edit the value of the **Data files location** property. The default value is `./data`. For more information, see the *IBM Cognos Analytics with Watson Installation and Configuration Guide*.

### Procedure

1. Go to **Manage > Configuration > System**, and select the **Data** tab.
2. Specify values, as required, for the following settings:

Property	Setting	Result
<b>Encrypt new data files?</b>	<b>Enabled</b> (default)	New uploaded data files are encrypted.
	<b>Disabled</b>	New uploaded data files are not encrypted.
<b>Size limit per upload of data (MB)</b>	<i>number</i> Default=100	The maximum size, in MB, of an uploaded data file.
<b>Size limit of stored data per user (MB)</b>	<i>number</i> Default=500	The maximum size of data storage per user, in MB.
<b>File upload inactivity timeout (ms)</b>	<i>number</i> Default=600000	The period of time before an inactive file upload process is terminated.

**Tip:** Updates to size limits might take a moment to refresh.

3. Click **OK**.

### Results

The configuration changes are saved and propagated to all dispatchers. You do not need to restart the service for the changes to take effect.

## Logging

Log messages provide information about the status of components and important events. Administrators and users can use these messages to troubleshoot problems.

IBM Cognos Analytics with Watson supports different types of logging, including the following main types of logging: audit logging, diagnostic logging, user session logging, and report performance logging.

By default, the IBM Cognos service for each installation sends information to the local `install_location/logs` directory. The audit messages are saved to the `cogaudit.log` file, and the diagnostic messages are saved to the `cognosserver.log` and `dataset-service.log` files. For audit logs, the administrator can specify the location, size and number of log files in IBM Cognos Configuration. For diagnostic logging, the size and number of log files is set in the **Manage** part of Cognos Analytics. Diagnostic logs are always written to the `install_location/logs` directory. Audit logging can be configured to also write to a database, remote log server, or system log. For more information, see [“Diagnostic logging” on page 101](#).

Session logging can be turned on by individual users for a single Cognos Analytics session after administrators enable this type of logging for the system. The messages are logged in the following log files in the *install\_location/logs* directory: *cognosserver-session-session\_id.log* and *dataset-service-session-session\_id.log*. For more information, see [“Setting up logging”](#) on page 99.

## Report performance logging

This type of logging is supported in IBM Cognos Analytics - Reporting for individual reports. A report author enables the option to log performance details by selecting the report run option **Include performance details**. The following details can be viewed in the report output: **Total execution time**, **Query execution time**, and **Rendering time**. Customers can use this information to self-diagnose performance or tuning issues before logging a service request.

For more information, see the sections about running reports and viewing performance details in the *IBM Cognos Analytics - Reporting Guide*.

## Setting up logging

Administrators can configure both session logging and diagnostic logging.

### Session logging

Session logging is used to log detailed user activity in every IBM Cognos Analytics with Watson component and service that is associated with the user's request.

The user does not need to know the components, services, or logging configuration details. There is no performance impact on other users.

Session logging is typically used when a user can reproduce a problem. It can be stopped at any time by the user.

Unique log files are generated for each user who enables session logging. The file names include a unique **Log identifier** that is generated when session logging is turned on by the user.

The administrator must enable session logging for the system, and then individual users can turn it on or off for themselves.

**Note:** Interactive queries in dashboarding do not record the original dashboard name with each interactive change. The reason for this is that there is no guarantee that the saved object will not be saved as another name, thereby attributing the dashboard usage stats to the wrong dashboard.

### Diagnostic logging

Diagnostic logging creates server log files that allow administrators and support personnel to troubleshoot intermittent or service-specific problems. The same diagnostic logging configuration is automatically set on all servers.

For more information, see [“Diagnostic logging”](#) on page 101.

## Procedure

1. Go to **Manage > Configuration > System**, and select **Logging**.
2. Specify values, as required, for the following settings:

Property	Setting	Result
<b>Size limit for server log file (MB)</b>	<i>number</i> Default=200	The maximum size, in MB, of the server log file. After a server log file reaches its size limit, a new "rolling" log file is created.  <b>Tip:</b> Server log files are used for "Diagnostic logging" on page <a href="#">101</a> .
<b>Maximum number of backup server log files</b>	<i>number</i> Default=10	The maximum number of server rolling log files that are stored as backups.  <b>Tip:</b> Server log files are used for "Diagnostic logging" on page <a href="#">101</a> .
<b>Enable user session logging</b>	<b>Enabled</b> (default)	User session logging occurs.  <b>Tip:</b> When this setting is turned on, the option <b>Log my session</b> is available for all users in their personal settings.
	<b>Disabled</b>	User session logging does not occur.
<b>Size limit for user session log file (MB)</b>	<i>number</i> Default=25	The maximum size, in MB, of the user session log file for each user session. After a user session log file reaches its size limit, a new "rolling" log file is created.
<b>Maximum number of backup log files (per user session)</b>	<i>number</i> Default=10	The maximum number of user session rolling log files that are stored as backups.
<b>Delete session log files after 48 hours</b>	<b>Enabled</b> (default)	All user session files log files are deleted after 48 hours.
	<b>Disabled</b>	User session files log files are not deleted.

3. Click **OK** to apply the changes.

You do not need to restart the IBM Cognos Analytics service.

## Results

The configuration changes are saved and propagated to all dispatchers. You do not need to restart the service for the changes to take effect.

## What to do next

Users can now enable session logging in their personal settings, by selecting the **Log my session** option, and turning on the setting **Session logging**. The users should record the **Log identifier** that is generated for the session before they turn off logging or close the browser. The administrator will need this identifier to find the session log files, `cognosserver-session-log_identifier.log` and `dataset-service-session-session_id.log`, in the `install_location/logs` directory.

## Diagnostic logging

Diagnostic logging can be configured by administrators to use for intermittent or service-specific problems. The same logging configuration is automatically set on all servers.

The diagnostic logging messages are logged in the `cognosserver.log` and `dataset-service.log` files in the `install_location/logs` directory. The administrators can specify the maximum size for log files and maximum number of log files to keep to avoid negative impact on performance.

This type of logging is a replacement for JAVA IPF logging (`ipfclientconfig.xml`) from previous versions of Cognos Analytics. Cognos Analytics processes the log messages from the product services using internally defined loggers. These loggers are abstracted into logging topics that can be enabled in the **Manage** user interface.

Diagnostic logging has no impact on session logging or audit logging.

**Tip:** You can still use `ipfclientconfig.xml` for native code components, such as Report Servers, or Framework Manager. `ipfclientconfig.xml` can impact audit logging so use it with caution.

## Configuring diagnostic logging

Administrators can specify restrictions on the size and number of log files that are used for diagnostic logging.

### Procedure

1. Start the procedure in the topic [“Setting up logging”](#) on page 99.
2. Specify the required values for the settings **Size limit for server log file** and **Maximum number of backup server log files**.
3. Click **OK**.

You do not need to restart the IBM Cognos service to change diagnostic logging.

## Enabling diagnostic logging for different topics

You can enable diagnostic logging on a specific product component, service, or function by changing the logging topic.

IBM Cognos Analytics with Watson processes the log messages from the product services using internally defined loggers. These loggers are abstracted into logging topics. The **DEFAULT LOGGING** topic that is set for diagnostic logging uses a set of logger names that are set at specific error levels. This is done so that the default logging is not too verbose and records only the most important messages.

You can enable diagnostic logging on a built-in topic or on a custom topic. To create a custom topic, you can download a JSON spec for a built-in topic and use it as a basis for creating your custom topic. Custom topics can be modified, but built-in topics cannot be modified.

### Procedure

1. Go to **Manage > Configuration**.
2. Select the **Diagnostic logging** tab.
3. Select one of the built-in or custom topics for which you want to enable logging.

By default, the following built-in topics are available:

- **AAA** - Access Manager Authentication logging
- **CM** - Content Manager logging
- **DEFAULT LOGGING** - logging using default settings
- **DISP** - Dispatcher logging
- **MOSER** - Modeling service logging

- **POGO\_MSGS** - Dispatcher SOAP message logging

To see all built-in topics, select the **Show all** checkbox.

For example, to generate logs for Cognos Analytics Mobile Reports, select the **MOB** topic.

4. Click **Apply**.
5. To restore **DEFAULT LOGGING**, click **Reset**.
6. To create a custom topic, do the following:
  - a) Click the **Built-in topics** tab.
  - b) Click the More icon  next to a built-in topic that is similar to the one you want to create and then select **Download topic**.
  - c) Edit the file and save it on your computer as *filename.json*.
  - d) Click the **Custom topic** tab.
  - e) Click the **Upload topic** icon .

Your new topic appears as an entry on the **Custom topics** tab.

## Results

The logs are now written to the `cognosserver.log` and `dataset-service.log` files in the `install_location/logs` directory.

## Enabling diagnostic logging for Java dumps

You can enable diagnostic logging for Java dumps.

### Procedure

1. Go to **Manage > Configuration > Diagnostic logging**.
2. On the **Built-in topics** tab, select the **Show all** check box.
3. Select the **JAVA\_DUMP** topic.
4. Click the More icon `***` and then select **Download topic**.
5. Create a customized `JAVA_DUMP.json` file:
  - a) Open the downloaded `JAVA_DUMP.json` in a text editor.
  - b) Edit the sections `Logger definitions` and `dumpDescription`, as required, to customize the information that you want to capture.
  - c) Save your changes.
6. Enable your custom `JAVA_DUMP.json` file for your Cognos Analytics environment.
  - a) In the **Diagnostic logging** panel, Select the **Custom topics** tab.
  - b) Click the **Upload topic** icon .
  - c) Navigate to the `JAVA_DUMP.json` file that you modified and then click **Open**.

The file is uploaded to Cognos Analytics and **JAVA\_DUMP** appears in the **Custom topics** list.

- d) Click **Apply**.

This message appears:

Successfully enabled topic `JAVA_DUMP`.

7. Go to `installation_location/configuration/data/logging` and open the file `dump_rules.properties` in a text editor and view the content.

**Tip:** This file was created when you enabled your customized `JAVA_DUMP` file and contains the customizations that you set.

**Note:** When a Java dump occurs, it can take a few minutes. After it finishes, two files are produced:

- *installation\_location/bin64/core.core\_id.dmp*
  - *installation\_location/bin64/heapdump.heapdump\_id.phd*
8. Analyze the .dmp and .phd files that were generated by a core dump, as necessary.
  9. When you are done, restore the JAVA\_DUMP.json file used by Cognos Analytics to its default version:
    - a) Select the **Built-in topics** tab and then select **AAA**.
    - b) Click **Reset**.
    - c) Select **AAA** again and then click **Apply**.
  10. To remove your custom **JAVA\_DUMP** topic, follow these steps:
    - a) Select the **Custom topics** tab and then select **JAVA\_DUMP**.
    - b) Click the More icon **\*\*\*** and click **Delete**.
    - c) Click **OK** to confirm the deletion and click **Apply**.

## Using diagnostic logging to troubleshoot Cognos service startup problems

IBM Cognos service startup problems is an example of a situation when diagnostic logging can help you discover the root cause of the problem.

If the Cognos service fails to start before the dispatcher is ready, you need to enable more detailed diagnostic logging in your installation directory before trying to start the service again. By default, minimal logging level is enabled.

### Procedure

1. From the IBM Cognos Analytics with Watson *installation\_location/wlp/usr/servers/cognosserver* directory, open the *bootstrap.properties* file.
2. In this file, add the system property **com.ibm.bi.logging.glug.hint.isready=false** to enable detailed logging.
3. Restart the Cognos service (from Cognos Configuration or from a command line).

At startup, the system property **com.ibm.bi.logging.glug.hint.isready=false** is examined by the logging service before any other services are available.

The restart fails again, but this time with detailed logs in the *installation\_location/logs/cognosserver.log* file. Use these logs to troubleshoot the problem.

4. After the problem is resolved, remove the system property **com.ibm.bi.logging.glug.hint.isready=false** from the *bootstrap.properties* file to disable detailed logging, and restart the Cognos service. After the restart, the default, minimal logging is restored.

**Tip:** If you are not concerned about the length of time that it takes to start the Cognos service, and if you have a sufficient amount of space available, you can leave this property set to false. This will leave detailed logging enabled until the message that the dispatcher is ready appears.

## Enabling IBM Cognos Analytics for Jupyter Notebook

Administrators can configure IBM Cognos Analytics with Watson to connect to a computer that is running IBM Cognos Analytics for Jupyter Notebook.

### Before you begin

IBM Cognos Analytics for Jupyter Notebook must be installed on another computer. For more information, see "Installing IBM Cognos Analytics for Jupyter Notebook" in *Installing and configuring Cognos Analytics*.

## About this task

For a demonstration of how to enable IBM Cognos Analytics for Jupyter Notebook, [watch this video](#).

## Procedure

1. Note the computer name where IBM Cognos Analytics for Jupyter Notebook is installed.
2. Go to **Manage > Configuration > System**, and select **Environment**.
3. In the **Jupyter service location** field, enter the following URL:

```
http://Jupyter_Notebook_server_name:port_number
```

**Tip:** Use `https://` if you have configured SSL on the Jupyter Notebook server. Note that if the Cognos Analytics server is secured with SSL, then the Jupyter Notebook server must also be secured with SSL.

4. Click **Apply**.

## Results

The configuration change is saved and propagated to all dispatchers. You do not need to restart the service for users to connect to Jupyter Notebook.

## What to do next

Ensure that you have assigned either the Notebook capability or roles that include the Notebook capability to your intended Jupyter Notebook users. For more information, see "Notebook capability" in the *IBM Cognos Analytics Managing Guide*. After you complete this task, users can start working with Jupyter Notebook in IBM Cognos Analytics with Watson.

## Enabling access to external Watson Studio notebooks

---

You can configure IBM Cognos Analytics with Watson to connect to an external Watson Studio environment. This allows Cognos Analytics users to access the Watson Studio account's projects and notebooks.

To perform this task, you must be assigned the External Content capability. For more information, see "External Content" in ["Initial access permissions for capabilities"](#) on page 159.

## Procedure

1. Go to **Manage > Configuration > System**, and select **Environment**.
2. In the **Watson Studio URL** field, enter the URL of the Watson Studio server.
3. Enter the Watson Studio API key and sign-on ID that you were assigned when you registered for the Watson Studio environment.
4. Click **Apply**.

## Results

The configuration change is saved and propagated to all dispatchers. You do not need to restart the service for users to connect to the Watson Studio environment.

## What to do next

Ensure that you have assigned either the Watson Studio secured function or roles that include the Watson Studio secured function to your intended Watson Studio notebook consumers. For more information, see "Watson Studio" in ["Initial access permissions for capabilities"](#) on page 159.

After you have enabled access to Watson Studio notebooks, users can perform these actions:

1. Import Watson Studio notebooks. For more information, see "Importing Watson Studio notebooks to Cognos Analytics" in the *IBM Cognos Analytics with Watson Notebook User Guide*.

2. • Add Notebook data to a report. For more information, see "Including output from a notebook" in the IBM Cognos Analytics with Watson *Reporting Guide*.
- Add Notebook data to a dashboard. For more information, see "Adding a notebook widget" in the IBM Cognos Analytics with Watson *Dashboards and Stories User Guide*.

## Advanced settings

You can configure advanced system settings, including a permissions filter and customized key/value pairs.

**Important:** Contact IBM support for details on how to configure advanced settings.

For information about configuring advanced system settings using the Administration console, see "Advanced settings configuration" in the *IBM Cognos Analytics with Watson Administration and Security Guide*.

## Customizing messages in the alerts banner

If you are assigned the System Administrator role, you can update a message that appears in the alerts banner.

**Note:** The System Administrator role is not available to Cognos Analytics on Cloud Hosted customers. To request a customized alert message in Cognos Analytics on Cloud Hosted, contact IBM Support.

### The alerts banner

The alerts banner can display two types of alerts: 1) What's New alerts and 2) Maintenance alerts.

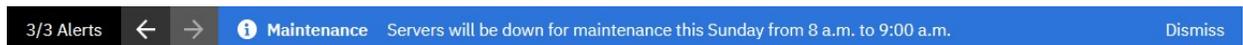
- What's New alerts

By default, users can click the arrow icon  in the alerts banner to see two **What's New** messages appear:



- Maintenance alerts

The administrator can add a Maintenance alert to help users stay informed of company-specific details.



### Add or remove a maintenance message

Add a message to the alerts banner to help users stay informed of upcoming maintenance.

1. Click **Manage > Configuration > System**, and select **Advanced Settings**.
2. Type `Glass.maintenanceMessage` in the **Key** field.

**Tip:** You must match the case as shown.

3. Enter your maintenance message in the **Value** field.

For example, type `Our servers will be down for maintenance this Saturday between 1:00 a.m. and 6:00 a.m.` in the **Value** field.

As another example, a message in the alert banner is written in English, but the users speak mainly Spanish. As the System Administrator, you replace the message with a translated version.

4. If you want to remove a maintenance message, follow these steps:
  - a. Type `Glass.maintenanceMessage` in the **Key** field.

b. Click in the **Value** field.

**Tip:** Even if a value is already set, it does not appear until you click in the field.

The current maintenance message appears.

c. Delete the message in the **Value** field.

5. Click **Apply**.

6. Refresh your browser window.

Depending on which setting you chose, your message appears in, or is removed from, the alerts banner.

## Add a link to a maintenance message

Add a link to a maintenance message that points users to a web site.

1. Click **Manage > Configuration > System**, and select **Advanced Settings**.

2. Type `Glass.maintenanceMessage` in the **Key** field.

**Tip:** You must match the case as shown.

3. Enter your maintenance message, including a reference to the link you are adding, in the **Value** field.

For example, type `For more information about our product, click More info` in the **Value** field.

4. Type `Glass.maintenanceLink` in the **Key** field.

**Tip:** You must match the case as shown.

5. Enter the URL of the web site that you want to link to in the **Value** field.

6. Click **Apply**.

7. Refresh your browser window.

Your maintenance message appears in the alerts banner. When you click **More info** to the right of the alerts banner, the web site that you linked to opens in a new tab.

8. Inform users that they can click **More info** to view the web site that you linked to.

## Disable or enable the What's New alerts

Specify whether the What's New messages appear in the alerts banner.

**Note:** If you create a maintenance message but disable the What's New messages, the maintenance message still appears.

1. Click **Manage > Configuration > System**, and select **Advanced Settings**.

2. Type `Glass.disableWhatsNewAlerts` in the **Key** field.

**Tip:** You must match the case as shown.

3. Type `true` in the **Value** field.

4. If you want to reinstate the What's New messages in the alerts banner, follow these steps:

a. Type `Glass.disableWhatsNewAlerts` in the **Key** field.

b. Type `false` in the **Value** field.

5. Click **Apply**.

6. Refresh your browser window.

Depending on which setting you chose, only the What's New messages disappear from, or are reinstated in, the alerts banner.

## Disable or enable all messages

You can remove the alerts banner. This prevents both the What's New messages and your maintenance message from appearing to users.

1. Click **Manage > Configuration > System**, and select **Advanced Settings**.
2. Type `Glass.disableAlertEntry` in the **Key** field.  
**Tip:** You must match the case as shown.
3. Type `true` in the **Value** field.
4. If you want to reinstate the What's New messages and, if you have one, a maintenance message in the alerts banner, follow these steps:
  - a. Type `Glass.disableAlertEntry` in the **Key** field.
  - b. Type `false` in the **Value** field.
5. Click **Apply**.
6. Refresh your browser window.

Depending on which setting you chose, the alerts banner either appears or does not appear to users.

## Defining authentication parameters for login URLs

Use the `Glass.urlLoginParameters` advanced setting to allow namespace logging parameters contained in a URL to be passed to the authentication provider.

For example, the administrator defines the parameters `CAMNamespace`, `CAMPassword`, and `CAMUsername`. A user then logs on by entering a Cognos Analytics URL that is appended with their credentials. The parameters are then passed to CAM for authentication. The login URL would appear as follows:

```
http://yourserver:yourport/bi?  
CAMNamespace=myNamespace&CAMUsername=myUser&CAMPassword=myPassword.
```

### Procedure

1. Click **Manage > Configuration > System**, and select **Advanced Settings**.
2. Type `Glass.urlLoginParameters` in the **Key** field.
3. Enter a parameter name in the **Value** field.  
**Tip:** You can enter multiple parameter names separated by commas.
4. Click **Apply**.

## Setting the SameSite attribute on cookies

Configure the `Configuration.cookieSameSite` cookie attribute to prevent cross-domain errors in your Cognos environment.

To prevent cross-site request forgery (CSRF) attacks, some browsers may return error messages if HTML files containing `iFrames` are hosted in a different domain than the report server. To avoid these errors, you can configure the `Configuration.cookieSameSite` advanced setting.

If you are embedding a Cognos Analytics dashboard in a Microsoft Teams environment, you must set this attribute. For more information, see [Embedding a dashboard in Microsoft Teams](#).

### Before you begin

The following configuration must be in place:

- SSL is enabled
- XSRF protection must be enabled. For more information, see [XSRF \(Cross-Site Request Forgery\)](#).

**Important:** You must enable SSL access *before* you set Configuration.cookieSameSite=None. Otherwise all users, including administrators, will be locked out of Cognos Analytics.

## Procedure

1. Click **Manage > Configuration > System**, and select **Advanced Settings**.
2. In the **Key** field, type the following:

```
Configuration.cookieSameSite
```

3. Type None in the **Value** field.
4. Click **Apply**.
5. Refresh your browser window.

## Results

Applications in your Cognos environment with a different domain no longer produce error messages.

## Enabling an option to include performance details

Set the DISP.zipi.IPAEnabled attribute to show the option **Include performance detail** when a user is preparing to run a report in the background.

If a user selects **Include performance detail**, an internal Cognos Analytics tool, IPPA (In Product Performance Assistant), is invoked when the report runs. IPPA can help Report and Dashboard Authors who require detailed performance analysis.

For more information, see [Using IPPA in IBM Cognos Analytics 11.2](https://www.ibm.com/support/pages/node/6457641) (https://www.ibm.com/support/pages/node/6457641).

## Procedure

1. Click **Manage > Configuration > System**, and select **Advanced Settings**.
2. Type DISP.zipi.IPAEnabled in the **Key** field.
3. Type true in the **Value** field.
4. Click **Apply**.
5. Refresh your browser window.

## Adjusting the chunk size of files uploaded to the cloud

You can change the default size of data chunks that are delivered as files are uploaded to a cloud storage location.

You may need to adjust the chunk size if a user receives an Error uploading report\_name message when they try to save a file to the cloud.

## Procedure

1. Click **Manage > Configuration > System**, and select **Advanced Settings**.
2. Type multipart-chunk-size-mb in the **Key** field.
3. Click in the **Value** field.

The default value, 15, appears.

4. Delete 15 and then enter a value that is larger than the number of MB of any files that you plan to save to the cloud.

For example, type 50 in the **Value** field.

5. Click **Apply**.

## Setting response headers for HTTP requests

If your environment does not include a web server, response headers for HTTP requests do not include a value for X-FRAME-OPTIONS. The following steps describe how to include X-FRAME-OPTIONS in the response headers.

**Note:** We recommend that you install a web server in your Cognos Analytics environment.

### Procedure

1. Click **Manage > Configuration > System**, and then select **Advanced Settings**.
2. Type `BIHeaderFilter.responseHeaders` in the **Key** field.
3. Type `[{"name": "X-FRAME-OPTIONS", "value": "SAMEORIGIN"}]` in the **Value** field.
4. Click **Apply**.
5. Type `BIResponseWrapper.staticExpiresDays` in the **Key** field.

**Note:** The default value is 7 (days).

6. Type a value, for example 10, in the **Value** field, signifying the number of days.

In this example, static content, such as .css file and .js files, will now stay in cache for ten days before it expires. This sets the value for the HTTP response headers "Expires" and "max-age" when responding to GET requests for static content.

7. Click **Apply**.
8. Refresh the page.

## Changing the query operator in searches

Configure the `SearchService.queryOperator` to change the query operator that is used in Cognos Analytics **Search** fields.

By default, search results on multi-term queries are based on the AND logical operator. Using the `SearchService.queryOperator` key, you can specify that multi-term queries use the OR logical operator instead.

### Procedure

1. Click **Manage > Configuration > System**, and select **Advanced Settings**.
2. Type `SearchService.queryOperator` in the **Key** field.
3. Click in the **Value** field.  
The default value, AND, appears.
4. Delete AND and then type OR in the **Value** field.
5. Click **Apply**.
6. Refresh your browser window.

### Results

Multi-term queries will now use the OR logical operator between terms.

## Limiting the number of emails sent when a report is delivered

You can control the number of emails that are sent when a report is delivered by email.

### Procedure

1. Click **Manage > Configuration > System**, and select **Advanced Settings**.
2. Type `limit.per.email.sender` in the **Key** field.
3. Click in the **Value** field.

The default value, 500, appears. This means that a single sender can send up to 500 emails every two minutes. After the counter reaches the limit, no additional emails are sent.

4. If you want to change the number of emails sent, delete 500 and type another number in the **Value** field.
5. Click **Apply**.

## Configuring the default view for the content page

The content page can be displayed in the tile view or list view. You can configure any of these views as the default view.

**Note:** The tile view is the default view if you don't configure this setting.

### Procedure

1. Click **Manage > Configuration > System**, and select **Advanced Settings**.
2. In the **Key** field, type `Content.defaultView`.
3. Click in the **Value** field, and specify one of the following values:

#### **tile**

Sets the content page default view to tile.

#### **list**

Sets the content page default view to list.

4. Click **Apply**.

## Disabling the default cleanup of labels in data modules

When a data module is created, the table and column labels are automatically cleaned up in English and some other languages so that the labels are easier to read. The cleanup is done only in data modules that are created from data server connections and uploaded files.

For example, characters such as underscore (`_`), dash (`-`), or slash (`\`) are replaced with the space character. As a result, a label such as `Vehicle_class` is changed to `Vehicle Class`.

If this cleanup produces unintended results, for example, removes diacritical marks from words in some languages, you can disable it. To do that, set the following advanced settings to **false**:

- **ModelingService.dbDefaultCleanLabels**

Disable the cleanup of both table and column labels in tables that are sourced from data servers.

- **DatasetService.cleanTableLabels** and **DatasetService.cleanColumnLabels**

Disable the cleanup of table and column labels in tables that are sourced from uploaded files. The settings must be used together.

### Procedure

1. Click **Manage > Configuration > System**, and select **Advanced Settings**.
2. Depending on the type of data that the tables in the data module are based on, specify the following settings:
  - To disable the cleanup of labels in tables that are sourced from data servers, in the **Key** field, type `ModelingService.dbDefaultCleanLabels`, and in the **Value** field, type `false`.
  - To disable the cleanup of labels in tables that are sourced from uploaded files, in the **Key** field, type `DatasetService.cleanTableLabels`. In the **Value** field, type `false`. Then, repeat the same step for **DatasetService.cleanColumnLabels**. Both settings must be specified.
3. Click **Apply**.

## 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*.

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 111](#).

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 be 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 *Secured Functions and Features*.

**Note:** Cognos Analytics Processor Value Units (PVUs) are licensed according to the dispatcher service. Each license must be associated with a unique dispatcher service. This association allows IBM License Metric Tool (ILMT) to accurately calculate the PVU value for each Cognos Analytics client license. For more information, see [License Metric Tool - Getting started](#).

### 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.

**Note:** Cognos Analytics Processor Value Units (PVUs) are licensed according to the dispatcher service. Each license must be associated with a unique dispatcher service. This association allows IBM License Metric Tool (ILMT) to accurately calculate the PVU value for each Cognos Analytics client license. For more information, see [License Metric Tool - Getting started](#).

For information about defining routing rules, see [“Dispatcher routing” on page 111](#).

**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”](#) on page 112.

## Setting routing rules for dispatchers

You can set routing rules for server groups that allow you to send specific types of reports to different servers.

### Procedure

1. Select **Manage > Configuration > Routing rules**.
2. Click **New routing rule**.

**Tip:** You can select the pencil icon  beside the tag name.

3. Assign a data tag.
  - a) Click the down chevron icon  in the **Data tag** field.  
Any existing tags are listed.
  - b) If you want to create a new tag:
    - i) Click **New data tag**.
    - ii) Enter a tag name.
    - iii) Click the Add icon .
    - iv) In **Team content** or **My content**, click one or more packages, data modules, or uploaded files.
    - v) Click **Select**.
    - vi) Click **Create**.
  - c) Click the data tag that you want to associate with the routing rule.

**Tip:** To modify the data objects associated with a tag or to change its name, select the pencil icon  beside the tag name.

4. Assign a group tag.
  - a) Click the down chevron icon  in the **Group tag** field.  
Any existing tags are listed.
  - b) If you want to create a new tag:
    - i) Click **New group tag**.
    - ii) Enter a tag name.
    - iii) Click the Add icon .

- iv) In the **Open File** panel, click a namespace, for example **Cognos**.
- v) Click the groups that you want to associate with the routing rule.
- vi) Click **Open**.
- vii) Click **Create**.

The tag is created.

- c) Click the group tag that you want to associate with the routing rule.

**Tip:** To modify the groups associated with a tag or to change its name, select the pencil icon  beside the tag name.

#### 5. Assign a role tag.

- a) Click the down chevron icon  in the **Role tag** field.

Any existing tags are listed.

- b) If you want to create a new tag:

- i) Click **New role tag**.

- ii) Enter a tag name.

- iii) Click the Add icon .

- iv) In the **Open File** panel, click a namespace, for example **Cognos**.

- v) Click one or more roles that you want to associate with the routing rule.

- vi) Click **Open**.

- vii) Click **Create**.

The tag is created.

- c) Click the role tag that you want to associate with the routing rule.

**Tip:** To modify the roles associated with an existing tag or to change its name, select the pencil icon  beside the tag name.

#### 6. Assign a server group.

- a) Click the down chevron icon  in the **Server group** field.

Any existing server groups are listed.

- b) Click **View server group details**.

- c) If server groups exist, the URL of each server group is listed. Go to step “6.e” on page 113.

- d) If the message **No server group found** appears, click the **Advanced Administration Console** link and then [create a server group](#).

- e) Click the server group that you want to associate with the routing rule.

#### 7. You can further modify your routing rules, as follows:

- To create additional routing rules, click **New routing rule**, as described in the previous steps.
- To see which data objects, groups, roles and server group URLs are associated with each routing rule, click the More button  next to the routing rule and then select **Detail view**.

 **Details for Rule 2**

Select a data, group, or role tag and map it to a server group to create a rule.

Data tag	Group tag	Role tag	Server group
<div style="border: 1px solid #ccc; padding: 2px;">my_data_tag</div> <ul style="list-style-type: none"> <li> Customer analysis <small>Team Content &gt; Samples &gt; Data</small></li> <li> California website visits <small>Team Content &gt; Samples &gt; Data</small></li> </ul>	<div style="border: 1px solid #ccc; padding: 2px;">my_group_tag</div> <ul style="list-style-type: none"> <li> testers <small>Directory &gt; Cognos</small></li> <li> reviewers <small>Directory &gt; Cognos</small></li> </ul>	<div style="border: 1px solid #ccc; padding: 2px;">my_role_tag</div> <ul style="list-style-type: none"> <li> Consumers <small>Directory &gt; Cognos</small></li> <li> Analytics Explorers <small>Directory &gt; Cognos</small></li> </ul>	<div style="border: 1px solid #ccc; padding: 2px;">my_server_group</div> <ul style="list-style-type: none"> <li> http:// my_server :9300/p2pd</li> </ul>

**Tip:** To return to the list of routing rules, click the back icon  beside the panel title, **Details for Rule number**.

- To create a rule with similar associations as an existing rule, click the More button  next to the routing rule and then select **Duplicate**. You can then modify the tags, as necessary.
  - To remove a routing rule, click the More button  next to the routing rule and then select **Delete**.
8. Click **Apply changes**.

Your changes to all routing rules are saved.

## Results

Reports will now 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 group or role running the report.

---

## Chapter 6. Schedules and 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

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 Action menu icon , and then click **Properties**.
2. In the **Properties** pane, click the **Schedule** tab, and then:
  - Click **Create schedule**.

Schedule Options Prompts

**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.

- 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: 1 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  Hour(s) ▼

between

and

**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.

**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.

**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  PDF  Excel

[Edit options](#)

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**

**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  PDF  Excel

[Edit options](#)

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**

**Priority**

3

**Format**

HTML

**Delivery**

Save

**Languages**

English (United States)

[Reset default options](#)

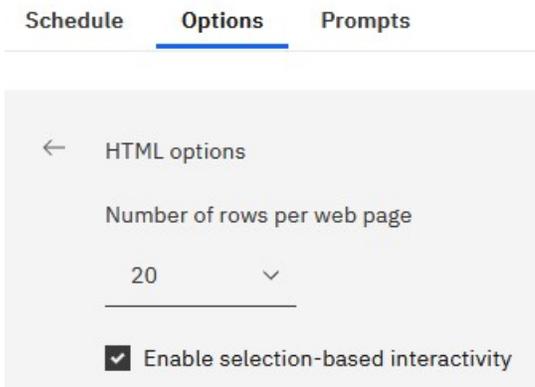
**Tip:**

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**.



**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**.

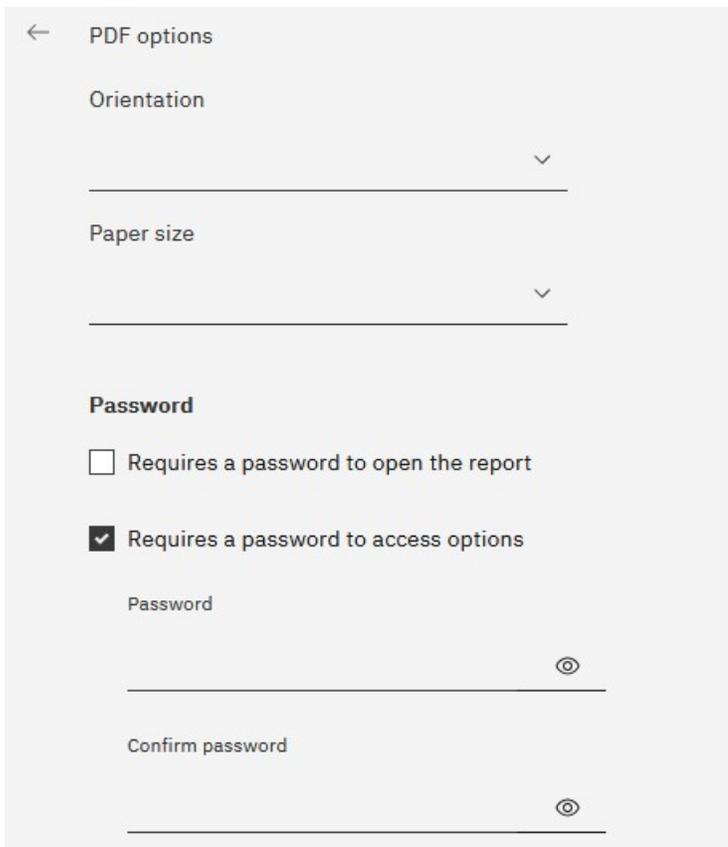


Figure 3. PDF options - part 1

**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 document's content
- Add or modify text annotations
- Fill in forms and sign the document
- Assemble the document (insert...create navigation elements)

Allow content extraction

- Extract text for screen reader devices
- Copy of text, images, and other content

Figure 4. 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 5. 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.



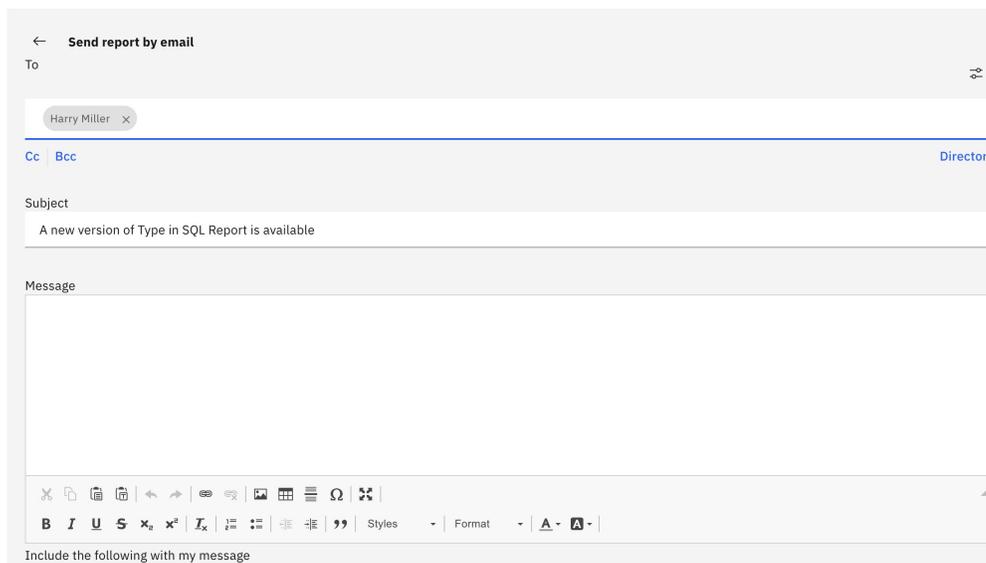
Figure 6. PDF options - part 1

**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**.



**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**.

Schedule Options Prompts

Summary

Send report to mobile device

Directory

Cognos

LDAP

Add Close

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

Network address

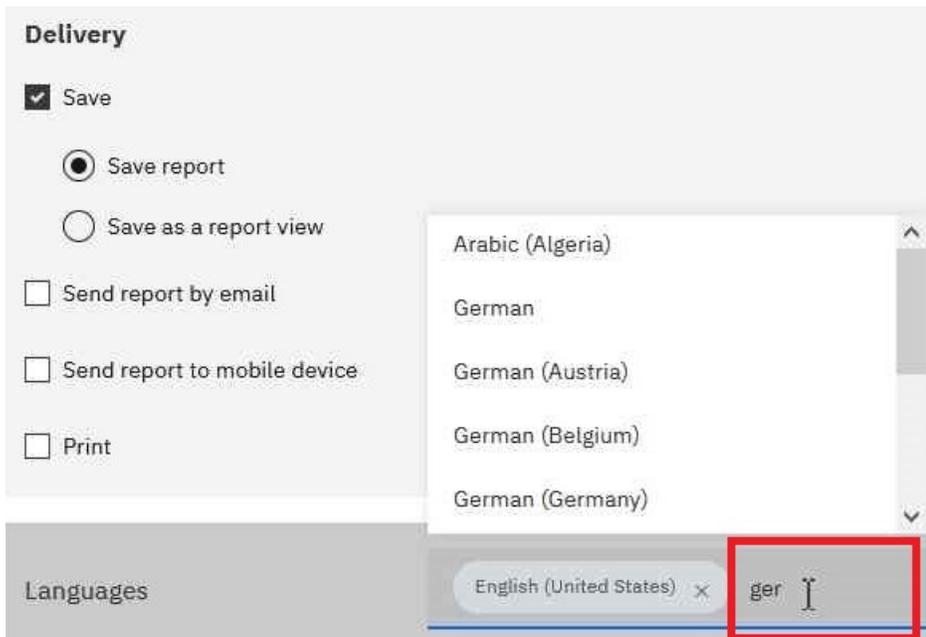
**Tip:** It may be convenient for you to have a printed copy of a report.

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).



**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**.



**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

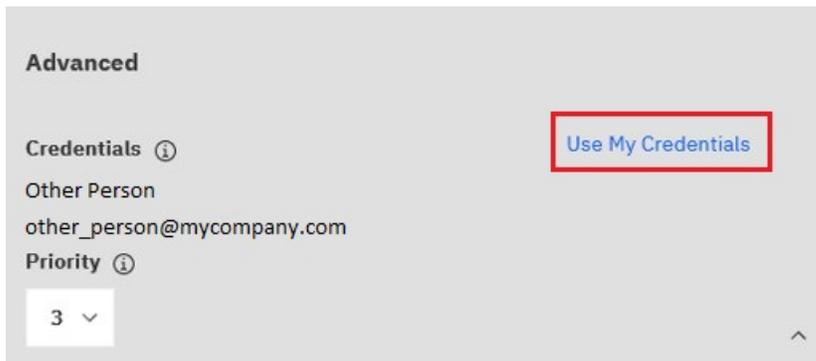
---

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 Action menu 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.



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.

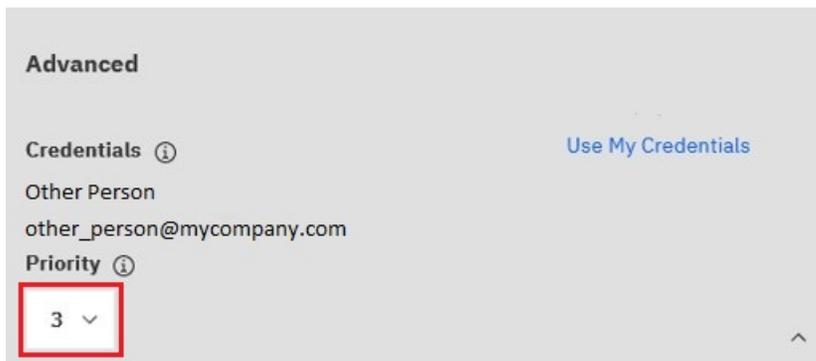
When you schedule a job, you set the priority for the whole job, not for individual entries within the job. You may want to set a low priority for a job with many entries so that other entries in the queue are not delayed.

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 Action menu 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.



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 shows 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 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 change the priority of an entry in the queue .

## Procedure

1. From the **Manage** menu, click **Activities**.
2. Click the type icon , and then click **Upcoming**.

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.

## Managing past activities from the Manage tool

---

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 .

### Procedure

1. From the **Manage** menu, click **Activities**.
2. Click the type icon , and then click **Past**.

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, click the Filter icon .

**Tip:** You can filter by the following attributes:

- The user who performed the activity.
- The activity owner.
- The activity status.
- The activity type.

The following diagram shows an example of how past activities are displayed from the Manage tool. 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. These two report runs appear in the list below the job that contained them.

## < Activities

Past ▾

2020-02-12

Stacked

Applied



Scheduled by: Harry Miller (hmiller)

Name	Request time	Run by	Status
>  Product line revenue	2/12/2020 2:50 PM	Harry Miller	Succeeded
>  Metrics	2/12/2020 2:53 PM	Harry Miller	Succeeded
>  Corporate website visits	2/12/2020 2:53 PM	Harry Miller	Succeeded
>  Global sales	2/12/2020 2:53 PM	Harry Miller	Succeeded

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 activity, click the More icon for the entry and choose an action:
  - Click **Run once** to perform the activity again.
  - Click **View versions** to see details about previous runs of the report.
  - Click **Run details** to see information about the most recent run of the report.

## 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.

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, and user who owns the entry.

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 and view the run history .

## Procedure

1. From the **Manage** menu, click **Activities**.
2. Click the type icon , and then click **Current**.
3. In the **Filter** section, specify the filtering options that you want to use.

**Tip:** If you want to use advanced filtering options, click **Advanced options**.

4. Click **Apply**.

The list shows the entries that you selected.

---

## Chapter 7. 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 with Watson 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 131](#).

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 133](#).

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.

---

### Creating tenants

System administrators must create and enable the tenant object before the tenant users can access IBM Cognos Analytics with Watson.

#### 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 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 with Watson, 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.

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 with Watson 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**.

## 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 with Watson 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.
- Terminate user sessions and customize tenants.
- Change tenancy on objects in the content store.

**Tip:** The **Tenant Administrators** role is one of the built-in entries in the Cognos namespace.

For information about the role of **System Administrators** in a multitenant environment, see [Chapter 7, “Tenant administration,”](#) on page 131.

## 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 with Watson 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.

## 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 with Watson and the tenants are created in **Manage > Multitenancy**. For more information, see [“Creating tenants” on page 131](#).

### 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](http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.ug_cra.doc/c_config_mt_advanced.html) (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 with Watson as a member of the **System Administrators** role.
2. In **Manage**, select the **Multitenancy** tab.
3. Select the **Add +** 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 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.

## Customizing tenants

---

You can apply themes to individual tenants. You can also specify that a customized home page, or a particular report or dashboard, be displayed when a user with a particular tenant ID opens IBM Cognos Analytics with Watson. You can also remove default user interface features for tenants.

Before setting customized themes and home pages (other than a dashboard or report) you must have created and uploaded custom themes or home pages. For more information, see [Chapter 9, “Customizing Cognos Analytics across all roles,”](#) on page 211.

In **Manage > Multitenancy**, click a tenant. The slide-out panel for that tenant has a **Customization** tab. For more information, see [“Applying themes, extensions, and views”](#) on page 247.

### Setting a default home page

Click the next  icon next to the default home page. You can now browse for a dashboard or report to be the default home page, or you can select a view in the list of views to be the default home page for all users of this tenant.

### Removing features

You can choose user interface features to remove for the tenant. Click the next  icon next to **Features**. A list of views is displayed. This list includes both the built-in views and any custom views that have been uploaded. Click a view to see a high-level grouping of features for the view. Click  next to a grouping to drill-down to a lower level of features. You can deselect any features in this list, or drill-down to another set of features to deselect. Click **Apply** to save your changes. You can revert your changes by clicking **Reset to defaults**.

### Setting a default theme

Click  next to the default theme. You can select a theme in the list of themes to be the default theme for this tenant.

### Creating a custom folder

Click  next to **Custom folder** to set a custom content folder for this tenant. When a user with this tenant ID logs in, the custom folder is displayed on the navigation bar below **Team content**.

### Setting the default location for uploaded files

Click  next to **Default upload location** to specify a folder in **Team content** as the default location for uploaded files for this tenant.

## Parameters

Add content here and for roles.

## Defining regional settings for tenants

---

A system administrator can specify regional settings for a tenant.

The regional settings apply to all IBM Cognos Analytics components, such as reporting, dashboarding, modeling, administration, and so on. These settings also apply to the companion applications such as IBM Cognos Analysis Studio, IBM Cognos Event Studio, and so on.

The following settings can be specified:

### Time zone

The time zone of the tenant users.

### Product language

The language of the IBM Cognos Analytics user interface.

### Content language

The language used to view and produce content in IBM Cognos Analytics, such as data in reports, dashboards, and stories.

### Bidirectional language support

This setting applies to languages such as Arabic, Hebrew, Urdu, or Farsi. Using this setting, you can control the direction of text in entry names, descriptions, labels and tooltips, input boxes, comments, and in structured text, such as email addresses, file paths, breadcrumbs, URLs, and date and time formats.

Select one of the following options from the **Base direction for text: Right-to-left, Left-to-right, Contextual**. When the **Contextual** option is selected, the text direction depends on the first letter in the text. If the letter belongs to a right-to-left script, the text direction is right-to-left. Otherwise, the text direction is left-to-right. Numbers and special characters do not influence the text direction. For example, if the text starts with a number followed by an Arabic letter, the direction is right-to-left. If the text starts with a number followed by a Latin letter, the direction is left-to-right

## Procedure

1. In **Manage**, select the **Multitenancy** tab.
2. From the tenant context menu, click **Properties**.
3. Click the **Regional** tab, and specify the settings.

## Results

By default, all tenant users inherit these settings. Depending on their access permissions, the users can personalize these settings later.

## Setting up notifications for tenants

---

A system administrator can configure an email account, called tenant sender, from which the tenant users receive emails.

The tenant sender account overwrites the default sender account that is specified when configuring the mail server for IBM Cognos Analytics.

**Tip:** The default sender is configured in IBM Cognos Configuration, under **Data Access > Notification**.

## Procedure

1. In **Manage**, select the **Multitenancy** tab.
2. From the tenant context menu, click **Properties**.

3. On the **Notifications** tab, select **Tenant Sender** and specify the corresponding email address. Click **Apply**.

### Results

The tenant sender email account is now associated with distributing IBM Cognos Analytics content.

## 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 137](#).

### 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 with Watson 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*.

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 137](#).

### 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 with Watson. This might be needed if the tenant was permanently moved to a different instance of IBM Cognos Analytics with Watson.

### 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 137.](#)

### 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**.

---

## Chapter 8. Managing access

Administrators define the levels of access that each user, role, and group has to the features and components in Cognos Analytics.

As administrator, you are responsible for securing the predefined roles in the Cognos Users namespace. You define which capabilities are assigned to each user, group, and role. You also manage capabilities as they relate to license role entitlements.

---

### Access permissions for an entry

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.

Permissions	Permitted Actions
Read	<p>View all the properties of an entry, including the report specification, report output, and so on, which are properties of a report.</p> <p><b>Note:</b> A dashboard requires read permission both on the dashboard itself and on any data sources that it uses.</p>
Write	<p>Modify properties of an entry.</p> <p>Delete an entry.</p> <p>Create entries in a container, such as a package or a folder.</p> <p>Modify the report specification for reports created in Reporting and Query Studio.</p> <p>Create new outputs for a report.</p>
Execute	<p>Process an entry.</p> <p>For entries such as reports, agents, and metrics, the user can run the entry.</p> <p>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.</p> <p>For credentials, users can permit someone else to use their credentials.</p> <p><b>Note:</b> Users must have execute permissions for the account they use with the run as the owner report option.</p>

Permissions	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. <b>Note:</b> 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.

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
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

Table 10. Access permissions required for actions (continued)

Action	Permissions required
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 11. Report access permissions and permitted actions

Permissions	Permitted actions
Read	<p>Users can view the report in the content pane.</p> <p>Users cannot expand the report to show the report parts.</p> <p>Users cannot drag the report.</p>
Read and Traverse	<p>Users can view the report in the content pane.</p> <p>Users cannot expand the report to show the report parts.</p> <p>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.</p> <p>Users can view saved output in the workspace.</p> <p>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.</p>
Execute	<p>Users can view the report in the content pane.</p> <p>Users cannot expand the report to show the report parts.</p> <p>Users can execute the report, but interactions are not available. Interactions are not available if:</p> <ul style="list-style-type: none"> <li>• a report is dragged to the canvas</li> <li>• if a user with execute permissions saves a report, and other users open the report</li> <li>• if a user with execute permissions opens a workspace created by other users</li> </ul> <p>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.</p>

*Table 11. Report access permissions and permitted actions (continued)*

<b>Permissions</b>	<b>Permitted actions</b>
Read and execute	<p>Users can view the report in the content pane.</p> <p>Users can expand the report to show the report parts.</p> <p>Users can execute the report and interactions are available.</p> <p>In the content pane, users cannot save report changes.</p> <p>If users add the report to the workspace and save it, report changes can be saved.</p> <p>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.</p>
Read, execute, traverse	<p>Users can view the report in the content pane.</p> <p>Users can expand the report to show the report parts.</p> <p>In the content pane, users can execute the report and interactions are available.</p> <p>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.</p>
Read, write, execute, traverse	<p>Users can view the report in the content pane.</p> <p>Users can expand the report to show the report parts.</p> <p>Users can add the report to the workspace.</p> <p>Users can execute the report and interactions are available.</p> <p>Users can change and save the report.</p> <p>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.</p>
Read, execute, set policy	<p>Users can view the report in the content pane.</p> <p>Users can expand the report to show the report parts.</p> <p>Users can execute the report and interactions are available.</p> <p>In the content pane, users cannot save report changes.</p> <p>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.</p>

For report parts, users with the following access permissions and combinations of permissions can perform the following actions:

*Table 12. Report part access permissions and permitted actions*

<b>Permissions</b>	<b>Permitted actions</b>
Read and execute	<p>Users can view the report.</p> <p>Users can expand the report to show the report parts.</p> <p>Users can drag the report part onto the canvas and can execute the report part.</p>

For folders, users with the following access permissions and combinations of permissions can perform the following actions:

<i>Table 13. Folder access permissions and permitted actions</i>	
<b>Permissions</b>	<b>Permitted actions</b>
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:

<i>Table 14. Workspace access permissions and permitted actions</i>	
<b>Permissions</b>	<b>Permitted actions</b>
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. 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.

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. Click **Manage > Configuration > System**, and select **Advanced Settings**.
2. Type SetPolicyPackage in the **Key** field.
3. Click in the **Value** field.  
The default value, TRUE, appears.
4. Type FALSE in the **Value** field.
5. Click **Apply**.
6. Refresh your browser window.

A package will now inherit the permissions of its parent folder.

**Tip:** You can also update the SetPolicyPackage value by editing the file `installation_directory\configuration\fm.ini`. However, the value in the **Advanced Settings** parameter overrides the value contained in the `fm.ini` file.

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

## 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 with Watson. 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.

## Setting access permissions for an entry

You can specify access permissions for all entries in Cognos Analytics.

Some examples of such entries are dashboards, reports, queries, packages, agents, namespaces, groups, users, or folders.

When setting access permissions, you can reference users, groups, and roles from different namespaces. 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**.

**Note:** For the access permissions to take effect, ensure that the **Everyone** group is removed from the entry security policy.

## About this task

To administer security, you must have **Set policy** permissions, or own the entries. For more information, see [“Access permissions for an entry”](#) on page 139.

### Note for Cognos Analytics On-Demand users:

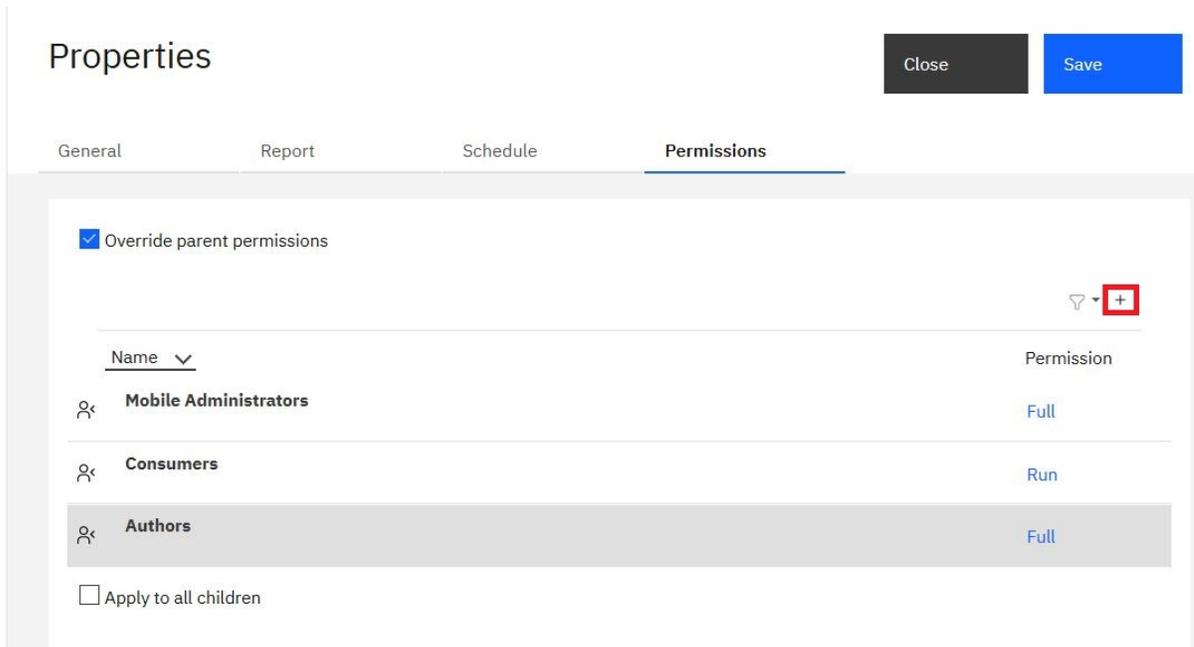
- In this offering, the [Standard built-in groups and roles](#) in the Cognos namespace do not exist.
- You cannot change the capabilities of a user, group, or role. Capabilities are determined by the user's [On-Demand subscription level](#).

## Procedure

1. In the Cognos Analytics **Content** pages, locate the entry for which you want to set access permissions, and select its checkbox.
2. From the entry context menu , click **Properties**.
3. In the **Properties** page, click the **Permissions** tab.
4. Select the **Override parent permissions** checkbox.

You can now modify permissions for users, groups, or roles that already have access for the entry, or add new users, groups, or roles to the security policy for the entry.

To add new users, groups, or roles, click the plus icon, as shown in the following image:



The screenshot shows the 'Properties' dialog with the 'Permissions' tab selected. The 'Override parent permissions' checkbox is checked. Below this, there is a table with columns for 'Name' and 'Permission'. The table lists three entries: 'Mobile Administrators' with 'Full' permission, 'Consumers' with 'Run' permission, and 'Authors' with 'Full' permission. A plus icon in a red box is highlighted next to a filter icon in the top right corner of the table area. At the bottom, there is an unchecked checkbox labeled 'Apply to all children'.

Name	Permission
Mobile Administrators	Full
Consumers	Run
Authors	Full

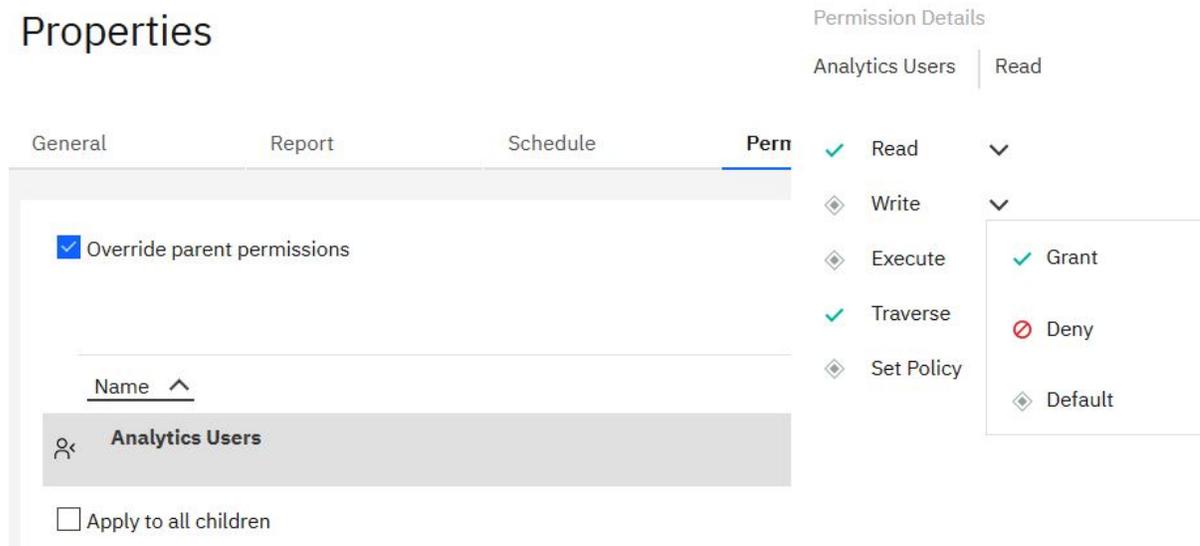
Locate the required items within the namespace, and click **Add**. The users, groups, or roles are added with the **Read** access. Click the arrow icon next to **Read** to assign a different type of access for the entry: **Run**, **Write**, or **Full**.



To remove a user, group, or role from the list, click its remove icon .

If the **Everyone** group is still in the list, remove this group after other users, groups, or roles are added.

To view and set more granular access permissions, click the permission name. The following detailed permissions are shown:



For more information, see [“Access permissions for an entry”](#) on page 139.

5. If you are setting permissions for an entry, such as a folder or a package, that contains other entries, and you want the children entries to inherit the same permissions, select the **Apply to all children** checkbox.
6. Click **Save** to apply the changes to the entry security policy.

## Security settings after installation

Your IBM Cognos software installation must already be configured to use an authentication provider, which is documented in the [Configuring IBM Cognos Analytics with Watson 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 Users** 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.

## Securing System Administrators and standard 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 standard roles.

If the group **Everyone** is a member of a standard role, remove the group from the role membership.

**Note:** For a list of the default capabilities that are assigned to each role, see [“Initial access permissions for capabilities”](#) on page 159.

### Procedure

1. From **Manage > People**, click **Accounts**.
2. Click the **Cognos** namespace.
3. For the role that you want to modify, click the More icon  and then click **Properties**.
4. 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.
5. On the **Permissions** tab, set access permissions for this role to prevent unauthorized users from creating, updating, or deleting the content, and then click **Apply**.
6. For each role that you want to modify, repeat steps 3 to 5.

## Securing the Cognos namespace

You can setup the Cognos namespace as follows.

### Procedure

1. From **Manage > People**, click **Accounts**.
2. Next to the Cognos namespace, click the context menu icon  and then click **Properties**.
3. 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.

4. If you want, select the **Apply to all children** check box.
5. Click **Apply**.

## Setting access for Team content

**Team content** is the root folder for all shared Cognos Analytics content. Permissions that are set for this folder provide a baseline on which object permissions and capabilities can be further refined.

### Procedure

1. From the **Open menu** , click **Content**.
2. Click the **Team content** tab, and in the actions toolbar, click the **Details** icon.



3. In the **Details** panel, click **Properties**.
4. In the **Properties** page, click the **Capabilities** tab to set global object capabilities, or the **Permissions** tab to set global access permissions for content.

## User capabilities

Content Manager reads the user's permissions at logon time. Depending on the permissions for the secured functions and features, the user can access specific components and perform specific tasks in the Cognos Analytics user interface.

The **Capabilities**, 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 Cognos Analytics.

Examples of the secured functions are **Administration** and **Reporting**. Examples of the secured features are **User Defined SQL** and **Bursting**.

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.

Users can see a list of the secured functions and features that are available to them in Personal menu  under **Profile and settings > Profile > My Capabilities > View details**.

For more information, see [“Initial access permissions for capabilities”](#) on page 159.

**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 to assign capabilities. If a capability's administration can be performed only via the **Manage** component, it is noted in its description in the following list.

### 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 **Administration console** or in **Data server connections** under **Manage** to define data sources, connections, and signons. In IBM Cognos Analytics with Watson 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**

Administrators with this capability can assign the [Develop Visualizations](#) secured function to users, groups, and roles, allowing them access to custom visualizations.



**CAUTION:** Be judicious when you assign **Develop Visualizations** access and ensure that you review files that are being uploaded. People who are permitted to upload files may be able to deliver malicious code.

- **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.

**Note:** To administer this capability and its secured functions, you must select **Manage > People > Capabilities**. You cannot administer this capability from the **Administration console**.

The following secured features are associated with this function:

- **Learning**

This secured feature allows the system to learn from an assignee's product usage.

**Tip:** This feature is not available as an object capability.

- **Use Assistant**

This secured feature allows designated users to use the Assistant. The **Use Assistant** capability can be set at the user level or source level.

## 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

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.

**Note:** To administer this capability, you must select **Manage > People > Capabilities**. You cannot administer this capability from the **Administration console**.

## Cognos Analytics for Mobile

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](#).

**Note:** To administer this capability and its secured functions, you must select **Manage > People > Capabilities**. You cannot administer this capability from the **Administration console**.

## 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 with Watson 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 168](#) section.

The following secured feature is associated with this function:

- **Create/Edit**

This secured function controls access to the **New > Dashboard** and **New > Story** functions. Users require Execute permissions for the Dashboard and Create/Edit capability to both create or edit dashboards and stories.

## 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 tracking for Cognos Desktop Tools products. Users with this capability are members of the Analytics Explorers role. This allows an admin to track the users in the license counter. Products that will count as a desktop tool include Planning Analytics 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.



**CAUTION:** Be judicious when you assign **Develop Visualizations** access and ensure that you review files that are being uploaded. People who are permitted to upload files may be able to deliver malicious code.

## 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

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](#).

**Note:** To administer this capability and its secured functions, you must select **Manage > People > Capabilities**. You cannot administer this capability from the **Administration console**.

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* section.

## **External Content**

This capability allows the assignee to use content from sources that are external to IBM Cognos Analytics.

**Note:** To administer this capability and its secured functions, you must select **Manage > People > Capabilities**. You cannot administer this capability from the **Administration console**.

The secured function associated with the External Content capability is **Watson Studio**. It allows the assignee to create assets in the Cognos Analytics content store that reference external Watson Studio Notebooks.

## **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.

**Note:** To administer this capability, you must select **Manage > People > Capabilities**. You cannot administer this capability from the **Administration console**.

## 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.

**Note:** To administer this capability, you must select **Manage > People > Capabilities**. You cannot administer this capability from the **Administration console**.

## 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.

- **Create/Delete**

Users can create new reports, use the Save as option for new reports and report views, and change models.

- **Edit Burst Definition**

Users can author burst reports.

- **Edit HTML Items**

Users can edit the HTMLItem button and hyperlink elements of the report specification when authoring reports.

- **Edit User Defined SQL**

Users can edit the SQL statements directly in the query specification.

**Tip:** Restrictions on who can use this feature are not enforced in Framework Manager. For example, a Framework Manager user who does not have **Edit User Defined SQL** rights in **IBM Cognos Administration** can still create a query subject.

- **Generate Burst Output**

Users can run burst reports.

- **Run HTML Items**

Users can use the HTMLItem button and hyperlink elements of the report specification when authoring reports.

- **Run User Defined SQL**

Users can run the query specifications that contain 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 **Run User Defined SQL** rights in **IBM Cognos Administration** can still run manually created SQL queries to search a database.

## Save to Cloud

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

Users who are assigned this capability can share a pin board that they created using Cognos Analytics for Mobile.

**Note:** To administer this capability, you must select **Manage > People > Capabilities**. You cannot administer this capability from the **Administration console**.

## 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 with Watson 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.

## View Generated Query Text

This capability allows users to view SQL or MDX query information about Cognos Analytics assets. By default, all users can view this query text. However, the administrator can remove this capability either [for all assets](#) or [for an individual asset](#).

## Visualization Alerts

Users who are assigned this capability can create an alert for a pin board in Cognos Analytics for Mobile.

**Note:** To administer this capability, you must select **Manage > People > Capabilities**. You cannot administer this capability from the **Administration console**.

## 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.

**Note:** The secured features associated with this capability are **Edit Data Module Defined SQL** and **Use Data Module Defined SQL**. However, these two capabilities are not active yet. Please do not use them.

## Setting access to user capabilities

You set access to the capabilities, also known as secured functions and features, by granting execute and traverse permissions for them to specified users, groups, or roles.

For example, to grant access to IBM Cognos Analytics with Watson - Reporting and all its functionality, you grant execute permissions for the **Reporting** secured function. If you want to grant access only to the **Create/Delete** secured feature within Reporting, grant traverse permissions for the **Reporting** secured function and execute permissions for the **Create/Delete** secured feature.

**Note:** A user must have execute and traverse permissions on a capability, or any of its sub-capabilities, for it to appear in the Personal menu  under **Profile and settings > Profile > My Capabilities > View details**.

## Before you begin

You must have set policy permissions to administer secured functions and features. Typically, this task is done by directory administrators.

Before you start setting permissions on capabilities, ensure that the initial security settings are already specified.

## Procedure

1. In **Manage**, click **People > Capabilities**.

A list of available secured functions appears. Some of the secured functions contain secured features that you access by expanding the secured function.

2. For the secured function or secured feature that you want to modify, click the context menu icon , and then click **Properties** or **Customize access**.

- On the **Access** tab, add the users, groups, or roles that need this capability, and specify permissions for them.

For secured features, turn on the **Override parent access** option. Only then you can continue with the rest of the steps.

- To add new users, groups, or roles to the capability, click the **Add member** icon , and select a namespace. Use one of the following methods to add entries:
  - In the selected namespace, click the users, groups, or roles that you want to add. To add multiple entries at once, use **Ctrl-click**. Click **Add** for the entries to be added to the capability.
  - To search for entries within the selected namespace, type text in the  **Find** field.

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, or click the **Type** icon  to filter either users, groups, or roles from the list of entries.

- For the new users, groups, or roles in the list, select the **Access** permission.

This permission includes the **Execute** and **Traverse** granular permissions. Alternatively, you can select the **Custom** permission, and choose the required combination of granular permissions.

**Important:**

The **Execute** permission is always necessary when setting access to capabilities. The **Traverse** permission is not always required. Any other permissions depend on the user role.

- To remove a user, group, or role from the list, click the **Remove member** icon .
- To apply your changes, click anywhere on the **Access** tab. The newly added users, groups, or roles, with the permissions that you specified for them, appear on this tab.

## Initial access permissions for capabilities

In IBM Cognos Analytics with Watson, 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 user capabilities”](#) on page 158.

### 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 [“Access permissions for an entry”](#) on page 139.

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	<b>Execute</b> and <b>Traverse</b>
Assign	<b>Traverse</b> and <b>Set Policy</b>
Manage	<b>Execute</b> , <b>Traverse</b> , and <b>Set Policy</b>
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 15. 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	<u>Assign</u>				✓	✓

### Administration capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 16. Administration capability and permissions for related groups and roles*

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	<u>Manage</u>			✓	✓	✓
Library Administrators	<u>Access</u>			✓		✓
Mobile Administrators	<u>Access</u>			✓		✓
Modelers	<u>Access</u>			✓		✓
Portal Administrators	<u>Access</u>			✓		✓
PowerPlay Administrators	<u>Access</u>			✓		✓
Report Administrators	<u>Access</u>			✓		✓
Server Administrators	<u>Access</u>			✓		✓

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 17. 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	Directory Administrators	<u>Assign</u>				✓	✓
Administration tasks	Server Administrators	<u>Access</u>			✓		✓
	Report Administrators	<u>Access</u>			✓		✓
	Directory Administrators	<u>Assign</u>				✓	✓
	PowerPlay Administrators	<u>Access</u>			✓		✓
Collaboration Administration	Directory Administrators	<u>Manage</u>			✓	✓	✓
Configure and manage the system	Server Administrators	<u>Access</u>			✓		✓
	Directory Administrators	<u>Assign</u>				✓	✓
Controller Administration	Directory Administrators	<u>Assign</u>				✓	✓
Data Sources Connections	Directory Administrators	<u>Manage</u>			✓	✓	✓
	Modelers	<u>Access</u>			✓		✓
Distribution Lists and Contacts	Directory Administrators	<u>Manage</u>			✓	✓	✓
Manage Visualizations	Directory Administrators	<u>Assign</u>				✓	✓
	Library Administrators	<u>Access</u>			✓		✓
Metric Studio Administration	Directory Administrators	<u>Assign</u>				✓	✓
Mobile Administration	Directory Administrators	<u>Assign</u>				✓	✓
	Mobile Administrators	<u>Access</u>			✓		✓

Table 17. 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
Planning Administration	Directory Administrators	<u>Assign</u>				✓	✓
PowerPlay Servers	Directory Administrators	<u>Assign</u>				✓	✓
	PowerPlay Administrators	<u>Access</u>			✓		✓
Printers	Directory Administrators	<u>Manage</u>			✓	✓	✓
Query Service Administration	Directory Administrators	<u>Assign</u>				✓	✓
	Server Administrators	<u>Access</u>			✓		✓
Run activities and schedules	Report Administrators	<u>Access</u>			✓		✓
	Directory Administrators	<u>Assign</u>				✓	✓
	PowerPlay Administrators	<u>Access</u>			✓		✓
Set capabilities and manage UI profiles	Directory Administrators	<u>Manage</u>			✓	✓	✓
Styles and portlets	Portal Administrators	<u>Access</u>			✓		✓
	Directory Administrators	<u>Manage</u>			✓	✓	✓
	Library Administrators	<u>Access</u>			✓		✓
Users, Groups, and Roles	Directory Administrators	<u>Manage</u>			✓	✓	✓

## AI capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 18. AI capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	<u>Assign</u>				✓	✓

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 19. 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	Directory Administrators	<u>Assign</u>				✓	✓
Use Assistant	Analytics Explorers	<u>Access</u>			✓		✓
	Analytics Users	<u>Access</u>			✓		✓
	Directory Administrators	<u>Assign</u>				✓	✓
	Mobile Analytics Users	<u>Access</u>			✓		✓

## Analysis Studio capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 20. 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	<u>Access</u>			✓		✓
Authors	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓
Modelers	<u>Access</u>			✓		✓
Report Administrators	<u>Access</u>			✓		✓

## Attach outputs capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 21. 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	<a href="#">Access</a>			✓		✓
Analytics Users	<a href="#">Access</a>			✓		✓
Directory Administrators	<a href="#">Assign</a>				✓	✓
Report Administrators	<a href="#">Access</a>			✓		✓

## Cognos Analytics for Mobile capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 22. 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	<a href="#">Access</a>			✓		✓
Analytics Users	<a href="#">Access</a>			✓		✓
Analytics Viewers	<a href="#">Access</a>			✓		✓
Directory Administrators	<a href="#">Assign</a>				✓	✓
Mobile Analytics Users	<a href="#">Access</a>			✓		✓
Report Administrators	<a href="#">Access</a>			✓		✓

## Cognos Insight capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 23. 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	<u>Assign</u>				✓	✓

### Cognos Viewer capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 24. 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	<u>Access</u>			✓		✓
Authors	<u>Access</u>			✓		✓
Consumers	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓
Analytics Viewers	<u>Access</u>			✓		✓
Modelers	<u>Access</u>			✓		✓
PowerPlay Administrators	<u>Access</u>			✓		✓
PowerPlay Users	<u>Access</u>			✓		✓
Query Users	<u>Access</u>			✓		✓
Readers	<u>Access</u>			✓		✓
Report Administrators	<u>Access</u>			✓		✓

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 25. 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	<u>Access</u>			✓		✓
	Authors	<u>Access</u>			✓		✓
	Consumers	<u>Access</u>			✓		✓
	Query Users	<u>Access</u>			✓		✓
	Analysis Users	<u>Access</u>			✓		✓
	Readers	<u>Access</u>			✓		✓
	Directory Administrators	<u>Assign</u>				✓	✓
	Analytics Viewers	<u>Access</u>			✓		✓
	Modelers	<u>Access</u>			✓		✓
	PowerPlay Administrators	<u>Access</u>			✓		✓
	PowerPlay Users	<u>Access</u>			✓		✓
Run With Options	Report Administrators	<u>Access</u>			✓		✓
	Authors	<u>Access</u>			✓		✓
	Consumers	<u>Access</u>			✓		✓
	Query Users	<u>Access</u>			✓		✓
	Analysis Users	<u>Access</u>			✓		✓
	Directory Administrators	<u>Assign</u>				✓	✓
	Modelers	<u>Access</u>			✓		✓
	PowerPlay Administrators	<u>Access</u>			✓		✓
	PowerPlay Users	<u>Access</u>			✓		✓

## Collaborate capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 26. Collaborate capability and permissions for related groups and roles*

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analysis Users	<u>Access</u>			✓		✓
Authors	<u>Access</u>			✓		✓
Consumers	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓
Modelers	<u>Access</u>			✓		✓
PowerPlay Administrators	<u>Access</u>			✓		✓
PowerPlay Users	<u>Access</u>			✓		✓
Query Users	<u>Access</u>			✓		✓
Report Administrators	<u>Access</u>			✓		✓

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 27. 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	<a href="#">Access</a>			✓		✓
	Authors	<a href="#">Access</a>			✓		✓
	Consumers	<a href="#">Access</a>			✓		✓
	Directory Administrators	<a href="#">Assign</a>				✓	✓
	Modelers	<a href="#">Access</a>			✓		✓
	PowerPlay Administrators	<a href="#">Access</a>			✓		✓
	PowerPlay Users	<a href="#">Access</a>			✓		✓
	Query Users	<a href="#">Access</a>			✓		✓
	Report Administrators	<a href="#">Access</a>			✓		✓

### Controller Studio capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 28. 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	<a href="#">Assign</a>				✓	✓

### Dashboard capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 29. Dashboard capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Explorers	<a href="#">Access</a>			✓		✓

Table 29. Dashboard capability and permissions for related groups and roles (continued)

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Users	<u>Access</u>			✓		✓
Analytics Viewers	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓

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 30. 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	<u>Access</u>			✓		✓
	Analytics Users	<u>Access</u>			✓		✓
	Directory Administrators	<u>Assign</u>				✓	✓

### Data Manager capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 31. 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	<u>Assign</u>				✓	✓

### Data sets capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 32. 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	<u>Assign</u>				✓	✓
Everyone	<u>Access</u>			✓		✓

### Desktop Tools capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 33. 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	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓

### Detailed Errors capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 34. 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	<u>Assign</u>				✓	✓

### Develop Visualizations capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 35. 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	<u>Access</u>			✓		✓
Analytics Users	<u>Access</u>			✓		✓

Table 35. Develop Visualizations capability and permissions for related groups and roles (continued)

Group or role	Permission level	Permission type				
		Read 	Write 	Execute 	Set policy 	Traverse 
Directory Administrators	<u>Assign</u>				✓	✓

### 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 36. 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	<u>Assign</u>				✓	✓

### 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 37. Email capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Explorers	<u>Access</u>			✓		✓
Analytics Users	<u>Access</u>			✓		✓
Analytics Viewer	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓

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 38. 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	<u>Access</u>			✓		✓
	Analytics Users	<u>Access</u>			✓		✓
	Directory Administrators	<u>Assign</u>				✓	✓
Include link in email	Analytics Explorers	<u>Access</u>			✓		✓
	Analytics Users	<u>Access</u>			✓		✓
	Analytics Viewer	<u>Access</u>			✓		✓
Share using email	Directory Administrators	<u>Assign</u>				✓	✓
	Analytics Explorers	<u>Access</u>			✓		✓
	Analytics Users	<u>Access</u>			✓		✓
Type in external email	Analytics Viewer	<u>Access</u>			✓		✓
	Directory Administrators	<u>Assign</u>				✓	✓
	Analytics Explorers	<u>Access</u>			✓		✓
	Analytics Users	<u>Access</u>			✓		✓
	Analytics Viewer	<u>Access</u>			✓		✓
	Directory Administrators	<u>Assign</u>				✓	✓

### Event Studio capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 39. Event Studio capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Authors	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓
Modelers	<u>Access</u>			✓		✓
Report Administrators	<u>Access</u>			✓		✓

### 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 40. 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	<u>Access</u>			✓		✓
Authors						
Consumers						
Analytics Viewers						
Modelers						
PowerPlay Administrators						
PowerPlay Users						
Query Users						
Readers						
Report Administrators						
Directory Administrators		<u>Assign</u>				✓

### Executive Dashboard capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 41. 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	<u>Access</u>			✓		✓
Authors	<u>Access</u>			✓		✓
Consumers	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓
Analytics Viewers	<u>Custom</u>			Permission Denied		Permission Denied
Modelers	<u>Access</u>			✓		✓
PowerPlay Administrators	<u>Access</u>			✓		✓
PowerPlay Users	<u>Access</u>			✓		✓
Query Users	<u>Access</u>			✓		✓
Readers	<u>Access</u>			✓		✓
Report Administrators	<u>Access</u>			✓		✓

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 42. 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	<a href="#">Access</a>			✓		✓
	Directory Administrators	<a href="#">Assign</a>				✓	✓
	Analytics Viewers	<a href="#">Custom</a>					
	Modelers	<a href="#">Access</a>					
	Query Users	<a href="#">Access</a>			✓		✓
	Report Administrators	<a href="#">Access</a>			✓		✓

### Exploration capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 43. Exploration capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Explorers	<a href="#">Access</a>			✓		✓
Directory Administrators	<a href="#">Assign</a>				✓	✓
Analytics Viewers	<a href="#">Custom</a>			Permission denied		Permission denied

### External Content capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 44. External Content capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	<a href="#">Manage</a>			✓	✓	✓

The secured feature in the following table is a child of the External Content capability.

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 45. Secured feature of the External Content capability and permissions for related groups and roles*

Secured feature	Group or role	Permission level	Permission type				
			Read	Write	Execute	Set policy	Traverse
Watson Studio	Directory Administrators	<u>Manage</u>			✓	✓	✓

## External Repositories capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 46. 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	<u>Assign</u>				✓	✓
Everyone	<u>Access</u>			✓		✓

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 47. 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	<u>Assign</u>				✓	✓
View external documents	Directory Administrators	<u>Assign</u>				✓	✓
	Everyone	<u>Access</u>			✓		✓

## Generate CSV Output

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 48. 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	<a href="#">Assign</a>				✓	✓
Everyone	<a href="#">Access</a>			✓		✓

### 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 49. 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	<a href="#">Assign</a>				✓	✓
Everyone	<a href="#">Access</a>			✓		✓

### 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 50. 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	<a href="#">Assign</a>				✓	✓
Everyone	<a href="#">Access</a>			✓		✓

### 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 51. 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	<a href="#">Assign</a>				✓	✓

Table 51. Generate XML Output capability and permissions for related groups and roles (continued)

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Everyone	<a href="#">Access</a>			✓		✓

## Glossary capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 52. Glossary capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Everyone	<a href="#">Access</a>			✓		✓
Directory Administrators	<a href="#">Assign</a>				✓	✓

## Hide Entries capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 53. Hide Entries capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Everyone	<a href="#">Access</a>			✓		✓
Directory Administrators	<a href="#">Assign</a>				✓	✓

## 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 54. 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	<a href="#">Assign</a>				✓	✓
Report Administrators	<a href="#">Access</a>			✓		✓

## Job capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 55. Job capability and permissions for related groups and roles*

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analytics Explorers	<u>Access</u>			✓		✓
Analytics Users	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓
Report Administrators	<u>Access</u>			✓		✓

## Lineage capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 56. Lineage capability and permissions for related groups and roles*

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Everyone	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓

## Manage content capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 57. 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	<u>Access</u>			✓		✓
Directory Administrators	<u>Manage</u>			✓	✓	✓

### 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 58. 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	<u>Assign</u>				✓	✓

### Metric Studio capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 59. 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	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓

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 60. 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	<u>Access</u>			✓		✓
	Directory Administrators	<u>Assign</u>				✓	✓

### Mobile capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 61. 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	<u>Assign</u>				✓	✓
Analytics Viewers	<u>Access</u>			✓		✓
Mobile Administrators	<u>Access</u>			✓		✓
Mobile Users	<u>Access</u>			✓		✓

### Notebook capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 62. Notebook capability and permissions for related groups and roles*

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Directory Administrators	<u>Assign</u>				✓	✓

### Planning Contributor capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 63. 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	<u>Assign</u>				✓	✓

### PowerPlay Studio capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 64. PowerPlay Studio capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Authors	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓
Modelers	<u>Access</u>			✓		✓
PowerPlay Administrators	<u>Access</u>			✓		✓
PowerPlay Users	<u>Access</u>			✓		✓

### Query Studio capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 65. Query Studio capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Authors	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓
Modelers	<u>Access</u>			✓		✓
Query Users	<u>Access</u>			✓		✓
Report Administrators	<u>Access</u>			✓		✓

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 66. 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	<a href="#">Access</a>			✓		✓
	Modelers	<a href="#">Access</a>			✓		✓
	Query Users	<a href="#">Access</a>			✓		✓
	Report Administrators	<a href="#">Access</a>			✓		✓
	Directory Administrators	<a href="#">Assign</a>				✓	✓

## Report Studio capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 67. Reporting capability and permissions for related groups and roles*

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Authors	<a href="#">Access</a>			✓		✓
Directory Administrators	<a href="#">Assign</a>				✓	✓
Library Administrators	<a href="#">Access</a>			✓		✓
Modelers	<a href="#">Access</a>			✓		✓
Report Administrators	<a href="#">Access</a>			✓		✓

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 68. 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
Create/Delete	Authors	<u>Access</u>			✓		✓
Edit Burst Definition	Library Administrators	<u>Access</u>			✓		✓
Edit HTML Items	Modelers	<u>Access</u>			✓		✓
Edit User Defined SQL	Report Administrators	<u>Access</u>			✓		✓
Generate Burst Output	Directory Administrators	<u>Assign</u>				✓	✓
Run HTML Items							
Run User Defined SQL							
Allow External Data	Directory Administrators	<u>Assign</u>				✓	✓
	Library Administrators	<u>Access</u>			✓		✓

### 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 69. 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	<u>Access</u>			✓		✓
Analytics Users	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓
Report Administrators	<u>Access</u>			✓		✓

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 70. 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	<u>Assign</u>				✓	✓
	Report Administrators	<u>Access</u>			✓		✓

## Scheduling capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 71. Scheduling capability and permissions for related groups and roles

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Analysis Users	<u>Access</u>			✓		✓
Authors	<u>Access</u>			✓		✓
Consumers	<u>Custom</u>					✓
Directory Administrators	<u>Assign</u>				✓	✓
Modelers	<u>Access</u>			✓		✓
PowerPlay Administrators	<u>Access</u>			✓		✓
PowerPlay Users	<u>Access</u>			✓		✓
Query Users	<u>Access</u>			✓		✓
Report Administrators	<u>Access</u>			✓		✓

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 72. 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	<u>Access</u>			✓		✓	
	Authors	<u>Access</u>			✓		✓	
	Consumers	<u>Custom</u> (Except for Schedule by day, where permission level = <u>Access</u> )					✓	
	Directory Administrators	<u>Assign</u>				✓	✓	
	Modelers	<u>Access</u>			✓		✓	
	Query Users	<u>Access</u>			✓		✓	
	Report Administrators	<u>Access</u>			✓		✓	
	PowerPlay Administrators	<u>Access</u>			✓		✓	
	PowerPlay Users	<u>Access</u>			✓		✓	
	Scheduling Priority	Report Administrators	<u>Access</u>			✓		✓
		Directory Administrators	<u>Assign</u>				✓	✓
		PowerPlay Administrators	<u>Access</u>			✓		✓

### 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 73. 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	<u>Manage</u>			✓	✓	✓

## 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 74. 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	<u>Assign</u>				✓	✓

## Share Pin Board capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 75. 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	<u>Access</u>			✓		✓
Analytics Users	<u>Access</u>			✓		✓
Directory Administrators	<u>Assign</u>				✓	✓
Report Administrators	<u>Access</u>			✓		✓

## Snapshots capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 76. 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	<u>Assign</u>				✓	✓
Everyone	<u>Access</u>			✓		✓
Modelers	<u>Access</u>			✓		✓

## Specification Execution capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 77. 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	<a href="#">Assign</a>				✓	✓

## Upload files capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 78. Upload files capability and permissions for related groups and roles*

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Everyone	<a href="#">Access</a>			✓		✓
Directory Administrators	<a href="#">Assign</a>				✓	✓
Analytics Viewers	<a href="#">Custom</a>			Permission denied		Permission denied
Modelers	<a href="#">Access</a>			✓		✓

## View Generated Query Text capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

*Table 79. View Generated Query Text capability and permissions for related groups and roles*

Group or role	Permission level	Permission type				
		Read	Write	Execute	Set policy	Traverse
Everyone	<a href="#">Access</a>			✓		✓
Directory Administrators	<a href="#">Assign</a>				✓	✓

## Visualization Alerts capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 80. 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	<a href="#">Access</a>			✓		✓
Analytics Users	<a href="#">Access</a>			✓		✓
Directory Administrators	<a href="#">Assign</a>				✓	✓
Mobile Analytics Users	<a href="#">Access</a>			✓		✓
Report Administrators	<a href="#">Access</a>			✓		✓

### Watch Rules capability

In the following table, a checkmark (✓) indicates that a permission is granted to a group or role for an object.

Table 81. 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	<a href="#">Access</a>			✓		✓
Authors	<a href="#">Access</a>			✓		✓
Consumers	<a href="#">Access</a>			✓		✓
Directory Administrators	<a href="#">Assign</a>				✓	✓
Modelers	<a href="#">Access</a>			✓		✓
PowerPlay Administrators	<a href="#">Access</a>			✓		✓
PowerPlay Users	<a href="#">Access</a>			✓		✓
Query Users	<a href="#">Access</a>			✓		✓
Report Administrators	<a href="#">Access</a>			✓		✓

### 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 82. 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	<a href="#">Assign</a>				✓	✓
Analytics Viewers	<a href="#">Custom</a>			Permission denied		Permission denied
Everyone	<a href="#">Access</a>			✓		✓
Modelers	<a href="#">Access</a>			✓		✓

## Removing capabilities from users

You can specify that certain groups, roles, or individual users are denied access to a user capability.

For example, you want to prevent every member of the **Consumers** group in the Cognos namespace from being able to view the SQL or MDX code of all metadata assets and any asset created from them. Follow the steps below, selecting the **View Generated Query Text** capability in step “2” on page 190.

### Procedure

1. From **Manage > People**, click **Capabilities**.

A list of available capabilities appears.

2. Find the capability that you want to deny from selected users, click the context menu icon , and then click **Customize access**.

3. Click the Add member icon  and add a group, role or individual member from whom you want to deny the capability.

4. In the **Permissions** box for the entry you added, select **Custom**.

The **Permissions** panel appears.

5. Select the **Deny** check box next to **Execute**.

## Object capabilities

Object capabilities specify the secured functions and features that users, groups, or roles can use with specific data modules, packages, data sets, and uploaded files. 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 user capabilities, control access to the different components and functionality in IBM Cognos software. For object capabilities to work, you must combine them with applicable user 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 the previously specified object capabilities.

Control access to object capabilities with the **Set Entry-Specific Capabilities** secured function. For more information, see “User capabilities” on page 148.

**Note:** The data module object capabilities are not applied with the option **Try this data module in Reporting** when editing the data module.

The following sections describe the object capabilities that you can specify for individual data modules, packages, data sets, and uploaded files or folders that contain these objects.

## 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.

## 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.

**Note:** To administer this capability and its secured functions, you must select **Manage > People > Capabilities**. You cannot administer this capability from the **Administration console**.

The following secured features are associated with this function:

- **Learning**

This secured feature allows the system to learn from an assignee's product usage.

**Tip:** This feature is not available as an object capability.

- **Use Assistant**

This secured feature allows designated users to use the Assistant. The **Use Assistant** capability can be set at the user level or source level.

## 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.

## 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 168](#) section.

The following secured feature is associated with this function:

- **Create/Edit**

This secured function controls access to the **New > Dashboard** and **New > Story** functions. Users require Execute permissions for the Dashboard and Create/Edit capability to both create or edit dashboards and stories.

## Data sets

This secured function controls access to the **Create data set** menu that is available from the package and data module context menus.

## Event Studio

This secured function controls access to Event Studio.

## 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* section.

## Desktop Tools

This secured function controls tracking for Cognos Desktop Tools products. Users with this capability are members of the Analytics Explorers role. This allows an admin to track the users in the license counter. Products that will count as a desktop tool include Planning Analytics For Microsoft Excel, Cognos Framework Manager, Cognos Cube Designer and Dynamic Query Analyzer, Transformer, and TM1 Writeback to bundled FLBI TM1 server.

## Glossary

This secured function controls access to the IBM InfoSphere Business Glossary.

## 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.

## 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.

- **Create/Delete**

Users can create new reports, use the Save as option for new reports and report views, and change models.

- **Edit Burst Definition**

Users can author burst reports.

- **Edit HTML Items**

Users can edit the HTMLItem button and hyperlink elements of the report specification when authoring reports.

- **Edit User Defined SQL**

Users can edit the SQL statements directly in the query specification.

**Tip:** Restrictions on who can use this feature are not enforced in Framework Manager. For example, a Framework Manager user who does not have **Edit User Defined SQL** rights in **IBM Cognos Administration** can still create a query subject.

- **Generate Burst Output**

Users can run burst reports.

- **Run HTML Items**

Users can use the HTMLItem button and hyperlink elements of the report specification when authoring reports.

- **Run User Defined SQL**

Users can run the query specifications that contain 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 **Run User Defined SQL** rights in **IBM Cognos Administration** can still run manually created SQL queries to search a database.

## 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 with Watson 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*.

## View Generated Query Text

This capability allows users to view SQL or MDX query information about Cognos Analytics assets. By default, all users can view this query text. However, the administrator can remove this capability either [for all assets](#) or [for an individual asset](#).

## 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.

**Note:** The secured features associated with this capability are **Edit Data Module Defined SQL** and **Use Data Module Defined SQL**. However, these two capabilities are not active yet. Please do not use them.

## Setting access to object capabilities

Use this functionality to specify the secured functions and features that users, groups, or roles can use with specific data modules, packages, data sets, and uploaded files.

You can specify object capabilities directly for data modules, packages, data sets, and uploaded files, or if these objects are stored in a folder, for the folder. Capabilities that are specified at the folder level apply only to data modules, packages, data sets, and uploaded files in that folder and its subfolders. For example, if a folder contains data modules, packages, reports, dashboards, and a subfolder that contains other packages and reports, only the data modules and packages in the folder and subfolder are affected by the capabilities.

The following capabilities must be applied globally; they cannot be applied at the folder level.

- **Generate CSV Output**
- **Generate PDF Output**
- **Generate XLS Output**
- **Generate XML Output**

### Before you begin

To set object capabilities, users must have access for the secured function **Set Entry-Specific Capabilities**. For more information, see [“User capabilities” on page 148](#). The users must also have set policy permissions for the data module, package, data set, and uploaded file, or own these objects. For more information, see [“Access permissions for an entry” on page 139](#).

When setting object capabilities for the first time after installing Cognos Analytics, start with the **Team content** capabilities, which should mirror the global capabilities. This provides an accurate baseline on which object capabilities can be further refined.

### Procedure

1. In **Team content** (or any other folder in the **Content** page), open the data module, package, data set, uploaded file, or folder properties page.
2. Click the **Capabilities** tab, and then click **Set capabilities**.
3. For the user, group, or role for which you want to specify object capabilities, select the checkbox **Override parent 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**.
4. In the **Grant** and **Deny** column, select or clear the applicable checkboxes 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.
5. If applicable, select the **Override child capabilities** checkbox.  
  
Use this option to specify object capabilities for a hierarchy of entries, for example, for all packages in a folder.
6. Click **Save**.

## Denying capabilities on an object

You can select an individual asset in Team content for which capabilities are denied from a specified user, group or role.

For example, you want to prevent every member of the **Consumers** group in the Cognos namespace from being able to view the SQL code of the package **Team content > FM packages > GO Sales**. Follow the steps below, selecting the **View Generated Query Text** capability in step “6” on page 195.

### Procedure

1. In **Team content**, open the data module, package, data set, uploaded file, or folder **Properties** page.
2. Click the **Capabilities** tab, and then click **Set capabilities**.
3. Select the checkbox **Override parent capabilities**.
4. If the user, group, or role from whom you want to deny the capability is not in the list, click **Add** and add it as a member.
5. In the left pane, select the check box of the member you added.
6. In the **Deny** column, select the check box of the capability that you want to deny from the users, groups, or roles you specified.
7. Click **Save**.

## Managing user licenses

---

Different levels of Cognos Analytics functionality correspond to specific types of user licenses, referred to as license roles. Each role entitles someone to use a unique set of capabilities. Your offering agreement specifies the maximum number of users who are entitled to use the product in each license role.

**Note:** The usage of each license role is calculated by Cognos Analytics, based on the capabilities of each user when they last logged in. Administrators do *not* assign licenses to users directly. Instead, they assign *capabilities* to users that correspond to their designated license role.

As administrator, you must ensure that the number of people with the capabilities defined for each license role does not exceed the number in your offering agreement. Therefore, you must:

- understand the requirements for the maximum number of users for each license role
- assign capabilities to users such that the number of users that can perform each license role does not exceed the defined maximum
- validate, periodically, the list of users for each license role
- track the actual license usage

**Important:** License usage information in IBM Cognos Analytics with Watson calculates the effective licenses that were used by individual users with their last login. Users' changed capabilities are not reflected in their licence usage until the users log in again. Also, for existing customers the license usage information is incomplete until all users log in again.

A license usage report is generated when the licenses page in **Manage > Licenses** is opened for the first time, when the **Refresh** button is clicked, or after a product restart.

The basic report contains information about license usage by user. Some customers might want to do additional reporting, for example, on license usage by tenant.

IBM Cognos Analytics with Watson has a few types of licensed roles, each of them associated with different capabilities. Refer to [this article](https://www.ibm.com/support/docview.wss?uid=ibm10735275) (https://www.ibm.com/support/docview.wss?uid=ibm10735275) to view the capabilities and permissions matrix that the IBM Cognos Analytics with Watson license model is based on.

**Note:** Cognos Analytics Processor Value Units (PVUs) are licensed according to the dispatcher service. Each license must be associated with a unique dispatcher service. This association allows IBM License Metric Tool (ILMT) to accurately calculate the PVU value for each Cognos Analytics client license. For more information, see [License Metric Tool - Getting started](#).

## Procedure

1. To access the licenses page in IBM Cognos Analytics with Watson, click **Manage > Licenses**.
2. To enter the number of owned licenses, click the **Owned** field for the licensed role, type the number, and click **Apply** to save the value.

This value is used for information purposes only and is not included in the license usage report.

3. Assign to users the capabilities that correspond with the license role you want them to have.

**Important:** Ensure that the number of users that can perform each license role does not exceed the defined maximum.

For more information, see [“Default permissions based on license roles”](#) on page 197.

4. Validate, periodically, the list of users for each license role.
  - a) Run a content maintenance task to ensure that users who are no longer with your company are removed from the Cognos Analytics content store.

For more information, see "Content Store Maintenance on External Namespaces." in the *IBM Cognos Analytics with Watson Administration and Security Guide*.

- b) For each license role, click the chevron  and review the list of users who last logged in with assigned capabilities associated with that license role.

For each user, follow these steps:

- i) Check the timestamp of their last login. If they are an infrequent user, confirm whether they still require a Cognos Analytics license.
- ii) Confirm that they are associated with the license role that you intended.

If they are associated with the wrong license role, modify the user's capabilities to correspond with their intended license role.

- iii) If the user should no longer have a license, remove their user profile.

**Tip:** Searching for a user in a namespace that has a large number of users can take time. Don't forget to use these methods to speed up your search.

- c) Click **Refresh** to refresh the used license information.
5. To generate the license usage report, click **Refresh**.

You can generate the report as often as you want.

**Remember:** The usage report provides license information on users according to their last login.

6. To view the license information for a specific role, click the right chevron icon .

This information is a subset of information from the full report.

7. To view the full report, click **Export** to save the information to a CSV file, and open the file.

**Tip:** In the exported file, the values in **Level** column correspond to specific license roles, as follows:

Level	License role
4	Analytics Administrator
3	Analytics Explorer
2	Analytics User
1	Analytics Viewer
0	Analytics for Mobile User
-1	The license role is unknown because the user has not logged in yet.

## What to do next

For more information, see the following topics:

- [Predefined license roles](#)
- [Assigning capabilities based on license roles](#)
- [Upgrade scenario: If your customized roles have the same names as the new license roles](#)

## 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 4](#).

The following table lists the predefined 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 <b>Manage</b> menu, including IBM Cognos Administration.
Analytics Explorer	Members have the same access permissions as Analytics Users. They can also access 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, upload files, and view generated SQL or MDX query text. 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.
Analytics for Mobile User	Members can use the Cognos Analytics for Mobile app to create and consume pin boards, receive alerts, use the Assistant, browse content, and open dashboards or explorations. They can also scan a QR code from the desktop to authenticate into the app.

## Default permissions based on license roles

In IBM Cognos Analytics with Watson, 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 role 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 206](#).

The following table maps the capabilities that are granted for each license role. 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 84. Cognos Analytics 11.2 capabilities by license roles*

Capability	Secured feature	Analytics for Mobile User	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrator	Comments
Adaptive Analytics			✓	✓	✓	✓	Not Applicable
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

Table 84. Cognos Analytics 11.2 capabilities by license roles (continued)

Capability	Secured feature	Analytics for Mobile User	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrator	Comments
	Mobile Administration					✓	
	Planning Administration					✓	You need a separate IBM Planning Contributor Licence
	PowerPlay Servers					✓	You need a separate PowerPlay license
	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				✓	✓	✓	

Table 84. Cognos Analytics 11.2 capabilities by license roles (continued)

Capability	Secured feature	Analytics for Mobile User	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrator	Comments
Attach Outputs				✓	✓	✓	
Cognos Analytics for Mobile		✓	✓	✓	✓	✓	
Cognos Insight				✓	✓	✓	Not Applicable
Cognos Viewer			✓	✓	✓	✓	
	Context Menu		✓	✓	✓	✓	
	Run with Options			✓	✓	✓	
	Selection		✓	✓	✓	✓	
	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		✓	✓	✓	✓	✓	

Table 84. Cognos Analytics 11.2 capabilities by license roles (continued)

Capability	Secured feature	Analytics for Mobile User	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrator	Comments
	Create/Edit			✓	✓	✓	
Data Manager			✓	✓	✓	✓	Not Applicable
Data sets				✓	✓	✓	
Desktop Tools					✓	✓	
Detailed Errors			✓	✓	✓	✓	
Develop Visualizations				✓	✓	✓	
Drill Through Assistant				✓	✓	✓	
Email			✓	✓	✓	✓	
	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			✓	✓	✓	

Table 84. Cognos Analytics 11.2 capabilities by license roles (continued)

Capability	Secured feature	Analytics for Mobile User	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrator	Comments
	Use Interactive Dashboard Features			✓	✓	✓	
Exploration				✓	✓	✓	
External Content				✓	✓	✓	
	Watson Studio			✓	✓	✓	
External Repositories			✓	✓	✓	✓	
	Manage Repository Connections			✓	✓	✓	
	View External Documents		✓	✓	✓	✓	
Generate CSV Output				✓	✓	✓	
Generate PDF Output				✓	✓	✓	
Generate XLS Output				✓	✓	✓	
Generate XML Output				✓	✓	✓	
Glossary			✓	✓	✓	✓	Integration with IBM InfoSphere Business glossary. Can use directly from Viewer
Hide Entries			✓	✓	✓	✓	

Table 84. Cognos Analytics 11.2 capabilities by license roles (continued)

Capability	Secured feature	Analytics for Mobile User	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrator	Comments
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
Planning Contributor			✓	✓	✓	✓	You need separate entitlement of IBM Planning Contributor

Table 84. Cognos Analytics 11.2 capabilities by license roles (continued)

Capability	Secured feature	Analytics for Mobile User	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrator	Comments
PowerPlay Studio				✓	✓	✓	You need a separate PowerPlay license
Query Studio				✓	✓	✓	
	Advanced			✓	✓	✓	
	Create			✓	✓	✓	
Report Studio				✓	✓	✓	
	Allow External Data			✓	✓	✓	
	Create/Delete			✓	✓	✓	
	Edit Burst Definition			✓	✓	✓	
	Edit HTML Items			✓	✓	✓	
	Edit User Defined SQL			✓	✓	✓	
	Generate Burst Output			✓	✓	✓	
	Run HTML Items			✓	✓	✓	
	Run User Defined SQL			✓	✓	✓	
Save to Cloud				✓	✓	✓	
	Manage Connections					✓	
Scheduling				✓	✓	✓	

Table 84. Cognos Analytics 11.2 capabilities by license roles (continued)

Capability	Secured feature	Analytics for Mobile User	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrator	Comments
	Schedule by Day			✓	✓	✓	
	Schedule by Hour			✓	✓	✓	
	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				✓	✓	✓	
Share Pin Board				✓	✓	✓	
Snapshots				✓	✓	✓	
Specification Execution						✓	
Upload files				✓	✓	✓	
View Generated Query Text				✓	✓	✓	
Visualization Alerts		✓		✓	✓	✓	
Watch Rules				✓	✓	✓	

Table 84. Cognos Analytics 11.2 capabilities by license roles (continued)

Capability	Secured feature	Analytics for Mobile User	Analytics Viewer	Analytics User	Analytics Explorer	Analytics Administrator	Comments
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](#)

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)) ([http://www-03.ibm.com/software/sla/sladb.nsf/searchlis/?searchview&searchorder=4&searchmax=0&query=\(IBM+Cognos+Analytics+11.1\)](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 license roles” on page 197](#).

#### 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 **Email Delivery Option** 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 **Attach Outputs** capability.
  - a. Click the More icon .
  - b. Click **Customize access**.
  - c. Click the Remove member icon  next to the **Everyone** group.
  - d. Click **OK**.
13. 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**.

## **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 197](#)

- 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**.



---

## Chapter 9. Customizing Cognos Analytics across all roles

The IBM Cognos Analytics with Watson user interface is built on an extensible model. In this model, the user interface screens are defined as views (such as home, authoring, dashboard, and modeler). You can customize these views for all users and roles by adding and removing user interface elements, such as buttons and menus. You can define new views to extend the Cognos Analytics user interface. You can also replace the default home page and sign-in page or substitute your own branding (colors, logos, and brand text) for the default branding on all views.

Customizations are packaged as compressed files that contain a `spec.json` file that defines the customization. The compressed file can also contain other files, depending on the type of the customization. Customizations can also be included in deployments.

You manage customizations for all users and roles with the **Manage > Customizations** slide-out panel. You use this panel to upload your customizations to the Cognos Analytics server, and to select which customizations to use.

### Note:

When you use the **Manage > Customizations** slide-out panel, your customizations are applied to all users and roles.

For example, if you upload the sample extension called

`SampleExtensionExcludeNotifications.zip`, it will remove the **Notifications** icon  from the Application Bar in the Home perspective for all users and roles. It will also remove the **Notifications** check box from the feature list when an administrator selects the properties of any role, clicks on the **Customization** tab, and navigates to **Features > Home > Application bar**.

Therefore, if your goal is to add or remove a feature for everyone in your Cognos environment, then you should use an extension. If your goal is to provide users and roles with different features, you should use individual [role customization](#), rather than an extension.

If you use role customizations to set specific features for user roles and then apply an extension that is based on those features, the extension will override all of your role customizations.

To assign home pages, features, themes, custom folders, and parameters to particular roles, use the **Manage > Accounts > Namespaces** slide-out panel. For more information, see [“Customizing roles” on page 7](#).

To assign custom themes and home pages to particular tenants, use the **Manage > Multitenacy** slide-out panel, and from the tenant properties panel, select the **Customization** tab. For more information, see [“Customizing tenants” on page 135](#).

Some types of customizations require the use of the JavaScript programming language. These customizations are described in the following topics.

- [“Creating a custom action controller” on page 229](#)
- [“Creating a view \(other than a sign-in view\)” on page 242](#)
- [“Creating a sign-in view” on page 244](#)

The other types of customizations do not require any programming knowledge.

The JSON schemas that are used to define customizations are provisional and can change in future releases of Cognos Analytics in a way that is not compatible with earlier versions.

## Customization samples

---

Customization samples are available that demonstrate how to create themes, extensions, and views. You can modify these samples to create your own customizations.

These sample files are installed with the product in an Easy Installation, and are an option in a Custom Installation. After product installation, you can find them in the *installation\_location/samples/* folder.

The customization samples are described in the following topics.

- [“Sample themes” on page 213](#)
- [“Sample extensions” on page 221](#)
- [“Sample views” on page 240](#)

### Using the samples

The customization samples illustrate how to implement commonly used customizations. You can view the sample code and modify it to create customizations for your users. To examine the contents of a customization sample, extract the .zip file. Each sample contains a `spec.json` file that contains the logic for the customization. There can also be other files or folders that contain image files, JavaScript files, and HTML files, depending on the customization.

To upload and use a sample theme or extension, follow the instructions in [“Applying themes, extensions, and views” on page 247](#).

## Creating themes

---

You can override the standard IBM Cognos Analytics with Watson theme for the Cognos Analytics user interface to reflect your corporate branding.

A theme is a .zip archive that contains a `spec.json` file and an `images` folder. The `spec.json` file contains the branding instructions for each theme. The `images` folder contains the graphic images that are associated with the theme. You can give the .zip file a name of your choosing, as long as it does not include underscores (`_`). Image file names cannot contain spaces. The sample customization, `SampleTheme_11_2.zip` is an example of a theme. You can modify its contents to create your own custom theme.



#### Attention:

When you are using a sample theme, you cannot reset your password after it expires.

Your specific theme may consist of a folder such as `myTheme` that contains a `.json` file and `images` folder (containing your graphics). When creating the zip file, do not include the folder (e.g., `myTheme`) in the zip file; Cognos Analytics will not be able to process it. Instead, select the `.json` file and `images` folder, then use an archiving program to create the .zip file. Do not use the Windows Explorer “send to compressed folder” feature to create the .zip file; the result would be an incompatible file.

The `spec.json` file that is used with `SampleTheme_11_2.zip` contains the following text:

```
{
  "name": "Sample_Theme",
  "schemaVersion": "2.0",
  "brandText": "The Sample Outdoors Company",
  "brandTextSmall": "Sample Outdoors Company",
  "images": {
    "brandIcon": "images/logo_large_white.svg",
    "favicon": "images/logo_fav.png"
  },
  "uiShellTheme": "light",
  "colors": {
    "appbarBackground": "#eeeeee",
    "appbarForeground": "#000000",
    "appbarSelectLine": "#033f38",
    "navbarBackground": "#1c96d4",
```

```

    "navbarForeground": "white",
    "navbarSelectLine": "#033f38",
    "appbarPushButtonBackground": "#c8d2d1",
    "navbarPushButtonBackground": "#007670",
    "personalMenuBackground": "inherit"
  }
}

```

The objects in the spec . json file map to the Cognos Analytics user interface elements. If any theme items are omitted from the theme, then the Cognos Analytics default theme item is used.

This table relates the user interface elements to the JSON objects.

<i>Table 85. Theme objects</i>	
<b>JSON description</b>	<b>Definition</b>
brandText	Brand text. Enter an empty string to leave this entry blank.
brandTextSmall	Small brand text. if omitted, brandText is used. Enter an empty string to leave this entry blank.
brandIcon	Brand icon
favicon	Brand icon to display in web browser tab.
uiShellTheme	Allows you to switch between carbon 10 (light) and 100 (dark/default) background
appbarBackground	Application bar background color
appbarForeground	Application bar foreground color
appbarSelectLine	Application bar selection line color
navbarBackground	Navigation bar background color
navbarForeground	Navigation bar foreground color
navbarSelectLine	Navigation bar selection line color
appbarPushButtonBackground	Application bar push-button background color
navbarPushButtonBackground	Navigation bar push-button background color
personalMenuBackground	Specifies the background color of the Personal menu icon 

## Sample themes

The following examples are available that illustrate the use of themes.

These samples are installed in the `<installation_location>/samples/themes` folder.

### **SampleTheme\_11\_2.zip**

A theme that modifies the branding and color scheme for the Cognos Analytics user interface.

### **SampleThemeBlueGreen\_11\_2.zip**

A theme that modifies the color scheme for the Cognos Analytics user interface.

### **SampleThemeDarkBlue\_11\_2.zip**

A theme that modifies the color scheme for the Cognos Analytics user interface.

### **SampleThemeLight\_11\_2.zip**

A theme that modifies the color scheme for the Cognos Analytics user interface.

## Example: Applying the IBM\_Blue\_Green sample theme

This example describes how to apply the *IBM\_Blue\_Green* sample theme. It also illustrates, with screen captures, how each property in the theme changes the corporate branding of Cognos Analytics.

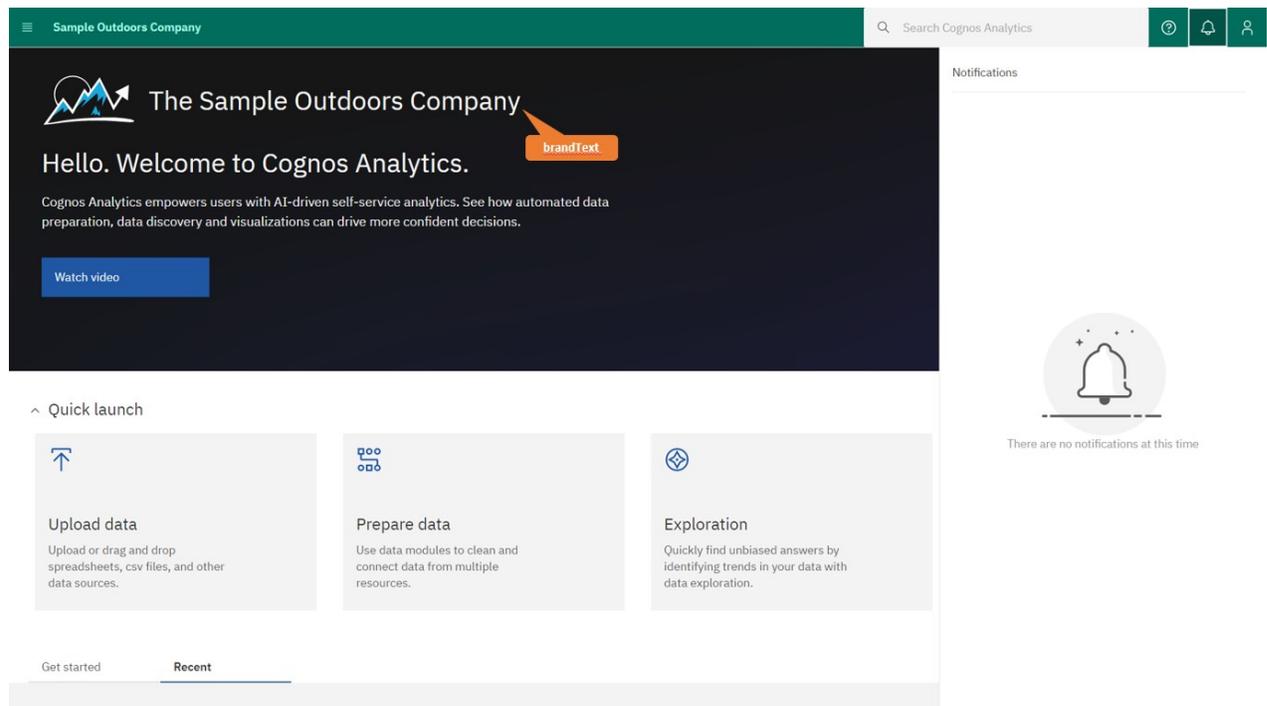
### Procedure

1. Click the Open menu icon , and then select **Manage > Customization**.
2. In the **Themes** tab, click the Upload theme icon .
3. Navigate to *installation\_location*\samples\themes, and then select the file `SampleThemeBlueGreen_11_2.zip`.
4. Click **Apply**.
5. Log out and log back in to Cognos Analytics to see the new theme. The colors and icons that are defined in the `spec.json` file appear in the Cognos Analytics window.

### View images that show how each parameter in the IBM\_Blue\_Green theme is applied

The `spec.json` file for the *IBM\_Blue\_Green* sample theme contains the parameter settings listed below. After each parameter setting, you can see its effect on the Cognos Analytics user interface.

#### "brandText": "The Sample Outdoors Company"



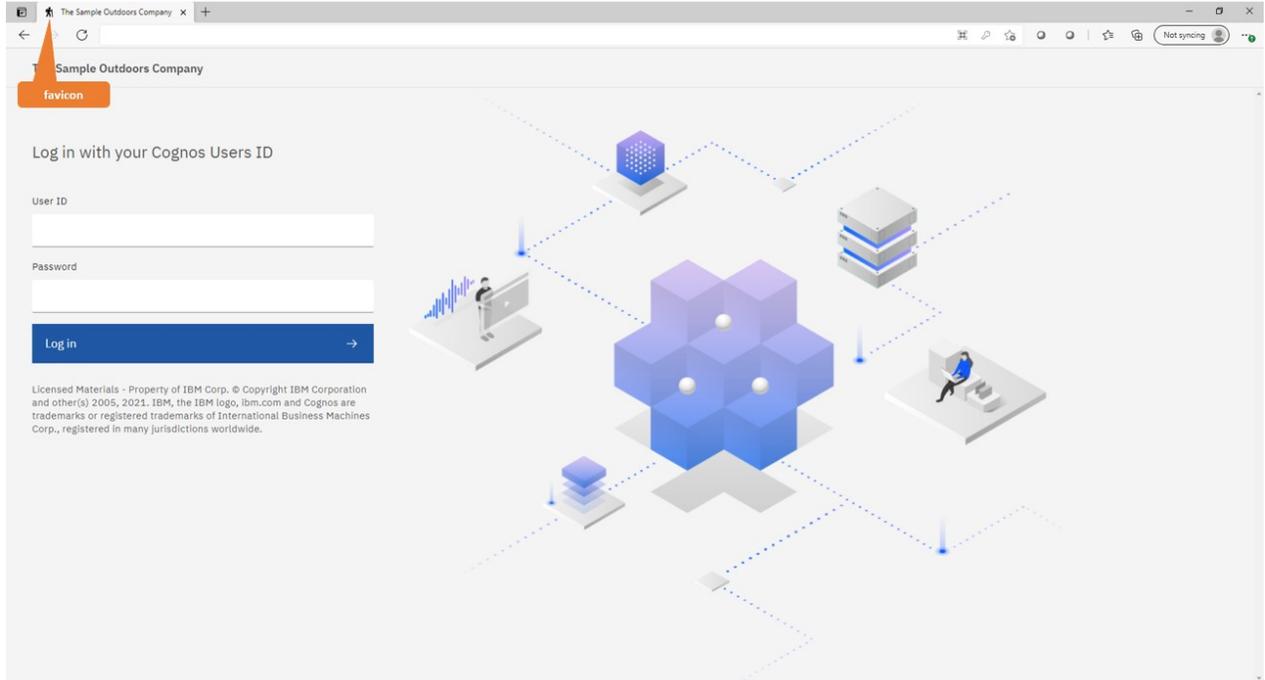
## "brandTextSmall": "Sample Outdoors Company"

The screenshot shows the Cognos Analytics dashboard for "Sample Outdoors Company". The top navigation bar is dark green with the company name and a search bar. A callout box labeled "brandTextSmall" points to the company name in the header. The main content area features a dark blue header with the company logo and name, followed by a welcome message and a "Watch video" button. Below this is a "Quick launch" section with three cards: "Upload data", "Prepare data", and "Exploration". The "Recent" tab is selected at the bottom. On the right, a "Notifications" panel shows a bell icon and the message "There are no notifications at this time".

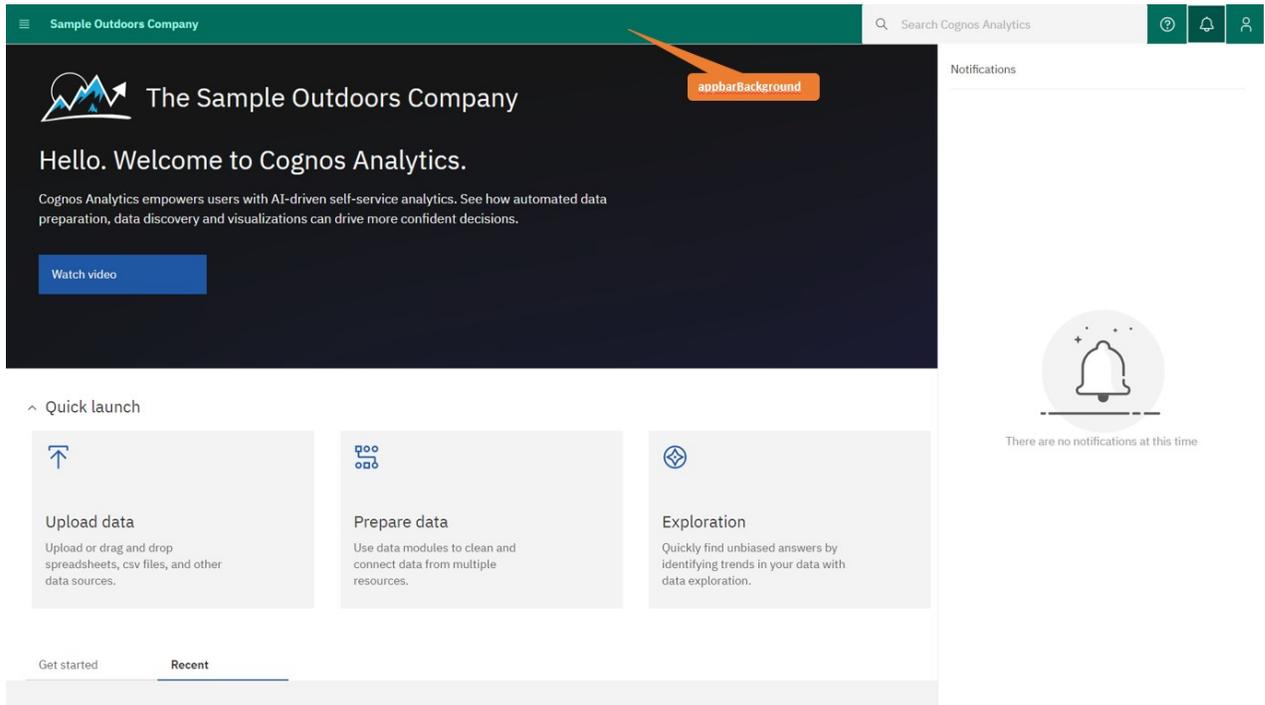
## "brandIcon": "images/logo\_large\_white.svg"

This screenshot is identical to the one above, but with a callout box labeled "brandIcon" pointing to the company logo in the header. The rest of the dashboard layout, including the navigation bar, main content area, and notification panel, remains the same.

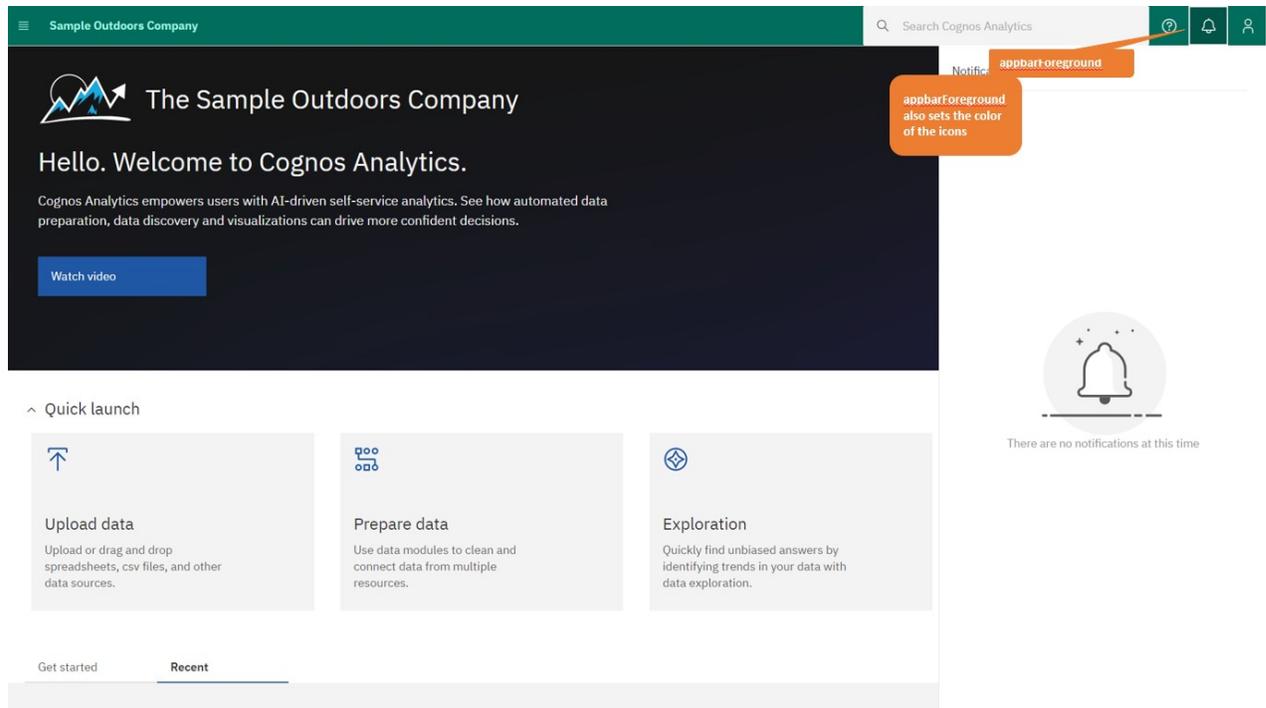
"favicon": "images/logo\_fav.png"



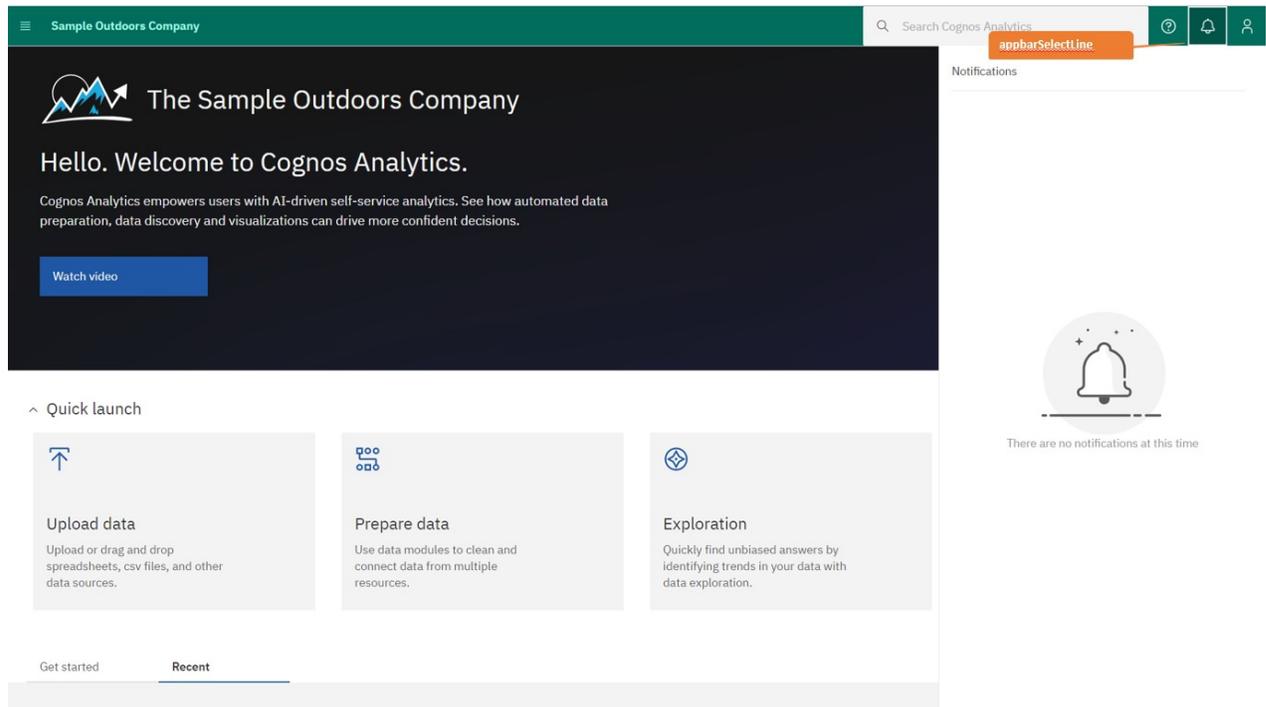
"appbarBackground": "#006d5d"



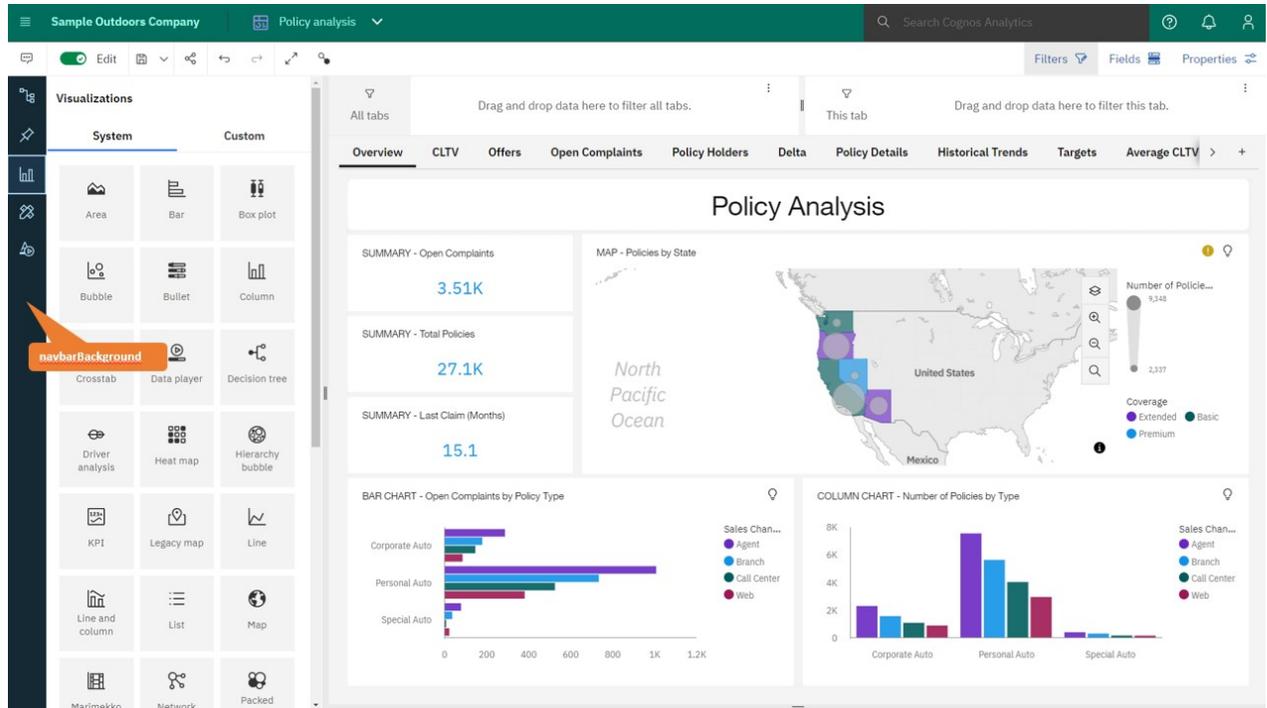
## "appbarForeground": "#a7fae6"



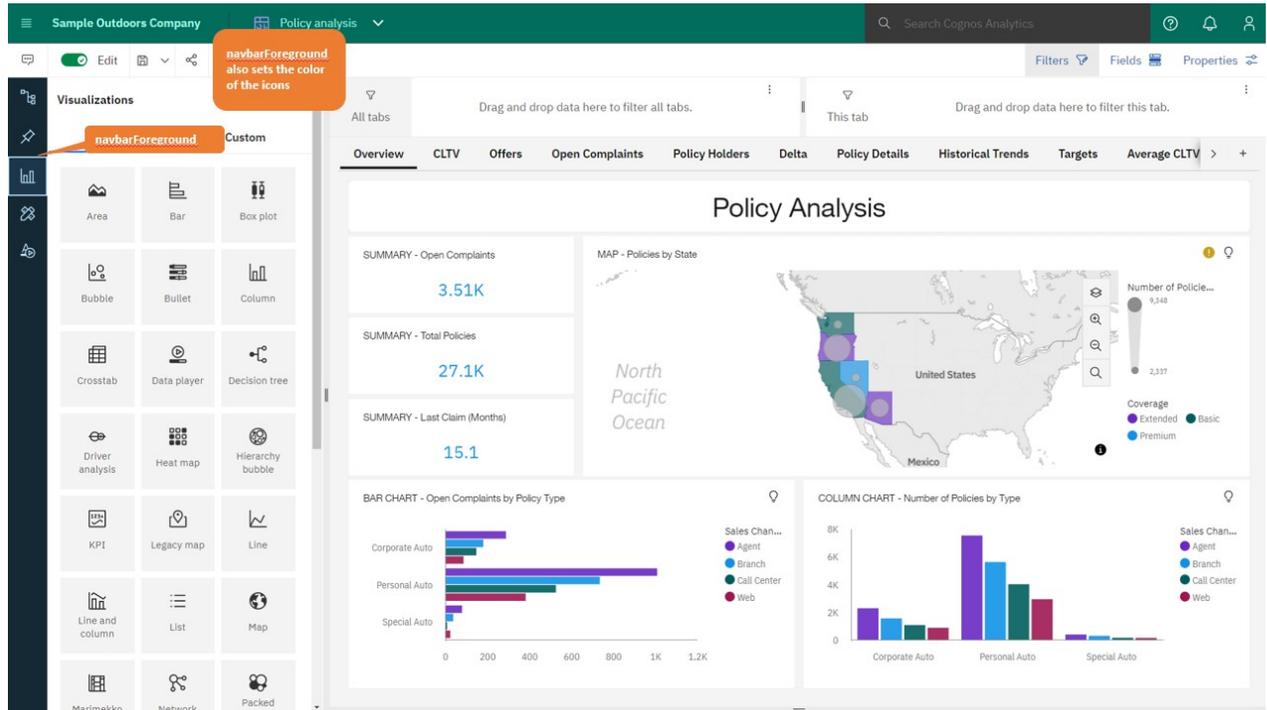
## "appbarSelectLine": "#6eedd8"



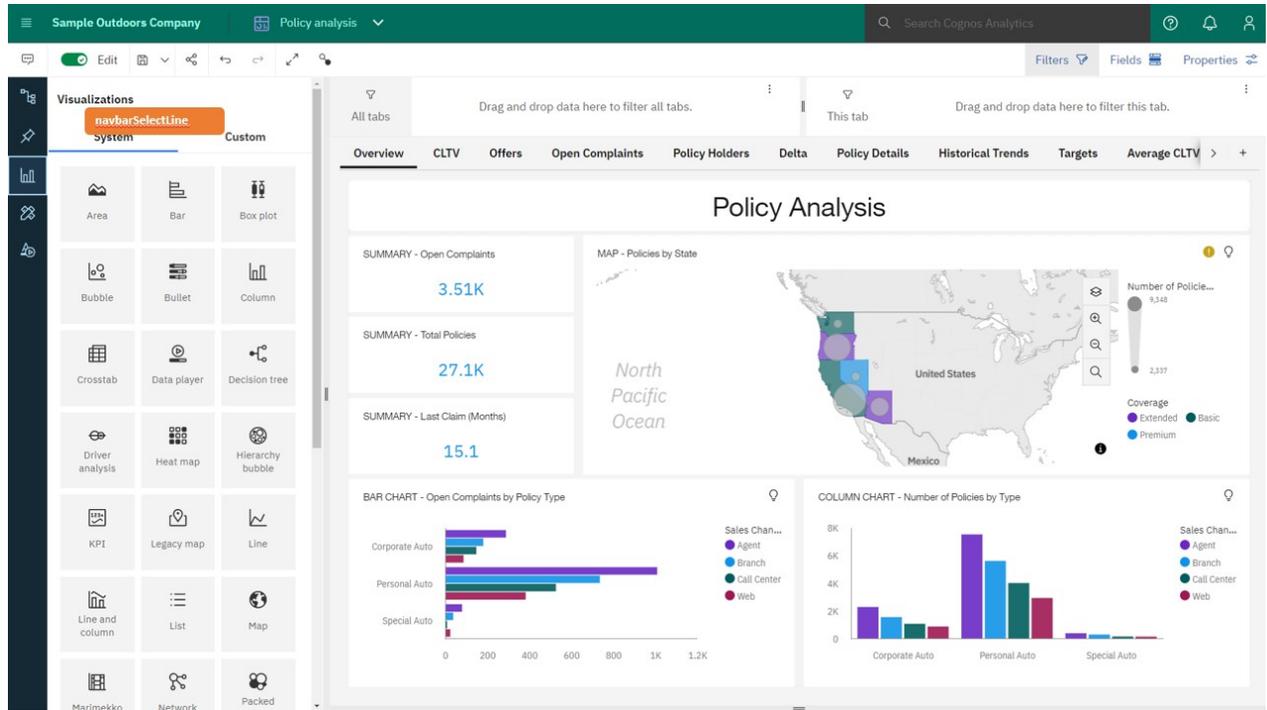
## "navbarBackground": "#152935"



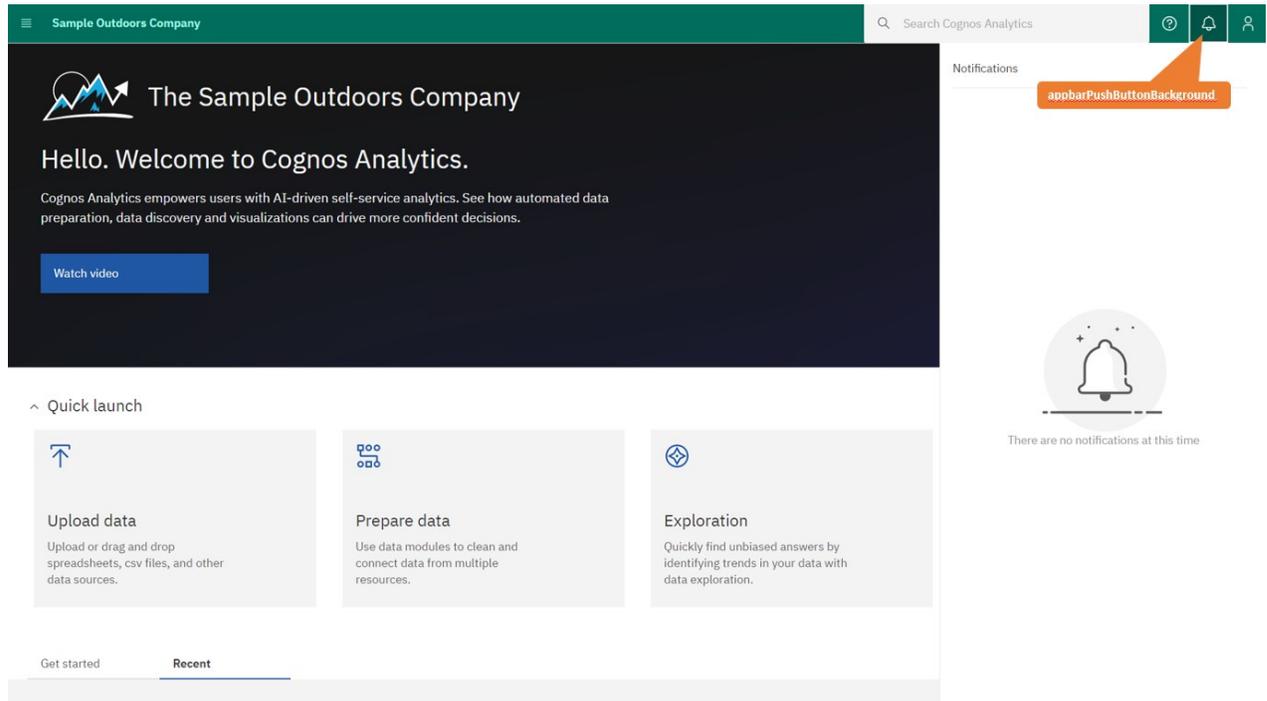
## "navbarForeground": "#c0e6ff"



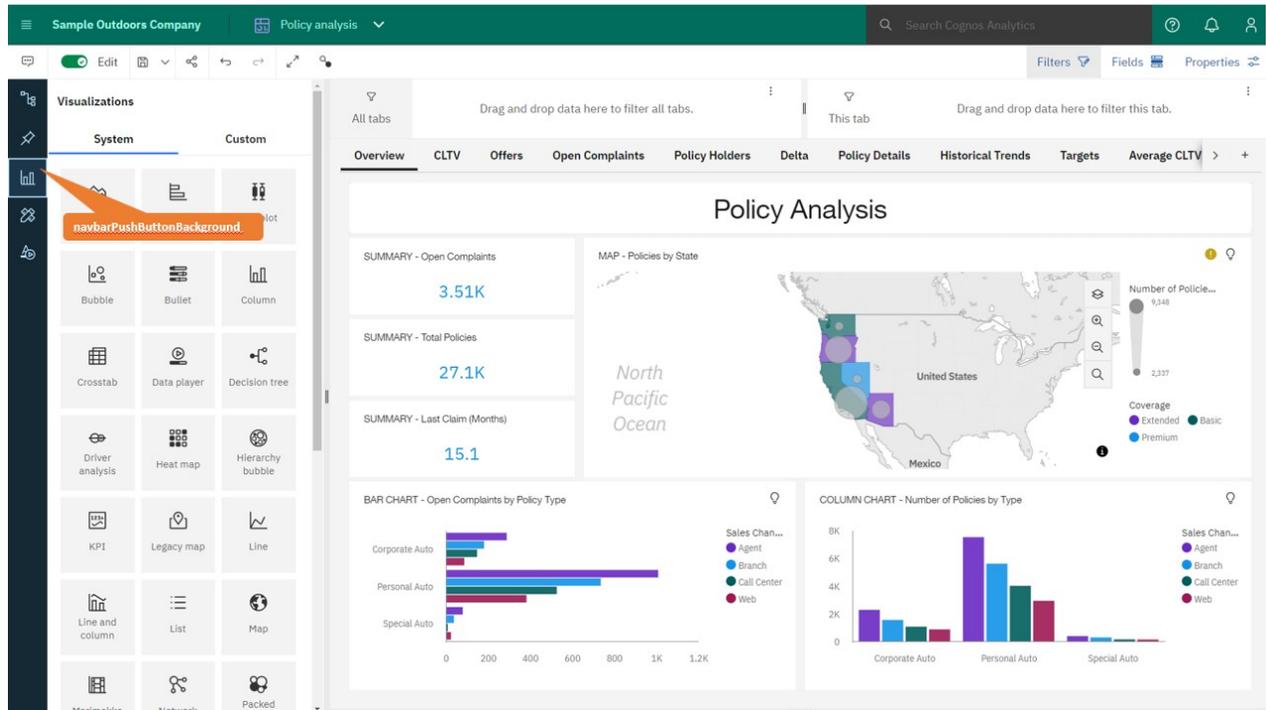
## "navbarSelectLine": "#7cc7ff"



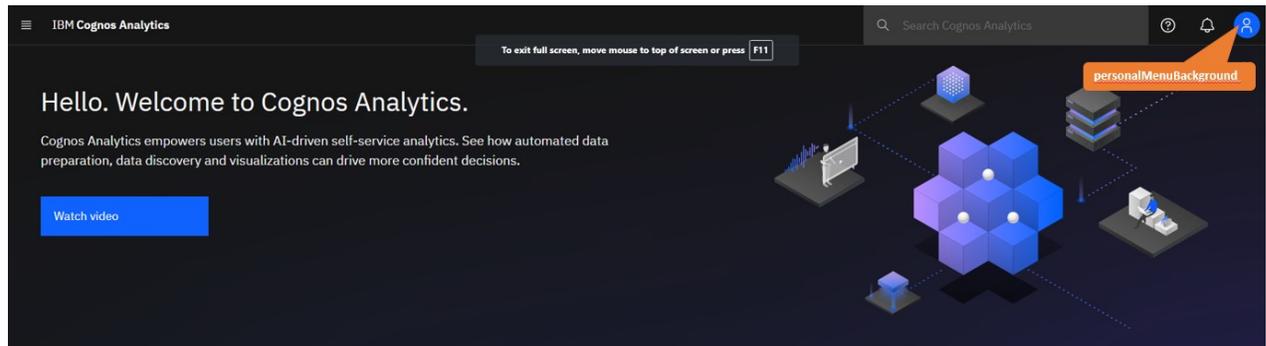
## "appbarPushButtonBackground": "#005448"



## "navbarPushButtonBackground": "#1d3649"



## "personalMenuBackground": "inherit"



### Quick launch

 <b>Upload data</b> Upload or drag and drop spreadsheets, csv files, and other data sources.	 <b>Prepare data</b> Use data modules to clean and connect data from multiple resources.	 <b>Exploration</b> Quickly find unbiased answers by identifying trends in your data with data exploration.	 <b>Present data</b> Create sophisticated, multi-page, multi-query dashboards, reports, or stories.
----------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------

Get started **Recent**

## Creating extensions

You can create extensions that add functions to the IBM Cognos Analytics with Watson user interface. For example, you can add buttons that, when clicked, open a particular report or dashboard. You can also remove default buttons from the user interface.

To create and upload extensions, you must have Portal Administrator or System Administrator privileges.



**CAUTION:** Be judicious when you assign **Develop Visualizations** access and ensure that you review files that are being uploaded. People who are permitted to upload files may be able to deliver malicious code.

Extensions are defined in a `spec.json` file that is contained in the root of the extension `.zip` file. Depending on the extension, there can also be folders that include images, HTML files, and JavaScript files. The structure and contents of the `spec.json` file is described in [“spec.json description” on page 249](#). The high-level structure of the file is show here.

```
{
  "name": "...",
  "schemaVersion": "1.0",
  "extensions": [
    {
      "perspective": "common",
      "features": [
        {
          "id": "...",
          "toolItems": [<tool_item1>,<tool_item2>,...],
          "collectionItems": [<collection_item1>,<collection_item2>,...],
          "excludeFeatures": [<exclude_feature1>,<exclude_feature2>,...],
          "excludeItems": [<exclude_item1>,<exclude_item2>,...]
        }
      ]
    }
  ]
}
```

The value of the `perspective` element indicates which views will use this extension. A value of `common` means that the extension is used for all views. The items contained in the `features` array are used depending on the action of the extension. These are illustrated in the following topics.

By creating extensions, you can modify existing views and create new views. The actions that an extension can perform are listed here and are described in the following topics. A single extension can perform one or more actions.

- Add a button to the Application or Navigation bars that performs an action such as displaying a web site, running a report, or opening a dashboard, a story, or a folder.
- Add a menu item to an existing menu that performs an action such as displaying a web site, running a report, or opening a dashboard, a story, or a folder.
- Add a menu along with its menu items.
- Remove a default user interface feature or item.
- Add custom shapes for use in dashboards.
- Add custom widgets for use in dashboards.

## Sample extensions

The following examples are available that illustrate the use of extensions.

**Note:** The samples covered in this topic are included with the Base Samples during a Cognos Analytics installation. After product installation, you can find them in the `installation_location/samples/extensions` folder.

IBM will provide support if the asset does not work as described for the product version(s) identified. However, we are unable to provide custom support for you such as adding features or troubleshooting environmental issues. These will be logged in our system as future Feature requests. These assets are functional examples. They are code samples with narrow requirements and a specific use case, providing a baseline. They do not include every possible feature/interactivity or environment/configuration. You can use these samples as-is (supported by IBM), or you can modify/extend these samples to suit your business needs (not supported).

### LearnPanelLink.zip

Adds an extension to the Custom widgets panel in Dashboarding and Stories that allows authors to add buttons that open specific topics in the Learn Pane.

**LinkWidget.zip**

Adds an extension to the Custom widgets panel in Dashboarding and Stories that allows authors to add buttons that open specific URLs.

**SampleExtensionContextMenuItem.zip**

Adds a new menu item to the context menu for all report objects. The new menu item launches a controller that displays information about the selected object in a popup window.

**SampleExtensionCustomMedia.zip**

Adds seven custom images to the Images tab in the Widgets panel in Dashboarding and Stories. JPG and PNG files are supported.

**SampleExtensionCustomMediaAll.zip**

Adds eight custom images to the Images tab in the Widgets panel in Dashboarding and Stories. It will also add the eight custom images to the Image Picker dialog in Reporting in the Image Gallery. JPG and PNG files are supported.

**SampleExtensionCustomShape.zip**

Adds custom shapes to the Widgets panel that can be used in dashboards and stories.

**SampleExtensionExcludeDelete\_11\_2.zip**

Removes the Delete button from the "content" perspective for all objects in the content pane.

**SampleExtensionExcludeNotifications.zip**

Removes the Notifications button from the "home" perspective.

**SampleExtensionMenuQuicklinks\_11\_2.zip**

Adds a menu to the application bar (across top of screen). Common reports and dashboards are accessed directly from this menu.

**SampleExtensionMenuUrlLinks\_11\_2.zip**

Demonstrates how to add a menu to the AppBar that contains two menu items that open external URLs. The URLs are opened in a separate browser tab.

**SampleExtensionOpenDashboard\_11\_2.zip**

Adds a menu item to the Open menu to open a dashboard in all perspectives.

**SampleExtensionOpenFolder\_11\_2.zip**

Shows the use of the skipAncestors option when opening a folder. Two menu items are added to the Open menu that open folders. Within the folder, the navigation breadcrumbs at the top of the screen will be either shown or hidden.

**SampleExtensionOpenFolderShowHideParent\_11\_2**

Shows the use of the skipAncestors option when opening a folder. Two menu items are added to the Open menu that open folders. Within the folder, the navigation breadcrumbs at the top of the screen will be either shown or hidden.

**SampleExtensionOpenPerspective\_11\_2.zip**

Creates a new view called "Custom view" and then adds an Open menu item to open it from all perspectives.

**SampleExtensionOpenReport\_11\_2.zip**

Adds a menu item to the Open menu to open a report in all perspectives.

**SampleExtensionOpenWebsite\_11\_2.zip**

Adds a menu item to the Open menu to open a website in all perspectives.

**SampleLogin.zip**

Creates a customized view for the Cognos Analytics sign-in page for the Sample Outdoors Company example. Not available in 11.1.0 and 11.1.1.

**SampleLoginMultiple.zip**

Creates a custom Sign In page where the user can choose between two or more authentication types via a dropdown. Not available in 11.1.0 and 11.1.1.

**SampleWelcome\_11\_2.zip**

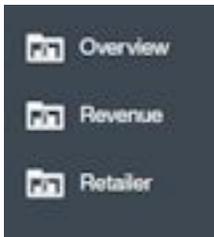
Creates a customized view for the Cognos Analytics welcome page for the fictional Sample Outdoors Company.

## Using the tabs collection extension

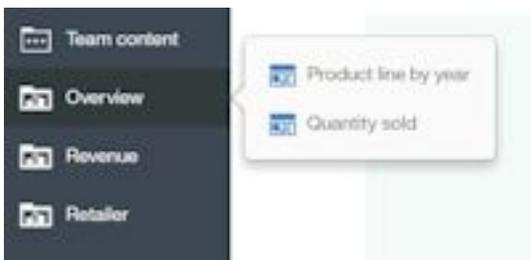
This task shows you how to install and use the tabs collection extension.

### About this task

The tabs collection extension emulates the portal pages available in older versions of IBM Cognos Business Intelligence. This extension adds three buttons to the navigation bar as shown here.



Each button corresponds to a tab in a portal page. Click the **Overview** button to display a subfolder that contains two items, the **Product line by year** dashboard, and the **Quantity sold** report. The subfolder is equivalent to a subtab in a portal page.



Click the **Revenue** button to display a subfolder that contains three items, the **By year** dashboard, the **By quarter** folder that contains four reports, and the **QTD** report.



Click the **Retailer** button to open a dashboard.

### Procedure

Upload the **Samples\_for\_Install** deployment archive. (If not already done.)

1. Use **Manage > Administration console** to open **IBM Cognos Administration**.
2. On the **Configuration** tab, click **Content Administration**.
3. On the toolbar, click the **New Import** button.
4. Select **Samples\_for\_Install** in the first step of the **New Import** wizard and complete the remaining steps of the wizard.

Upload the `SampleExtensionTabs.zip` sample extension.

5. In the **Manage > Customizations** slide-out panel, select the **Extensions** tab, click **Upload**

**extension** (↑), browse to the `<installation_location>/samples/extensions` folder, and select `SampleExtensionTabs.zip`.

### Results

You can now use this extension.

## Modifying icons to appear against a light background

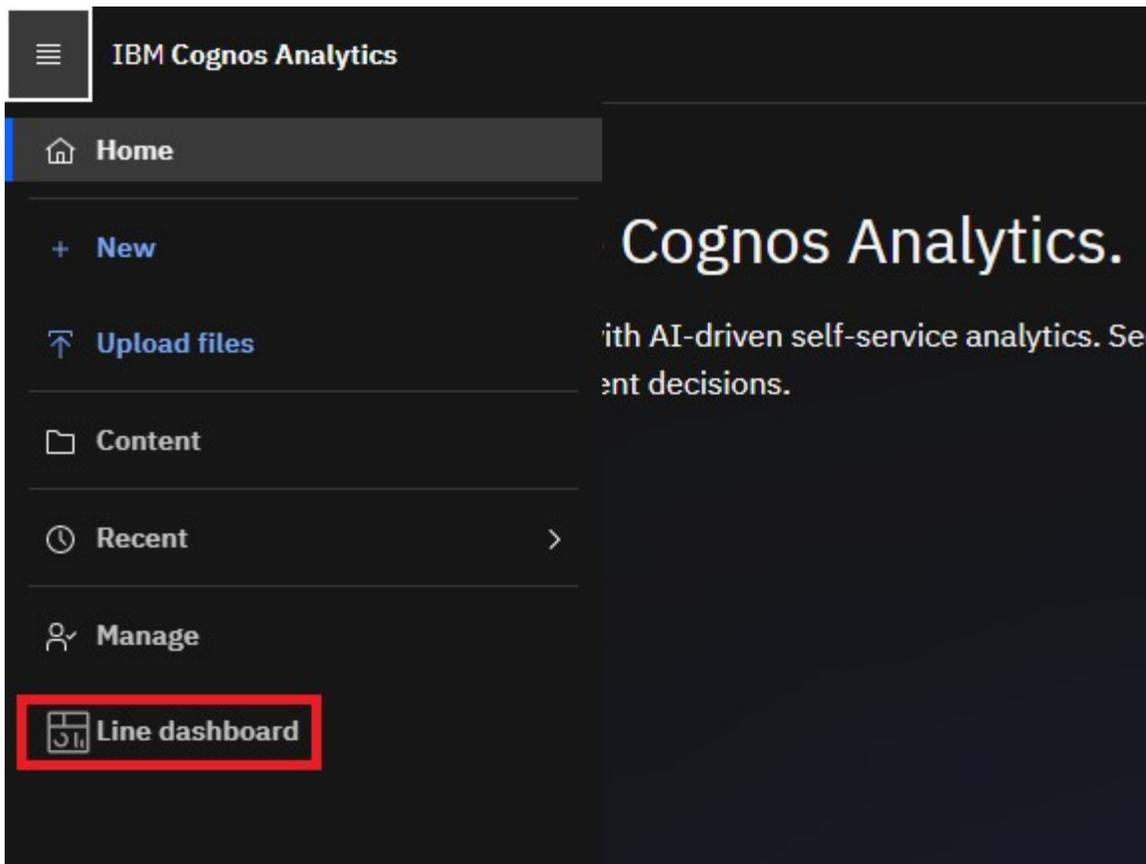
You can change the color of icons in the sample extensions to ensure that they contrast sufficiently against the background color of your theme.

### About this task

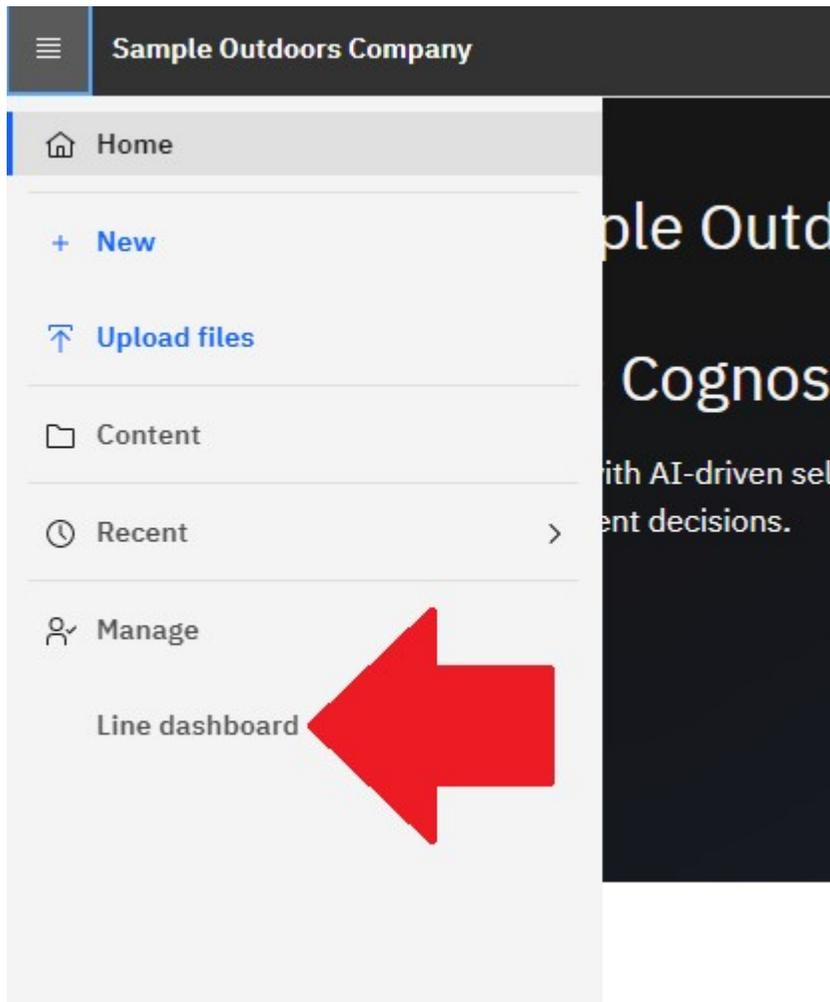
Many of the Cognos Analytics sample extensions contain icons that are designed to work with the default theme, **IBM Carbon X**, which has a dark background. However, if you apply a theme without a dark background, these icons become indiscernible.

### Example

The extension `SampleExtensionOpenDashboard_11_2.zip` includes the icon `dashboard.svg`. It has a light color, hexadecimal color code `#f4f4f4`, as shown next to the **Line dashboard** option in the following diagram:



If you apply a theme in which the background is a light color, you can no longer see the icon:



To fix this issue, follow these steps:

## Procedure

1. Download the extension.
2. Unzip the contents of the extension.
3. Modify the color of the image(s) in the images folder and save the changes.

For example, after you unzip the extension `SampleExtensionOpenDashboard_11_2.zip`, change the color of the icon from a light color (`#F4F4F4`) to a dark color (`#161616`):

- a. In the `images` folder, open the file `dashboard.svg` in a text editor.
- b. Replace this text:

```
<style type="text/css"> .st0{fill:#F4F4F4;} .st1{fill:none;} </style>
```

with this text:

```
<style type="text/css"> .st0{fill:#161616;} .st1{fill:none;} </style>
```

- c. Save the file.
4. Create a `.zip` file that contains all the files and folders.
  5. Upload the revised extension.

## Results

The black icon is visible against the light background.

For more information, see these topics:

- [Creating extensions](#)
- [Creating themes](#)

## Adding a button or a menu item

You can add buttons and menu items to perform various actions, such as displaying a web site, running a report, opening a dashboard, a story, or a folder. You can also create custom actions.

All buttons require an action controller. There are four built-in action controllers that perform common actions. These actions are shown here.

### **bi/glass/api/IFrameOpener**

Opens a web page.

### **bi/glass/api/ReportOpener**

Runs a report.

### **bi/glass/api/DashboardOpener**

Opens a dashboard.

### **bi/glass/api/FolderOpener**

Opens a folder.

You can also write custom action controllers using JavaScript.

The content of the `json.spec` file are similar for buttons and menu items and they are described together. The main difference is that the value of the `type` element is `button` for a button and `menuItem` for a menu item. Other differences are noted in the following topics.

## Using built-in action controllers

There are four built-in action controllers available. These action controllers can open a web page, run a report, open a folder, and open a dashboard or story. The action controllers are described in the following sections.

### Opening a web page

Use the `bi/glass/api/IFrameOpener` action controller to open a web page. The available options are shown here.

#### **url**

Specifies the web page URL to open.

#### **title**

Specifies the web page title to display.

The `SampleExtensionButtonWebsite.zip` sample extension opens a web page. The `spec.json` file is shown here.

```
{
  "name": "Sample_Button_Website",
  "schemaVersion": "1.0",
  "extensions": [
    {
      "perspective": "common",
      "comment": "There is a special meta perspective called COMMON. Adding
        contributions to this perspective will cause the extension to be
        applied to All perspectives.",
      "features": [
        {
          "id": "sample.common.button.openWebsite",
          "toolItems": [
            {
              "comment": "This code will display a custom Website button that opens
```

```

        the specified URL in an iFrame.",
        "id": "sample.iframeOpener.website",
        "containerId": "com.ibm.bi.glass.navbarTrailingGroup",
        "label": "Website",
        "type": "Button",
        "icon": "images/web.png",
        "weight": 100,
        "actionController": "bi/glass/api/IFrameOpener",
        "options": {
            "url": "http://www.ibm.com/analytics/us/en/technology/products/cognos-
analytics/",
            "title": "Website"
        }
    }
}
}]]
}}

```

The button label is Website and the button icon is the web.png image this is in the images folder. The action controller is bi/glass/api/IFrameOpener and it requires two options, the web page URL (url) and the web page title to display when the page is opened (title). The other elements in the spec.json file are described in [“spec.json description” on page 249](#).

## Running a report

Use the bi/glass/api/ReportOpener action controller to run a report. The available options are shown here. Either the id or the path must be specified.

### id

Specifies the storeID of the report to run.

### path

Specifies the path of the report to run.

The SampleExtensionButtonReport.zip sample extension runs a report. The spec.json file is shown here.

```

{
  "name": "Sample_Button_Report",
  "schemaVersion": "1.0",
  "extensions": [
    {
      "perspective": "common",
      "comment": "There is a special meta perspective called COMMON. Adding contributions
to this perspective will cause the extension to be applied to All
perspectives.",
      "features": [
        {
          "id": "sample.common.button.openReport",
          "toolItems": [
            {
              "comment": "This adds a button to the navbar to directly open a popular
report.",
              "id": "sample.report.opener",
              "containerId": "com.ibm.bi.glass.navbarLeadingGroup",
              "label": "QTD revenue",
              "type": "Button",
              "icon": "common-report",
              "weight": 800,
              "comment": "The greater the weight, the higher the item appears in the
container.",
              "actionController": "bi/glass/api/ReportOpener",
              "options": { "path": ".public_folders/Samples/Extensions/QTD revenue" }
            }
          ]
        }
      ]
    }
  ]
}
}]]
}}

```

The action controller is bi/glass/api/ReportOpener and it requires one option, the path to the report (path). .public\_folders is the root folder for **Team content** and .my\_folders is the root folder for **My content**. If the report name contains a slash(/), it must be encoded as %2F. The other elements in the spec.json file are described in [“spec.json description” on page 249](#).

## Opening a dashboard or a story

Use the `bi/glass/api/DashboardOpener` action controller to open a dashboard or a story. The available options are shown here. Either the `id` or the `path` must be specified.

### id

Specifies the storeID of the dashboard or story to open.

### path

Specifies the path of the dashboard or story to open.

The `SampleExtensionButtonDashboard.zip` sample extension opens a dashboard. The `spec.json` file is shown here.

```
{
  "name": "Sample_Button_Dashboard",
  "schemaVersion": "1.0",
  "extensions": [
    {
      "perspective": "common",
      "comment": "There is a special meta perspective called COMMON. Adding contributions
        to this perspective will cause the extension to be applied to
        All perspectives.",
      "features": [
        {
          "id": "sample.common.button.openDashboard",
          "toolItems": [
            {
              "comment": "This code adds a button to directly open a core dashboard.",
              "id": "sample.dashboard.opener",
              "containerId": "com.ibm.bi.glass.navbarLeadingGroup",
              "label": "Line dashboard",
              "type": "Button",
              "icon": "common-dashboard",
              "weight": 900,
              "comment": "The greater the weight, the higher the item appears in the
                container.",
              "actionController": "bi/glass/api/DashboardOpener",
              "options": {"path": ".public_folders/Samples/Extensions/Line dashboard"}
            }
          ]
        }
      ]
    }
  ]
}
```

The action controller is `bi/glass/api/DashboardOpener` and the only option is the path to the dashboard (`path`) which is determined in the same way as the path to a report. The other elements in the `spec.json` file are described in [“spec.json description” on page 249](#).

## Opening a folder

Use the `bi/glass/api/FolderOpener` action controller to open a folder. The available options are shown here. Either the `id` or the `path` must be specified.

### id

Specifies the storeID of the folder to open.

### path

Specifies the path of the folder to open.

### skipAncestors

Specifies whether ancestor folders should be displayed (`false`) or hidden (`true`) when the folder is opened. The default value is `false`.

The `SampleExtensionButtonFolder.zip` sample extension opens a folder. The `spec.json` file is shown here.

```
{
  "name": "Sample_Button_Folder",
  "schemaVersion": "1.0",
  "extensions": [
    {
      "perspective": "common",
      "comment": "There is a special meta perspective called COMMON. Adding contributions
```



The custom action controller is the `SampleContextMenuItem.js` file and is located in the `js/controllers` folder in the extension. The file is shown here.

```
/**
 * Licensed Materials - Property of IBM
 *
 * IBM Cognos Products: BI Glass
 *
 * Copyright IBM Corp. 2015
 *
 * US Government Users Restricted Rights - Use, duplication or disclosure restricted by
 * GSA ADP Schedule Contract with IBM Corp.
 */
define([], function() {
    'use strict';

    var SampleAction = function(){

        /**
         * Called by the ApplicationController whenever this view is created
         *
         * @public
         * @returns {Promise} promise resolved to the root DOM element for this view.
         */
        this.isVisible = function(context, target) {
            return target.options[0].type === 'report';
        },

        /**
         * Called by the ApplicationController whenever this view is destroyed
         *
         * @public
         */
        this.execute = function(context, target) {
            var info = 'This sample menu item extension opens an alert.
                \n\nThe alert contains information about the selected report.
                \n\nType: ' + target.options[0].type + '\nName: ' + target.options[0].name
                + '\nID: ' + target.options[0].id;
            alert(info);
        }

    };

    return SampleAction;
});
```

This JavaScript code uses the Action API in a JavaScript AMD module. These modules require the JavaScript Q library. The Action API consists of two methods.

#### **void execute(context, target)**

##### **context**

This object contains utility methods.

##### **target**

This object contains information about the button or menu item that is created by the extension.

- For a button or menu item in an Application bar or navigation bar menu, this object contains the `options` property for the item.
- For a menu item in a contextual menu of an object, this object contains an array of the type, name, and Store ID of the object.

#### **boolean isVisible(context, target)**

This method is only applicable to menu items. The menu item is displayed if this method returns `true`; otherwise the menu item is hidden.

## Adding a menu

You can add a menu and its associated menu items to the Application or Navigation bars.

The `SampleExtensionMenuQuicklinks.zip` sample extension adds a menu and six menu items. Part of the `spec.json` file is shown here.

```
{
  "name": "Sample_Menu_Quicklinks",
  "schemaVersion": "1.0",
  "extensions": [
    {
      "perspective": "common",
      "comment": "There is a special meta perspective called COMMON. Adding contributions to this perspective will cause the extension to be applied to All perspectives.",
      "features": [
        {
          "id": "sample.common.menu.openMultipleItems",
          "toolItems": [
            {
              "comment": "This code adds a custom menu item to the App Bar in the trailing group.",
              "id": "custom.appbar.trailingGroup.menu",
              "containerId": "com.ibm.bi.glass.appbarTrailingGroup",
              "type": "Menu",
              "label": "Quick links",
              "icon": "images/debug.svg",
              "weight": 650
            },
            {
              "comment": "This code adds a submenu item to the custom menu created above.",
              "id": "custom.appbar.trailingGroup.menuItem1",
              "containerId": "custom.appbar.trailingGroup.menu",
              "comment": "The containerId is the ID of the parent menu.",
              "type": "MenuItem",
              "actionController": "v1/ext/Sample_Menu_Quicklinks/js/controllers/SampleMenuQuicklinks",
              "comment": "The actionController determines the actions for the menu item.",
              "label": "Home",
              "icon": "common-home",
              "weight": 900
            },
            {
              "comment": "This code adds a submenu item to the custom menu created above.",
              "id": "custom.appbar.trailingGroup.menuItem2",
              "containerId": "custom.appbar.trailingGroup.menu",
              "comment": "The containerId is the ID of the parent menu.",
              "label": "Line dashboard",
              "type": "MenuItem",
              "icon": "common-dashboard",
              "weight": 800,
              "actionController": "bi/glass/api/DashboardOpener",
              "comment": "The actionController determines the actions for the menu item.",
              "options": {"path": ".public_folders/Samples/Extensions/Line dashboard"}
            }
          ], ...
        }
      ]
    }
  ]
}
```

In this example, the menu is located in the Application bar trailing group.

## Removing a user interface element

You can remove default user elements from all or specified views.

**Note:** If you modify and apply this extension, you may notice changes that you didn't expect. As an alternative, you can [remove a feature for a role](#).

The `SampleExtensionExcludeNotifications.zip` sample extension removes the **Notifications** button from the Navigation bar. The `spec.json` file is shown here.

```
{
  "name": "Sample_Exclude_Notifications",
  "schemaVersion": "1.0",
  "extensions": [
    {
      "perspective": "home",
```

```

    "comment": "This code will apply only to the HOME perspective.",
    "features": [{
      "id": "sample.home.exclude.notifications",
      "excludeItems": ["com.ibm.bi.share.notifications"],
      "comment": "Above, EXCLUDEITEMS will remove the Notifications button from the
        Nav Bar of the HOME perspective.",
      "comment": "EXCLUDEITEMS must be applied at the individual perspective level.
        It can not be used globally via the COMMON perspective."
    }]
  }
}

```

## Adding dashboard shapes

You can create custom shapes for use in dashboards.

The `SampleExtensionCustomShape.zip` sample creates three new shapes for use in dashboards. This sample is installed like any other extension. After it is installed, the following three new shapes appear in the **Shapes** panel.



**Note:** Only .svg files can be used as dashboard shapes.

The contents of the `spec.json` file are shown here.

```

{
  "name": "Sample_Custom_Shape",
  "comment": "This sample will add 3 custom images to the bottom of the Shape panel in
Dashboarding.",
  "schemaVersion": "2.0",
  "extensions": [
    {
      "perspective": "dashboard",
      "comment": "The custom shapes are for the dashboard perspective only.",
      "features": [
        {
          "id": "com.ibm.bi.dashboard",
          "collectionItems": [
            {
              "containerId": "com.ibm.bi.dashboard.shapes",
              "id": "sample_custom_shape_music",
              "name": "Music",
              "options": {
                "templatePath": "v1/ext/Sample_Custom_Shape/images/music_32.svg"
              }
            },
            {
              "containerId": "com.ibm.bi.dashboard.shapes",
              "id": "sample_custom_shape_relationship",
              "name": "Relationship",
              "options": {
                "templatePath": "v1/ext/Sample_Custom_Shape/images/relationship_32.svg"
              }
            },
            {
              "containerId": "com.ibm.bi.dashboard.shapes",
              "id": "sample_custom_shape_traffic",
              "name": "Traffic",
              "options": {
                "templatePath": "v1/ext/Sample_Custom_Shape/images/traffic_32.svg"
              }
            }
          ]
        }
      ]
    }
  ]
}

```

The custom shapes are contained in the `images` folder of the sample.

## Uploading custom images

You can add your own custom images to Cognos Analytics for use in dashboards, stories, and reports.

The [SampleExtensionCustomMedia.zip](#) (dashboards and stories only) and [SampleExtensionCustomMediaAll.zip](#) (reports, dashboards, and stories) samples provide a way to add new images for use in Cognos objects. These samples are installed like any other extension.

After you upload these extensions, you can select images as follows:

- **Dashboard and Stories:** After either of the above extensions are installed, dashboard and story authors can select their custom images in the **Widgets** panel. For more information, see the *Dashboards and Stories guide*.
- **Reporting:** After the [SampleExtensionCustomMediaAll.zip](#) extension is installed, report authors can select the **Toolbox** icon , select **Layout**, drag the **Image** object  to the report, and then double-click it. For more information, see the *Reporting guide*.

The images available in the image library have the following descriptions:

- Lightning strike above a city at night
- Lightning in a dark purple sky
- Heavy traffic in a city at night
- Hiker on a hill in the forest
- Several tents on a mountain
- Graph with increasing revenue highlighted
- Graph of increasing revenue
- Group of people in a Call Center

### Sample\_Custom\_Media

The contents of the spec.json file for Sample\_Custom\_Media is shown here.

```
{
  "name": "Sample_Custom_Media",
  "comment": "This sample extension will add seven custom images to the Widgets panel in Dashboarding and Stories.",
  "comment": "We currently only support the addition of JPG and PNG files.",
  "schemaVersion": "1.0",
  "extensions": [
    {
      "perspective": "dashboard",
      "comment": "The custom images are for the DASHBOARD perspective only.",
      "features": [
        {
          "id": "com.ibm.bi.common.media",
          "comment": "This is the ID for the MEDIA panel. It will be the container for the images below.",
          "collectionItems": [
            {
              "containerId": "com.ibm.bi.common.media",
              "id": "customImage1",
              "name": "Lightning above city",
              "comment": "The NAME is the text of the tooltip for the image.",
              "options": {
                "altText": "Lightning strike above a city at night.",
                "comment": "The ALTTEXT is shown as a Property for the selected image.",
                "imageLink": "v1/ext/Sample_Custom_Media/images/SE_background.jpg"
              }
            },
            {
              "containerId": "com.ibm.bi.common.media",
              "id": "customImage2",
              "name": "Lightning in sky",
              "options": {
                "altText": "Lightning in a dark purple sky.",
                "imageLink": "v1/ext/Sample_Custom_Media/images/weather_background3.jpg"
              }
            },
            {
              "containerId": "com.ibm.bi.common.media",
              "id": "customImage3",
              "name": "Night city traffic",
```

```

        "options": {
            "altText": "Heavy traffic in a city at night.",
            "imageLink": "v1/ext/Sample_Custom_Media/images/
story_scene1_background.jpg"
        }, {
            "containerId": "com.ibm.bi.common.media",
            "id": "customImage4",
            "name": "Hiker on hill",
            "options": {
                "altText": "Hiker on a hill in the forrest.",
                "imageLink": "v1/ext/Sample_Custom_Media/images/login_background.jpg"
            }
        }, {
            "containerId": "com.ibm.bi.common.media",
            "id": "customImage5",
            "name": "Tents on mountain",
            "options": {
                "altText": "Several tents on a mountain.",
                "imageLink": "v1/ext/Sample_Custom_Media/images/welcome_background.jpg"
            }
        }, {
            "containerId": "com.ibm.bi.common.media",
            "id": "customImage6",
            "name": "Increasing revenue highlighted",
            "options": {
                "altText": "Graph with increasing revenue highlighted.",
                "imageLink": "v1/ext/Sample_Custom_Media/images/
story_scene5_background2.jpg"
            }
        }, {
            "containerId": "com.ibm.bi.common.media",
            "id": "customImage7",
            "name": "Increasing revenue",
            "options": {
                "altText": "Graph of increasing revenue.",
                "imageLink": "v1/ext/Sample_Custom_Media/images/
story_scene5_background.jpg"
            }
        }
    }
}

```

## Sample\_Custom\_Media\_All

The contents of the spec.json file for Sample\_Custom\_Media\_All is shown here.

```

{
    "name": "Sample_Custom_Media_All",
    "comment": "This sample extension will add eight custom images to the Widgets panel in
Dashboarding and Stories.",
    "comment": "It will also add the same eight custom images to the IMAGE PICKER dialog in
Reporting.",
    "comment": "Only JPG and PNG files are supported at this time.",
    "comment": "These types of extensions are not additive. You must specify all of the custom
images you require in one extension.",
    "comment": "Otherwise, the last uploaded extension (not UPDATED) will take precedence and
become your final library of images.",
    "schemaVersion": "1.0",
    "extensions": [
        {
            "perspective": "common",
            "comment": "The custom images will apply to all perspectives - reporting,
dashboarding, and stories.",
            "features": [
                {
                    "id": "com.ibm.bi.common.media",
                    "comment": "This is the ID for the Widgets panel. It will be the container
for the images below.",
                    "collectionItems": [
                        {
                            "containerId": "com.ibm.bi.common.media",
                            "id": "customImage1",
                            "name": "Lightning above city",
                            "comment": "The NAME is the text of the tooltip for the image
within the Image Library tab.",
                            "options": {
                                "altText": "Lightning strike above a city at night.",
                                "comment": "The ALTTEXT is shown in the Description Property
for the selected image once it is placed on the dashboard.",
                                "imageLink": "v1/ext/Sample_Custom_Media_All/images/

```



## Adding a dashboard widget

You can create custom widgets for use in dashboards.

You can create custom widgets for use in dashboards. Custom widgets are installed in the same way as other extensions. The widget action is determined by a JavaScript file that can execute any JavaScript actions and displays the results in the widget.

A simple custom widget contains a `spec.json` file, a JavaScript file, and a folder that contains images that are used by the widget. The `spec.json` file is shown here.

```
{
  "name": "SampleWidgetExt_old",
  "schemaVersion": "1.0",
  "extensions": [
    {
      "perspective": "dashboard",
      "comment": "Sample custom widgets for dashboard",
      "features": [
        {
          "id": "com.ibm.bi.dashboard.widgets",
          "collectionItems": [
            {
              "containerId": "com.ibm.bi.dashboard.widgets",
              "id": "Hello",
              "title": "Hello!",
              "iconUrl": "v1/ext/SampleWidgetExt/images/ibm.png",
              "widget": "v1/ext/SampleWidgetExt/helloParam.js",
              "scroll": "scrollNone",
              "disableTitle": true,
              "params": {
                "name": "IBM"
              }
            }
          ]
        }
      ]
    }
  ]
}
```

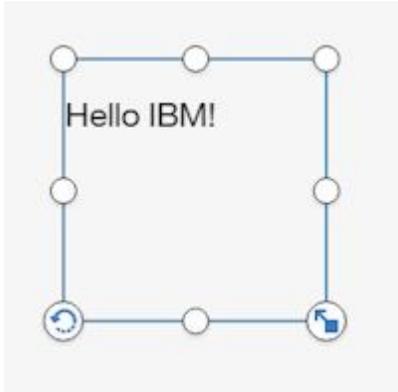
This widget calls the `helloParam.js` JavaScript file, which is shown here.

```
define([
  'jquery',
  'dashboard/widgets/CustomWidget'
], function( $, Base ) {
  var Widget = Base.extend({
    onInit: function(params) {
      this.name = params.name;
    },
    onRender: function() {
      var root = this.getContentRootNode();
      $(root).append('<h1 class="titleColor titleFontSize">Hello ' + this.name + '!</h1>');
    }
  });
  return Widget;
});
```

The `images` folder contains the `ibm.png` graphic image.

After the extension is installed, users who create a dashboard will see a new icon, **Custom widgets** .

After they click **Custom widgets** , they can drag the custom widget onto the dashboard canvas. The custom widget is shown here.



## compatibleProductVersion

Use the `compatibleProductVersion` parameter in your extension's `spec.json` file to indicate which versions of Cognos Analytics the extension supports.

If an extension using the `compatibleProductVersion` setting is uploaded to a version of Cognos Analytics that does not meet the version criteria, after a System Administrator or Tenant Administrator subsequently logs in or refreshes their browser, they are notified by a message in the alert banner.

### Attributes

The `compatibleProductVersion` parameter uses these attributes:

- **min** - the earliest version of Cognos Analytics in which the extension is supported
- **max** - the latest version of Cognos Analytics in which the extension is supported
- both **min** and **max** - indicates the range of versions in which the extension is supported

For example, in the following snippet, the `compatibleProductVersion` parameter specifies a range of supported versions between release 11.1.7 and release 11.2.2:

```
compatibleProductVersions: {  
  min: "11.1.7",  
  max: "11.2.2" // (and/or)  
}
```

### Global context vs individual context

You can configure `compatibleProductVersion` in two contexts:

- **Global context:** Every extension is subject to the `compatibleProductVersion` setting. The `compatibleProductVersion` setting appears at the root of the `spec.json` file, before the extensions array.

For example, red box 1 in [Figure 1: spec.json file with compatibleProductVersion settings](#) contains a `compatibleProductVersion` setting applied to all extensions.

- **Individual context:** An individual extension is subject to your supported-versions declaration. The `compatibleProductVersion` setting appears in the extensions array.

For example, red boxes 2 and 3 in [Figure 1: spec.json file with compatibleProductVersion settings](#) contain `compatibleProductVersion` settings applied to a single extension.

### Example spec.json file

The following `spec.json` file contains both global and individual `compatibleProductVersion` settings.

In this fictional example, the extension is uploaded to Cognos Analytics version 11.2.4.

```

{
  "name": "Sample_Button_Website_2",
  "schemaVersion": "1.0",
  "compatibleProductVersion": {
    "min": "11.2.0",
    "max": "11.2.5".
  },
  "extensions": [{
    name: "myExtension1",
    "compatibleProductVersion": {
      "min": "11.2.0",
      "max": "11.2.2"
    }, {
    name: "myExtension2",
    "compatibleProductVersion": {
      "min": "11.2.3",
      "max": "11.2.5"
    }
  ]
}

```

Figure 7. spec.json file with compatibleProductVersion settings

### Process for checking the version compatibility

**Note:** When a compatibleProductVersion setting appears in both global and individual contexts, it must pass *both* version criteria checks in order for the extension to be supported in the current version of Cognos Analytics.

When the extension above is uploaded, Cognos Analytics checks the version compatibility in the following order:

1. Check the global compatibleProductVersion setting (see box 1):

- a. min value = 11.2.0, which is less than 11.2.4. Result=**Pass**
- b. max value = 11.2.5, which is greater than 11.2.4. Result=**Pass**

**Result:** Both values in the global compatibleProductVersion setting passed the compatibility check. Therefore, there is not a global constraint that all extensions are not supported. Because the global compatibility check passed, proceed to step **2**, the individual compatibility checks.

2. Check the individual compatibleProductVersion settings:

a. Check the setting for myExtension1 (see box 2):

- i) min value = 11.2.0, which is less than 11.2.4. Result=**Pass**
- ii) max value = 11.2.2, which is less than 11.2.4. Result=**Fail**

**Result:** Both values in this individual compatibleProductVersion setting did not pass the compatibility check. Therefore, the extension myExtension1 is *not* supported in Cognos Analytics release 11.2.4.

b. Check the setting for myExtension2 (see box 3):

- i) min value = 11.2.3, which is less than 11.2.4. Result=**Pass**
- ii) max value = 11.2.5, which is greater than 11.2.4. Result=**Pass**

**Result:** Both values in this individual compatibleProductVersion setting passed the compatibility check. Therefore, the extension myExtension2 is supported in Cognos Analytics release 11.2.4.

## Perspective

A perspective is a specific view within the product.

For example, when you are creating a dashboard object, you are in the dashboard perspective.

All of the [sample extensions](#) contain a perspective element in their `spec.json` file. The value of the perspective element indicates which views will use this extension. A value of `common` means that the extension is used for all views.

The current perspective is found in the URL in your browser:

`http://myserver:9300/bi/?perspective=dashboard&id=iC2094F0D0...`

Perspective examples

- Home: occurs when viewing the Welcome page, defined as `http://servername:9300/bi/?perspective=home`

**Important:** When you set `"perspective": "Home"` in an extension, your custom buttons appear in the Welcome page at `http://servername:9300/bi/?perspective=home`. However, if you also set a different Cognos Analytics page as your Home page (by clicking **Personal menu icon** > **Profile and settings** > **Settings**), your customizations won't appear when you log in to Cognos Analytics. In this case, you must use a different perspective in your extension.

- Content: occurs when viewing the Content page (e.g., navigating My Content, Team Content, or Samples)
- Dashboard: occurs when viewing or editing a dashboard.
- Authoring: occurs when viewing or editing a report.
- Story: occurs when viewing or editing a story.
- Explore: occurs when viewing/editing an exploration.
- Ca-modeller : occurs when viewing/editing a data module.
- CreateBoard : occurs on the first screen of dashboard creation, when choosing a template

## Creating views

The IBM Cognos Analytics with Watson user interface consists of views, such as home, sign-in, authoring, dashboard, and modeling. You can create custom views to augment the built-in views.

Views are defined in a `spec.json` file that is contained in the root of the view .zip file. Custom views also include an HTML `div` element that replaces the central pane of the Cognos Analytics user interface. Custom views can also add or remove menus and buttons from the Application and Navigation bars, or remove one or both of these bars altogether. The structure and contents of the `spec.json` file is described in [“spec.json description”](#) on page 249. The high-level structure of the file is show here.

```
{
  "name": "<name>",
  "schemaVersion": "2.0",
  "extensions": [
    {
      "perspective": "<view_name>",
      "type": "<home_or_login>",
      "excludeCommon": true,
      "features": [
        {
          "id": "<id>",
          "toolItems": [<tool_item1>, <tool_item2>, ...],
          "content": {
            "type": "<path_to_javascript_file>",
            "options": {
              ...
            }
          }
        }
      ],
      "cssStyles": [
        "<path_to_css_file>"
      ]
    }
  ]
}
```

```
}  
  }]  
}
```

Views are packaged as extensions and a view .zip file can contain extension elements as well. For example, the `SampleExtensionButtonOpenPerspective.zip` sample defines a custom view and also adds a button to the Navigation bar of the home view that displays the custom view.

The `content` element contains the path to, and the name of, the JavaScript file that runs in order to create the custom view. The `options` element contains any options required by the JavaScript file. The JavaScript files uses the Asynchronous module definition (AMD) API.

A special type of view is a sign-in view. This type of view allows you to create a custom sign-in page for Cognos Analytics. The value of the `type` element determines if a view is a sign-in view (value is `login`) or not (value is `home`).

Unlike extensions, views have to be explicitly invoked in order for them to open. There are three ways to invoke a view.

- A button or menu item can be defined to open the view.
- The view can be opened by using a URL as follows.

```
http://<server>:<port>/bi/?perspective=<view_name>
```

- The view can be set to be the default home view for a user or for a role, or for all users. For more information, see [“Applying themes, extensions, and views” on page 247](#).

## Sample views

The following examples are available that illustrate the use of views.

These sample files are installed with the product in an Easy Installation, and are an option in a Custom Installation. After product installation, you can find them in the `installation_location/samples/extensions` folder.

### **SampleLogin.zip**

A replacement view for the Cognos Analytics sign-in page.

### **SampleLoginMultiple.zip**

A replacement view for the Cognos Analytics sign-in page that prompts the user for a namespace.

### **SampleWelcome.zip**

A replacement view for the Cognos Analytics welcome page.

## Using the customized welcome view

This task shows you how to install and use the custom welcome view.

### Procedure

Upload the **Samples\_for\_Install** deployment archive. (If not already done.)

1. Use **Manage > Administration console** to open **IBM Cognos Administration**.
2. On the **Configuration** tab, click **Content Administration**.
3. On the toolbar, click the **New Import** button.
4. Select **Samples\_for\_Install** in the first step of the **New Import** wizard and complete the remaining steps of the wizard.

Upload the sample extensions.

5. In the **Manage > Customizations** slide-out panel, select the **Extensions** tab, click **Upload extension** () , browse to the `<installation_location>/samples/extensions` folder, and select `SampleWelcome.zip`.
6. Repeat the preceding step for `SampleExtensionsAll.zip`.

7. In your web browser, type `<webserver_name>:<port_number>/bi/?perspective=sampleWelcome` to view the customized welcome view.

## Results

The customized welcome view is shown here. It has a new menu (**Quick links**) on the application bar and new buttons on the navigation bar (**Line dashboard**, **QTD revenue**, **2016 reports**, and **Website**). The **Notifications** button on the navigation bar is removed. The main screen has a new image, new text, and a link to a video.



## Using the customized sign-in view

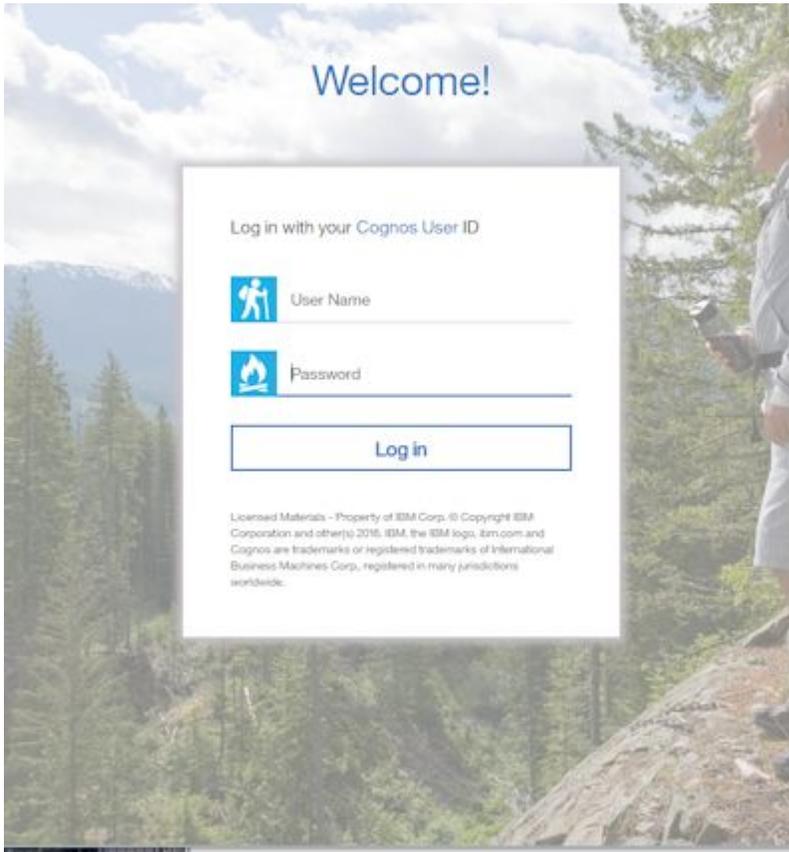
This task shows you how to install and use the custom sign-in view.

### Procedure

1. Extract the files in `SampleLogin.zip`.
2. Edit `login/js/views/SampleLoginView.js` and locate the line that contains `{name: 'CAMNamespace', value: 'CognosEx'}`.
3. Replace `CognosEx` with the name of one of your authentication namespaces (as defined in **IBM Cognos Configuration**).
4. Save `SampleLoginView.js` and re-create the `.zip` file.
5. In the **Manage > Customizations** slide-out panel, select the **Extensions** tab, click **Upload extension** (↑), browse to the `<installation_location>/samples/extensions` folder, and select `SampleLogin.zip`.
6. On the **Views** tab, click > next to the default sign-in view. Select the **Sample login** view as the default sign-in view.
7. Sign out of IBM Cognos Analytics with Watson.
8. Access your Cognos Analytics server.

## Results

The customized sign-in view is shown here. It has a customized background and new text in the sign-in dialog box.



## Creating a view (other than a sign-in view)

The `SampleWelcome.zip` sample is an example of a view that replaces the built-in home view with an alternate version that includes branding for the **Sample Outdoors Company**.

The `SampleWelcome.zip` sample contains a `spec.json` file that defines the view. This file is shown here.

```
{
  "name": "Sample_Welcome",
  "schemaVersion": "2.0",
  "extensions": [
    {
      "perspective": "Sample welcome",
      "type": "home",
      "features": [
        {
          "id": "com.sample.welcome",
          "excludeItems": ["com.ibm.bi.glass.common.cognosLogo"],
          "toolItems": [
            {
              "id": "brandLogoHomePage",
              "containerId": "com.ibm.bi.glass.appbarLeadingGroup",
              "type": "bi/glass/app/plugins/GlassPlugin",
              "class": "cognosIcon cognosLogo",
              "label": "theme.current.brandTextSmall",
              "icon": "theme.current.images.brandIconSmall",
              "weight": 995
            }
          ],
          "content": {
            "type": "v1/ext/Sample_Welcome/js/views/SampleWelcomeView",
            "options": {
              "info": {
                "title": "Sample welcome",
                "icon": "v1/ext/Sample_Welcome/images/bee_blue.svg"
              }
            }
          }
        }
      ],
      "cssStyles": [
        "v1/ext/Sample_Welcome/css/SampleWelcomeCSS.css"
      ]
    }
  ]
}
```

```
}]
}
```

The view is referred to as `Sample_welcome` in the managing customization panels. The `spec.json` file links to a `SampleWelcomeView.js` file in the `js/views` subfolder of the view. The `"type": "home"` entry indicates this view can be set to be the default home view. The `cssStyles` element defines the `.css` file used when displaying the view.

The `SampleWelcomeView.js` file is shown here.

```
/**
 * Licensed Materials - Property of IBM
 *
 * IBM Cognos Products: BI Glass
 *
 * Copyright IBM Corp. 2015
 *
 * US Government Users Restricted Rights - Use, duplication or disclosure restricted
 * by GSA ADP Schedule Contract with IBM Corp.
 */
define(['q',
        'text!./SampleWelcomeView.html',
        ], function(Q, html) {
    'use strict';

    var ContentView = function(){

        /**
         * Called by the ApplicationController whenever this view is created
         *
         * @public
         * @returns {Promise} promise resolved to the root DOM element for this view.
         */
        this.open = function(context, options) {
            this.logger = context.logger;
            this.options = options;
            var deferred = Q.defer();

            var root = document.createElement('div');
            root.setAttribute('class', 'welcome');

            root.innerHTML = html;
            deferred.resolve(root);
            return deferred.promise;
        };

        /**
         * Called by the ApplicationController whenever this view is destroyed
         *
         * @public
         */
        this.close = function() {
            this.logger.info('close');
        };

        /**
         * Called by the ApplicationController whenever this view is shown
         *
         * @public
         */
        this.onShow = function() {
            this.logger.info('onShow');
        };

        /**
         * Called by the ApplicationController whenever this view is hidden
         *
         * @public
         */
        this.onHide = function() {
            this.logger.info('onHide');
        };

        /**
         * Called by the ApplicationController whenever display Info is required for this view
         *
         * @public
         * @returns {Object} displayInfo - The displayInfo for this view.
         * @returns {string} displayInfo.title - The title.
         */
    };
});
```

```

    * @returns {string} displayInfo.icon - The icon.
    */
    this.getDisplayInfo = function() {
        this.logger.info('getDisplayInfo');
        return {
            'title':this.options.info.title,
            'icon': this.options.info.icon
        };
    };
};

return ContentView;
});

```

This file refers to the `SampleWelcomeView.html` that is displayed when the view is invoked.

This JavaScript code uses the View API in a JavaScript AMD module. This implementation uses the JavaScript Q library. The View API consists of the following methods.

#### **promise open(content, options)**

This method is invoked when the view is opened. It returns a Q promise object with the DOM element that represents the view as the resolved value.

##### **context**

Contains the context object.

##### **options**

Contains the options included in the `spec.json` file.

#### **void close()**

Invoked just before closing the view.

#### **void onShow()**

Invoked just before showing the view.

#### **void onHide()**

Invoked just before hiding the view.

#### **getDisplayInfo()**

Returns the title and associated icon of the view.

## Creating a sign-in view

With a custom sign-in view, you can replace the default IBM Cognos Analytics with Watson sign-in page. You can use your own branding and make other changes to the sign-in page.

A high-level overview of the structure of the JavaScript required to perform a sign-in is shown here.

The `SampleLogin.zip` sample is an example of a view that replace the built-in sign-in view with an alternate version. The `SampleWelcome.zip` sample contains a `spec.json` file that defines the view. This file is shown here.

```

{
  "name": "Sample_Login",
  "schemaVersion": "2.0",
  "extensions": [{
    "perspective": "sampleLogin",
    "type": "login",
    "excludeCommon": true,
    "features": [{
      "id": "com.sample.login",
      "toolItems": [],
      "content": {
        "type": "v1/ext/Sample_Login/login/js/views/SampleLoginView",
        "options": {
          "info": {
            "title": "Sample login"
          }
        }
      }
    }
  ]
},
  "cssStyles": ["v1/ext/Sample_Login/login/css/SampleLoginCSS.css"]
}]

```

```

    }]
  }
}

```

This spec.json file is similar to the same file for the SampleWelcome.zip sample except that the value of the type element is login and the Application and Navigation bars are excluded from this view.

A high-level overview of the structure of the JavaScript required to perform a sign-in is shown here.

```

/**
 * @typedef {Object} LoginError
 * @property {string} message - error message
 */
/**
 * performs a login
 *
 * @public
 * @param {Object[]} loginPrompts - object containing the login prompts
 * @param {string} loginPrompts[].name - name of the login prompt
 * @param {string} loginPrompts[].value - value of the login prompt
 * @return {Promise<undefined|LoginError>} promise resolved with no object when
 * the login is successful, rejected with an error when it fails.
 */
signin: function(loginPrompts)

```

The SampleLoginView.js file is shown here.

```

/**
 * Licensed Materials - Property of IBM
 * IBM Cognos Products: BI Glass
 * Copyright IBM Corp. 2017
 * US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP
 * Schedule Contract with IBM Corp.
 */
define(['q',
  'text!./SampleLoginView.html',
  ], function(Q, html) {
  'use strict';

  var ContentView = function() {

    /**
     * Called by the ApplicationController whenever this view is created
     *
     * @public
     * @returns {Promise} promise resolved to the root DOM element for this view.
     */
    this.open = function(context, options) {
      this.logger = context.logger;
      this.options = options;
      var deferred = Q.defer();

      var root = document.createElement('div');
      root.setAttribute('class', 'welcome');

      root.innerHTML = html;

      var loginBtn = root.getElementsByClassName('sample.loginBtn')[0];
      loginBtn.onclick = function() {
        document.getElementsByClassName('sampleIncorrectLoginText')[0].innerHTML='';
        var uid = document.getElementsByClassName('sample.username')[0].value;
        var pwd = document.getElementsByClassName('sample.password')[0].value;
        var loginPrompts = [
          {name: 'CAMNamespace', value: 'CognosEx'},
          {name: 'h_CAM_action', value: 'logonAs'},
          {name: 'CAMUsername', value: uid},
          {name: 'CAMPASSWORD', value: pwd}
        ];
        this.signin(loginPrompts).catch(this._loginError.bind(this));
      }.bind(this);

      deferred.resolve(root);
      return deferred.promise;
    },

    /**
     * Called by the ApplicationController whenever this view is destroyed
     *

```

```

    * @public
    */
    this.close = function() {
        this.logger.info('close');
    },

    /**
     * Called by the ApplicationController whenever this view is shown
     *
     * @public
     */
    this.onShow = function() {
        this.logger.info('onShow');
    },

    /**
     *
     * The live code below retrieves the product's error message.
     * If you would like to include your own error message, use the following commented
code instead:
     *
     * this._loginError = function() {
     *     document.getElementsByClassName('sampleIncorrectLoginText')[0].innerHTML='You
have entered an invalid username/password combination.';
     *     this.logger.error('loginError',arguments);
     * },
     *
     *
     */
    this._loginError = function(error) {
        document.getElementsByClassName('sampleIncorrectLoginText')
[0].innerHTML=error.message;
        this.logger.error('loginError',arguments);
    },

    /**
     * Called by the ApplicationController whenever this view is hidden
     *
     * @public
     */
    this.onHide = function() {
        this.logger.info('onHide');
    },

    /**
     * Called by the ApplicationController whenever display Info is required for this view
     *
     * @public
     * @returns {Object} displayInfo - The displayInfo for this view.
     * @returns {string} displayInfo.title - The title.
     * @returns {string} displayInfo.icon - The icon.
     */
    this.getDisplayInfo = function() {
        this.logger.info('getDisplayInfo');
        return {
            'title':this.options.info.title,
            'icon': this.options.info.icon
        };
    }
}

};

return ContentView;

});

```

A sign-in view uses one additional method.

### **promise login(credentials)**

This method submits a sign-in request and returns a promise object that is rejected if the sign-in attempt fails.

#### **credentials**

Contains the sign-in information.

```

[{'name':'CAMNamespace',value:'<namespace>'},
{'name':'h_CAM_action',value:'logonAs'}],

```

```
{name: 'CAMUsername', value: <username>},  
{name: 'CAMPASSWORD', value: <password>}]
```

## Creating a sign-in view with a namespace prompt

Using a custom sign-in view with a namespace prompt, you can replace the default IBM Cognos Analytics with Watson sign-in page. You can specify that the user must select from a list of namespaces when signing in. You can also use your own branding and make other changes to the sign-in page.

A high-level overview of the structure of the JavaScript required to perform a sign-in is shown here.

The `SampleLoginMultiple.zip` sample is an example of a view that replace the built-in sign-in view with an alternate version. The `SampleLoginMultiple.zip` sample contains a `spec.json` file that defines the view. This file is shown here.

```
{  
  "name": "Sample_Login_Multiple",  
  "schemaVersion": "2.0",  
  "extensions": [{  
    "perspective": "sampleLoginMultiple",  
    "type": "login",  
    "excludeCommon": true,  
    "features": [{  
      "id": "com.sample.login.multiple",  
      "toolItems": [],  
      "content": {  
        "type": "v1/ext/Sample_Login_Multiple/login/js/views/SampleLoginView",  
        "options": {  
          "info": {  
            "title": "Sample login namespaces"  
          }  
        }  
      }  
    }  
  },  
  {  
    "cssStyles": ["v1/ext/Sample_Login_Multiple/login/css/SampleLoginCSS.css"]  
  }  
}]  
}
```

This `spec.json` file is similar to the same file for the `SampleLogin.zip` sample in that the Application and Navigation bars are excluded from this view.

**Updated: June 8th, 2022.** `SampleLoginMultiple.zip` has been updated to include a fourth option in the namespace dropdown that can be used for OIDC non-ROPC-based namespaces. When selected, it hides the User ID/Password fields as they are not required.

## Applying themes, extensions, and views

You manage themes, extensions, and views with the **Managing > Customization** slide-out panel. You can upload, delete, and modify themes, extensions, and views. You can also set a default theme for all users, and set default home and sign-in views.

The **Managing > Customization** slide-out panel has four tabs, **Themes**, **Extensions**, **Views**, and **Parameters**. You upload themes on the **Themes** tab, and you upload extensions and views on the **Extensions** tab.

### Uploading themes

To upload a theme, on the **Themes** tab, click **Upload theme** () and browse to the theme in the file system. The theme is uploaded and validated. If the theme is invalid, an error message is displayed. Otherwise, the theme is added to the list of available themes. To see the theme you added, refresh your browser.

You can click **More** () next to a theme, to update, delete, or download the theme.

**Tip:** If you apply a theme to a distributed environment, wait at least five minutes for it to take effect.

## Setting a default theme

You can select a theme to be the default theme for all users. On the **Themes** tab of the **Managing > Customization** slide-out panel, select the check box next to a theme, and then click **Apply**.

You can also set default themes for roles in the **Manage > Accounts** slide-out panel. If a user has a role which has a default theme, that theme is used instead of the theme selected for all users. For more information, see [“Customizing roles” on page 7](#).

## Uploading extensions and views

To upload an extension or a view, on the **Extensions** tab, click **Upload extension** () and browse to the extension or view in the file system. The extension or view is uploaded and validated. If the extension is invalid, an error message is displayed. Otherwise, the extension is added to the list of uploaded themes. To see the extension you added, refresh your browser.

You can click **More** () next to an extension or view to update, delete, or download the extension or view.

**Note:** An extension can be coded for use only with specific versions of Cognos Analytics. If you upload such an extension and your Cognos Analytics version does not meet the version criteria, the following message appears in the alerts banner the next time you log in:

```
Some or all features of extension your_extension_name may be disabled due to a failed check on property compatibleProductVersion.
```

## Setting a default home view

On the **Views** tab of the **Managing > Customization** slide-out panel, click  next to the default home view. You can now browse for a dashboard or report to be the default home view, or you can select a view in the list of home views to be the default home view for all users.

You can also set default home views for roles in the **Manage > Accounts** slide-out panel. If a user has a role which has a default home view, that view is used instead of the home view selected for all users. For more information, see [“Customizing roles” on page 7](#).

A user can also select a personal default home view from any view. In any view, a user can click **More** () and then click **Set as home** to define a personal default home view. This default home view takes precedence over default home views created for roles or all users.

## Setting a default sign-in view

On the **Views** tab of the **Managing > Customization** slide-out panel, click  next to the default sign-in view. You can now select a view in the list of sign-in views to be the default sign-in view for all users.

## Running Cognos Analytics with customized extensions and views disabled

If an uploaded extension or view contains errors, it can render IBM Cognos Analytics with Watson unusable. In this case, you can run Cognos Analytics with customized extensions and views disabled.

### Procedure

Start Cognos Analytics by typing the URL `<webserver_name>:<port_number>/bi/?factoryMode=true`.

### Results

Cognos Analytics starts with all extensions disabled. You can now correct or delete your customized extensions or views before you restart Cognos Analytics with the standard URL.

## spec.json description

The `spec.json` file in an extension defines the additions and deletions the extension makes to the default IBM Cognos Analytics with Watson user interface. The structure and contents of this file are explained here.

The structure and contents that are described here are provisional. They can change in future releases of Cognos Analytics. These changes may not be backward compatible.

### **name**

Specifies the name of the extension. The name can contain alphanumeric characters, underscores (`_`), and spaces ().

### **schemaVersion**

Specifies a numeric value for the schema version. Can be `1.0` or `2.0`. The default value is `1.0`.

### **extensions**

Contains an array of perspective objects.

#### **perspective**

Specifies the view that is being extended. The options are the following.

##### **common**

Applies to all views.

##### **<view\_name>**

Applies to the `<view_name>` view, which can be a built-in view (home, authoring, dashboard, or modeller) or an uploaded view.

#### **type**

If the extension is a view, specifies the type. The possible values are `login` for a sign-in view and `home` for a home view. This element is only used in schema version 2.0. If it is omitted and schema version 2.0 is specified, then the view is not included in the list of possible default home or sign-in views.

#### **excludeCommon**

Specifies whether view contributions are received from the `/common` folder. The possible values are `false` to receive all contributions or `true` to receive no contributions. Any missing contributions can be added to the extension.

#### **lensable**

If `false`, this view is not included in the list of views for which features can be omitted. For more information, see [“Customizing roles” on page 7](#).

The default value is `true`.

#### **comment**

An optional comment.

#### **features**

Contains an array of feature groupings.

##### **id**

Specifies the unique identifier of the feature.

#### **toolItems**

Contains an array of user interface elements that are being added.

##### **id**

The unique identifier for the new user interface element.

##### **containerId**

Specifies the placement of the user interface element.

- If the user interface element is a menu or a button, the element is located in the application or navigation bars.

The values of `containerId` corresponding to the button or menu placement are shown in the following list.

1. `com.ibm.bi.glass.navbarLeadingGroup`
2. `com.ibm.bi.glass.navbarTrailingGroup`
3. `com.ibm.bi.glass.appbarLeadingGroup`
4. `com.ibm.bi.glass.appbarCenterGroup`
5. `com.ibm.bi.glass.appbarTrailingGroup`

- If the user interface element is a menu item, the value of `containerId` is the id of the menu that contains the menu item.

**label**

Specifies the text label for the user interface element. This text cannot be localized.

**type**

Specifies the user interface element type. The possible values are shown here.

- Button
- Menu
- MenuItem

**icon**

Specifies the user interface element image to be displayed. The path is relative to the image file in the extension zip archive.

**weight**

Specifies a numeric value that determines the placement of the user interface element in the container. A higher value moves up the element in the container.

**push**

Specifies whether when the button is pressed a second time, the action of the first press is undone. For example, opening and then closing a folder. The value can be `true` or `false`. The value must be `true` for a button that opens a folder.

**coachMark**

Specifies a coach mark.

**title**

Specifies the title of the coach mark.

**contents**

Specifies the contents of the coach mark.

**actionController**

Specifies the action to be taken when the user interface element is clicked. The available actions are listed here.

**bi/glass/api/IFrameOpener**

Opens a web page.

**bi/glass/api/ReportOpener**

Opens a particular report.

**bi/glass/api/DashboardOpener**

Opens a particular dashboard.

**bi/glass/api/FolderOpener**

Opens a particular folder.

**v1/ext/<name>/js/controllers/controller\_name**

Runs the custom controller that is packaged in the extension. The controller is the file `js/controllers/controller_name.js`.

**options**

Contains an array of options to pass to the action controller. The options vary depending on which action controller is used. For the options used by the built-in action controllers, see [“Using built-in action controllers”](#) on page 226.

**collectionItems**

Contains an array of user interface elements that are being added.

**containerId**

Specifies where the user interface element is located.

**id**

Specifies the unique identifier of the user interface element.

**content**

Contains definitions for a view.

**type**

Contains a link to the JavaScript file to run when this view is invoked.

**options**

Contains parameters to be passed to the JavaScript file.

**cssStyles**

Contains an array of links to .css files to be used for this view.

**excludeFeatures**

Contains an array of ids of user interface features to exclude. This feature cannot be applied to the common view.

**excludeItems**

Contains an array of ids of user interface items to exclude. This feature cannot be applied to the common view.

## JSON schema validation

When you upload a spec .json file, it is validated against the following schema.

```
{
  "type": "object",
  "definitions": {
    "extType": {
      "type": "string",
      "minLength": 1,
      "pattern": "^v1/ext/.+ $"
    },
    "noEmptyString": {
      "type": "string",
      "minLength": 1
    },
    "toolItem": {
      "type": "object",
      "properties": {
        "id": {
          "$ref": "#/definitions/noEmptyString"
        },
        "title": {
          "type": "string"
        },
        "type": {
          "$ref": "#/definitions/noEmptyString"
        },
        "actionController": {
          "$ref": "#/definitions/noEmptyString"
        },
        "label": {
          "$ref": "#/definitions/noEmptyString"
        },
        "containerId": {
          "$ref": "#/definitions/noEmptyString"
        },
        "icon": {
          "type": "string"
        },
        "weight": {
          "type": "number"
        },
        "class": {
          "type": "string"
        }
      }
    }
  }
}
```

```

    "comment": {
      "type": "string"
    },
    "options": {
      "type": "object"
    },
    "push": {
      "type": "string",
      "enum": [
        "true",
        "false"
      ]
    },
    "coachMark": {
      "type": "object",
      "properties": {
        "title": {
          "type": "string"
        },
        "contents": {
          "type": "string"
        }
      },
      "additionalProperties": false,
      "required": [
        "title"
      ]
    },
    "lensable": {
      "type": "boolean"
    }
  },
  "required": [
    "id"
  ]
},
"collectionItem": {
  "type": "object",
  "properties": {
    "id": {
      "$ref": "#/definitions/noEmptyString"
    },
    "containerId": {
      "$ref": "#/definitions/noEmptyString"
    },
    "label": {
      "$ref": "#/definitions/noEmptyString"
    },
    "lensable": {
      "type": "boolean"
    }
  },
  "required": [
    "id",
    "containerId"
  ]
},
"collectionContainerItem": {
  "type": "object",
  "properties": {
    "id": {
      "$ref": "#/definitions/noEmptyString"
    },
    "label": {
      "$ref": "#/definitions/noEmptyString"
    },
    "lensable": {
      "type": "boolean"
    }
  },
  "required": [
    "id"
  ]
},
"collectionContainer": {
  "type": "object",
  "properties": {
    "id": {
      "$ref": "#/definitions/noEmptyString"
    },
    "items": {
      "type": "array",

```

```

        "items": {
          "$ref": "#/definitions/collectionContainerItem"
        }
      },
      "lensable": {
        "type": "boolean"
      }
    },
    "additionalProperties": false,
    "required": [
      "id"
    ]
  },
  "feature": {
    "type": "object",
    "properties": {
      "id": {
        "$ref": "#/definitions/noEmptyString"
      },
      "excludeItems": {
        "type": "array",
        "items": {
          "$ref": "#/definitions/noEmptyString"
        }
      },
      "excludeFeatures": {
        "type": "array",
        "items": {
          "$ref": "#/definitions/noEmptyString"
        }
      },
      "toolItems": {
        "type": "array",
        "items": {
          "$ref": "#/definitions/toolItem"
        }
      },
      "content": {
        "type": "object",
        "properties": {
          "type": {
            "$ref": "#/definitions/extType"
          },
          "options": {
            "type": "object"
          }
        }
      },
      "additionalProperties": false,
      "required": [
        "type"
      ]
    },
    "cssStyles": {
      "type": "array",
      "items": {
        "$ref": "#/definitions/extType"
      }
    },
    "collectionItems": {
      "type": "array",
      "items": {
        "$ref": "#/definitions/collectionItem"
      }
    },
    "collectionContainers": {
      "type": "array",
      "items": {
        "$ref": "#/definitions/collectionContainer"
      }
    },
    "comment": {
      "type": "string"
    },
    "lensable": {
      "type": "boolean"
    }
  },
  "additionalProperties": false,
  "required": [
    "id"
  ]
},

```

```

"extension": {
  "type": "object",
  "properties": {
    "perspective": {
      "$ref": "#/definitions/noEmptyString"
    },
    "features": {
      "type": "array",
      "minItems": 1,
      "items": {
        "$ref": "#/definitions/feature"
      }
    },
    "type": {
      "type": "string",
      "enum": [
        "home",
        "login"
      ]
    },
    "excludeCommon": {
      "type": "string",
      "enum": [
        "true",
        "false"
      ]
    },
    "lensable": {
      "type": "boolean",
      "default": true
    },
    "comment": {
      "type": "string"
    }
  },
  "additionalProperties": false
},
"properties": {
  "schemaVersion": {
    "type": "string",
    "enum": [
      "1.0",
      "2.0"
    ]
  },
  "name": {
    "type": "string",
    "pattern": "[a-zA-Z0-9_ ]+ $"
  },
  "extensions": {
    "type": "array",
    "minItems": 1,
    "items": {
      "$ref": "#/definitions/extension"
    }
  },
  "comment": {
    "type": "string"
  }
},
"additionalProperties": false,
"required": [
  "name",
  "extensions"
]
}

```

## Creating a global color palette

**11.1.0** Administrators can create global color palettes that are available to report, dashboard, and story authors.

### About this task

You can create the following types of color palettes:

## Categories

Used for visualizations that support discrete colors, like a bar or pie chart.

## Continuous

Used for visualizations that support color transitions, like a map or a heat map.

Some visualizations support both types of color palettes. For example, if you drop a measure on to the color slot of a bar chart, you can add a color gradient to the bars for that measure. The following visualizations support both types of color palettes:

- Bar, floating bar, stacked bar
- Floating column, stacked column
- Bubble, packed bubble, hierarchical packed bubble
- Marimekko
- Radial
- Scatter plot
- Tree map

Color palettes are grouped into the following categories:

### Custom

Created by a user (report, dashboard, or story author). Available only to the user who created them. For more information about custom palettes, see *Creating a color palette* in the *Dashboards and Stories Guide*.

### Global

Created by the system administrator. A global palette is available to all users but only an administrator can modify it. A user can duplicate a global palette and then modify the duplicated version.

### System

Default palettes available in IBM Cognos Analytics with Watson. A system palette can't be changed but a user can duplicate it and then modify the duplicated version.

## Procedure

1. Click **Manage > Customization**, and then select the **Palettes** tab.
2. Click the plus sign icon **+**.

The **Create color palette** window opens with the categorical view showing.

3. To create a continuous color palette, click the Continuous palette icon .
4. Enter a name for your palette.
5. Click the **Grid** or **Wheel** tab.

In the **Grid** tab, you can select colors from a grid of color swatches. In the **Wheel** tab, you can select a color by doing one of the following things:

- Clicking the color wheel
  - Typing the color in HSB (hue, saturation, brightness) or RGB (red, green, blue) notation
  - Typing the color in hex code
6. Under **Color guide**, click **Automatic** or **Custom**.

### Categorical color palette

Contains a set of swatches. In **Automatic**, when you select a color from the grid or wheel, all swatches in the palette are filled with colors that are related to the color you selected, starting from the currently selected swatch. In **Custom**, you must select each swatch and then select a color for it.

### Continuous color palette

Contains one continuous swatch. In **Custom**, when you select a color from the grid or wheel, the swatch is filled with the color you selected. The color gradually increases in intensity from one end of the swatch to the other. **Automatic** is not available for a continuous color palette.

7. To undo a selection, click the **Remove swatch** icon .
8. To add more swatches to the palette, click **Add swatch** .
9. To reverse the colors in the palette, click **Reverse palette** .
10. Click **Save** when you are finished.

### Results

The color palette appears under **Global** and is available to all report, dashboard, and story authors.

## 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.

For more information, see [Chapter 1, “Managing people,” on page 1..](#)

### 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. Click **Manage > Customization**, and then select the **Profiles** tab.
2. Update any settings in the **Regional options** section that you want to change.
3. To change the default location for uploaded files, click  next to **Default upload location**.  
**Tip:** By default, uploaded files are saved in **My content**. When the upload was initiated from a specific folder in **Team content** or **My content**, the files can be saved to that folder.  
If you specify a new shared location in **Team content** for uploaded files at the role, tenant, or global level, users can save the uploaded files to this new default location.
4. If you want to change the permissions of the default user profile:
  - a) Click **Permissions > Edit**.
  - b) Click  or the Remove selected item icon  to add or remove users, groups, or roles to the default user profile.
  - c) Click  for a user, group, or role and then select **Read, Run, Write, or Full**, as necessary.

5. Click **Apply**.

## Results

Each user who logs on to IBM Cognos software for the first time will automatically inherit these settings but can change them later.

## Viewing or changing a user profile

You can view or change a user profile.

### About this task

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.

### Procedure

1. Click **Manage > People**, and then select **Accounts**.
2. Click the namespace that contains the user.
3. Click the name of the user whose preferences you want to view or change.
4. Click the **General**, **Personal**, or **Permissions** tabs to view or change the settings.
5. Click away from the slide-out panel to exit.

The slide-out panel closes. If you made changes, the message **username was edited.** appears.

## 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 Analytics.

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. Click **Manage > People**, and then select **Accounts**.
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. For more information, see [“Finding users, groups, and roles” on page 17](#).
4. Click the More icon  next to the user's name and then select  **Delete profile**.
5. Click **OK** to confirm you want to delete the user's profile.

## Results

When the user next logs on, they will be assigned the current default user profile. They can later modify their own profile if they wish.

## 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. Click **Manage > People**, and then select **Accounts**.
2. Click the namespace that contains the user.
3. Find the source user whose user profile you want to copy. You can use the Search feature to find a user. For more information, see [“Finding users, groups, and roles” on page 17](#).
4. Click the More icon  next to the user's name and then select  **Copy user profile**.
5. Select the settings that you want to copy:
  - regional settings and view options
  - all content in the user's **My content** folder
  - any [portal pages](#) that the user may have migrated from a old version of Cognos Business Intelligence.

**Tip:** For information about enabling My portal pages, see [“Configuring appearance” on page 95](#).

6. Specify whether you want the user profile of the source user to be deleted after you finish copying it to other users.
7. Click **Next**.
8. Select one or more target users who you want to receive the copied user profile and then click **Add**.  
**Tip:** To select multiple users, hold down the Ctrl key while you click each user's name.
9. If you want, on the **Summary** page, change any settings, including the source and target users.
10. Click **Apply**.

## Setting global parameters

---

Administrators can set global parameters that can be used across reports by all roles.

**Note:** You can also set default report parameters for specific roles in the **Manage > Accounts** slide-out panel. If a user has a role with customized parameters, when they run any report with those parameters, they will see the default values that you set. For more information, see [“Customizing roles” on page 7](#).

### Procedure

1. Go to **Manage > Customization**, and select the **Parameters** tab.
2. Depending on the version of Cognos Analytics, perform one of the following steps:
  - In version 11.1.4 and later, click the **New** link, and type the parameter name in the space provided. Press **Enter** on the keyboard.
  - In version 11.1.3 and earlier, click the **Import** link, and import the parameter from your report, located in either **My content** or **Team content**.
3. From the parameter context menu , click **Properties**.
4. Specify a custom label for the parameter. To specify a language-specific label, next to **Languages**, click **Set**. You can also add a description of the parameter, or disable it.
5. **11.1.4** Select the **Applied to all roles** check box.

When you select this property, all system and tenant user roles can use this parameter.

**Tip:** If you are a Cognos Analytics on-premises user, and want to customize this parameter for specific roles, don't select the **Applied to all roles** check box. Instead, proceed to step 6.

6. Customize the parameter for specific roles in the following way:
  - a) In **Manage > People**, select the **Accounts** tab.
  - b) Locate the role for which you want to customize this parameter, and in the role **Properties** panel, select the **Customization** tab.
  - c) Next to **Parameters**, click **Settings**.
  - d) Select the check box next to the parameter that you specified in step 2.  
Click **OK** to finish setting this parameter without changing the default value. To set a specific value, select the **Set values** link, change the value, and then click **Apply**.
  - e) If needed, repeat steps b to d for other roles. The parameter values that you select can be different for different roles.
7. Log out, and log back in.

### Results

Report authors can use the **My parameters**  pane to tailor reports according to their role and to maintain consistency across reports.

## Setting the `_as_of_date` global parameter

You can set up the global parameter `_as_of_date`, and make it available to all system and tenant roles. The on-premises administrators can customize this parameter for specific user roles.

### Procedure

1. Go to **Manage > Customization**, and select the **Parameters** tab.
2. Depending on the version of Cognos Analytics, perform one of the following steps:
  - In version 11.1.4 and later, click the **New** link, and type `_as_of_date` in the space provided. Press **Enter** on the keyboard. Alternatively, click the **Import** link, and import the `_as_of_date` parameter from the sample "Global parameter date picker" report. This report is located in **Team content > Calendars > Tools**.
  - In version 11.1.3 and earlier, click the **Import** link, and import the `_as_of_date` parameter from the sample "Global parameter date picker" report. This report is located in **Team content > Samples > Relative dates > Tools**.
3. From the `_as_of_date` parameter context menu , click **Properties**.
4. Specify a custom label for the parameter. To specify a language-specific label, next to **Languages**, click **Set**. You can also add a description of the parameter, or disable it.
5. Select the **Applied to all roles** checkbox.

When you select this property, all system and tenant user roles can use this parameter.

If you are a Cognos Analytics on-premises user, and want to customize this parameter for specific roles, don't select the **Applied to all roles** checkbox. Instead, proceed to step 6.

6. Customize the `as_of_date` parameter for specific roles in the following way:
  - a) In **Manage > People**, select the **Accounts** tab.
  - b) Locate the role for which you want to customize this parameter, and in the role **Properties** panel, select the **Customization** tab.
  - c) Next to **Parameters**, click **Settings**.
  - d) Select the checkbox next to the `_as_of_date` parameter that you specified in step 2.

Click **OK** to finish setting this parameter without changing the default date, which is the current date. To set a specific date, select the **Set values** link, select the date, and click **Apply**.
  - e) If needed, repeat steps b to d for other roles. The date that you select can be different for different roles.
7. Log out, and log back in.

### Results

All users in the system or tenant can now see the **My Parameters** dialog box, and the `_as_of_date` parameter is available to users when they run reports or dashboards that include the relative date filters and measures. The users can customize this parameter for their needs. For more information, see "Customizing the reference date" in the *Cognos Analytics Modeling Guide*.

# Chapter 10. Managing cloud storage

You can configure Cognos Analytics to connect to a cloud storage service that is offered by a third party company. Cognos Analytics users can then save their reports to the cloud.

To manage cloud storage, you must be assigned the **Manage connections** secured function, which is associated with the Save to Cloud capability. For more information, see [“Save to Cloud” on page 156](#).

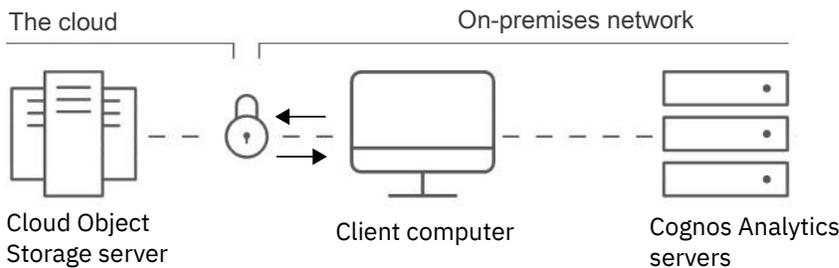
## Cloud storage at a glance

Cloud storage, also known as Cloud Object Storage (COS), is a technology that companies offer as a service to other companies or applications.

**First**, as the administrator, you [create an instance of a storage service with a Cloud Object Storage provider](#).

**Second**, you [configure a storage connection in Cognos Analytics](#) that is integrated with the Cloud Object Storage service.

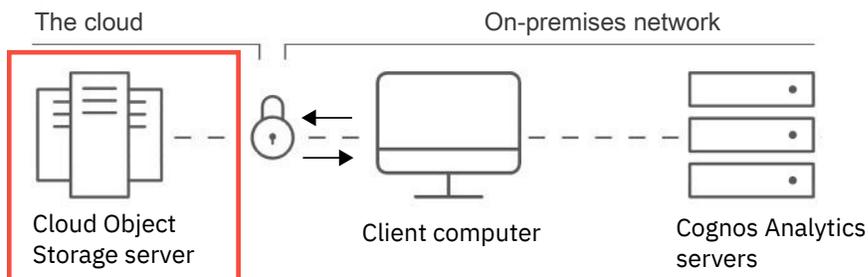
The integration of Cognos Analytics servers and a Cloud Object Storage server is shown in this diagram:



## Creating a connection with a Cloud Object Storage provider

Create a connection with a Cloud Object Storage provider to establish a storage service that you can then integrate with Cognos Analytics.

This is the first stage in enabling the save to cloud feature in Cognos Analytics.



**Choose the company that you want as your Cloud Object Storage provider:**

- [IBM](#)
- [Amazon](#)
- [MinIO](#)
- [Google](#)

## Creating an IBM storage connection

Create a connection to an IBM Cloud Object Storage (COS) service so that Cognos Analytics users can save their reports on the cloud.

For an overview of the IBM COS service, see [About IBM Cloud Object Storage](https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-about-cloud-object-storage) (https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-about-cloud-object-storage).

### Step 1: Create an IBM Cloud Platform account

Create an [IBM Cloud Platform account](https://cloud.ibm.com/docs/services/cloud-object-storage/basics?topic=cloud-object-storage-provision#provision-account) (https://cloud.ibm.com/docs/services/cloud-object-storage/basics?topic=cloud-object-storage-provision#provision-account).

### Step 2: Create a COS service instance

Create a service instance (https://cloud.ibm.com/docs/services/cloud-object-storage/basics?topic=cloud-object-storage-provision#provision-instance).

#### Tips for Cognos Analytics administrators:

- Initially, a COS service instance has no service credentials. Before you can configure Cognos Analytics to connect to your Cloud Object Storage service, you must assign it a service credential.

### Step 3: Create your service credentials

Create your COS service credentials (https://cloud.ibm.com/docs/services/cloud-object-storage?topic=cloud-object-storage-service-credentials).

#### Tips for Cognos Analytics administrators:

- Make a note of the values of the COS properties listed in the following table. You will need these values later when you configure Cognos Analytics to [connect to this IBM Cloud Object Storage connection](#).

Property in IBM COS service credentials	Related property when you configure Cognos Analytics
apikey	Access Key ID
resource_instance_id	Secret access key

### Step 4: Create a bucket

Create some buckets to store your data (https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-getting-started-cloud-object-storage).

#### Tips for Cognos Analytics administrators:

- Choose a predefined, standard bucket
- When you create a bucket you select a **Resiliency** value, for example: `Regional`, and then a **Location** value, for example: `eu-gb`.

#### Important:

Make a note of the **Location** value. You must select this same value later when you configure Cognos Analytics to [add a location to your connection](#).

## Creating an Amazon storage connection

Create a connection to an Amazon Simple Storage Service (S3) so that Cognos Analytics users can save their reports on the cloud.

For an overview of Amazon Simple Storage Service (S3), see [Amazon S3 Basics](https://docs.aws.amazon.com/AmazonS3/latest/gsg/AmazonS3Basics.html) on the Amazon Web Services (AWS) web site (<https://docs.aws.amazon.com/AmazonS3/latest/gsg/AmazonS3Basics.html>).

### Step 1: Create an AWS account

Create an Amazon Web Services (AWS) account on the AWS web site (<https://portal.aws.amazon.com/billing/signup#/start>).

### Step 2: Create an Amazon S3 service

Create an Amazon Simple Storage Service (S3) on the AWS web site (<https://docs.aws.amazon.com/AmazonS3/latest/gsg/SigningUpforS3.html>).

### Step 3: Create your service credentials

Create a new access key and secret access key (<https://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html#create-aws-access-key>) as part of your service credentials.

#### Tips for Cognos Analytics administrators:

- Even if you already have an access key, you must create a new one so that you can also record your secret access key.
- Make a note of the values of the AWS properties listed in the following table. You will need these values later when you configure Cognos Analytics to [connect to this IBM Cloud Object Storage connection](#).

Property in Amazon Web Services (AWS) Management Console	Related property when you configure Cognos Analytics
AWSAccessKeyId	Access Key ID
AWSSecretKey	Secret access key

### Step 4: Create a bucket

Create a Bucket on the AWS web site (<https://docs.aws.amazon.com/AmazonS3/latest/gsg/CreatingABucket.html>).

#### Tips for Cognos Analytics administrators:

- Choose a predefined, standard bucket.
- When you create a bucket you select a region, for example: Asia Pacific (Tokyo).

#### Important:

Make a note of the region. You must select this same value later when you configure Cognos Analytics to [add a location to your connection](#).

- If you want to encrypt your bucket with server side encryption, you can edit the permissions for the bucket by specifying this customer master key (CMK):

```
x-amz-server-side-encryption: AES256
```

For more information, see [Protecting data using server-side encryption with Amazon S3-managed encryption keys \(SSE-S3\)](#)

## Creating a MinIO storage connection

Create a connection to a MinIO Storage environment so that Cognos Analytics users can save their reports on the cloud.

For an overview of MinIO Object Storage server, see [MinIO](https://www.ibm.com/support/knowledgecenter/SSBS6K_3.1.2/manage_cluster/minio.html). (https://www.ibm.com/support/knowledgecenter/SSBS6K\_3.1.2/manage\_cluster/minio.html).

### Step 1: Install MinIO

Install MinIO (<https://docs.min.io/docs/minio-quickstart-guide>).

### Step 2: Run MinIO

**Note:** For details, see the [MinIO Quickstart Guide](https://docs.min.io/docs/minio-quickstart-guide.html) (https://docs.min.io/docs/minio-quickstart-guide.html).

#### Example of retrieving MinIO parameters

In this example, we install MinIO on Windows and note the values that are required to configure Cognos Analytics:

1. Install MinIO server on a Windows computer.
2. Create a folder C:\my\_data\_folder.
3. In a command line window, cd to the directory where you installed MinIO server.
4. Type `minio.exe server C:\my_data_folder`.

A list of parameters for your MinIO instance appears in the command window.

5. To configure Cognos Analytics later, make a note of these parameters:

- Access key
- Secret access key
- Endpoint

**Tip:** You will use these values to [create a MinIO storage connection in Cognos Analytics](#).

### Step 3: Create a bucket

#### Example

1. Enter the MinIO endpoint URL that you noted previously in a browser window.  
The MinIO browser appears.
2. Enter the access key and secret access key that you noted previously.
3. Follow the instructions to create a bucket.

## Creating a Google Cloud Platform storage connection

Create a connection to a Google Cloud Platform (GCP) S3 storage connection so that Cognos Analytics users can save their reports on the cloud.

For more information about GCP storage connections, see [Cloud Storage Overview](https://cloud.google.com/storage/docs) (https://cloud.google.com/storage/docs).

### Step 1: Create a Google Cloud Platform account

1. Go to the [Google Cloud Platform](https://console.cloud.google.com) page (https://console.cloud.google.com).
2. Follow the instructions to create a GCP account.

## Step 2: Create a project

1. Go to the [Project selector page](https://console.cloud.google.com/projectselector2) (https://console.cloud.google.com/projectselector2)
2. Click **CREATE PROJECT**.
3. Enter a project name and then click **CREATE**.

## Step 3: Create a storage service account

1. In the Navigation menu, select **Storage** to go to your [Storage browser page](https://console.cloud.google.com/storage/browser) (https://console.cloud.google.com/storage/browser)
2. Click **Enable Billing**, if you haven't already enabled billing.
3. Click **CREATE SERVICE ACCOUNT**.
  - a. Enter a service account name and description.

**Note:** The **Service account ID** field is populated automatically.
  - b. Click **CREATE**.
  - c. Grant the service account access to your project.
  - d. Grant users access to the service account.
  - e. Click **DONE**.

## Step 4: Create an HMAC key

Create an HMAC key for your service account.

1. In the Google Cloud console, go to the Cloud Storage **Buckets** page.
2. Click **Settings**.
3. Select the **Interoperability** tab.
4. In the **Request endpoint** section, copy and save in a text file the value in the **Storage URI** field.

**Note:** You will use this value when you create the storage connection in Cognos Analytics.
5. Click **+ Create a key for a service account**.
6. Select the service account you want the HMAC key to be associated with.
7. Click **Create key**.
8. Copy and save in the text file the values of these two fields:

- **Access key**
- **Secret**

**Note:** You will use these values when you create the storage connection in Cognos Analytics.

Property in GCP service credentials	Related property when you configure Cognos Analytics
Access key	Access key ID
Secret	Secret access key
Storage URI	Service endpoint

## Step 5: Create a bucket

Follow the steps in [Creating storage buckets](#).

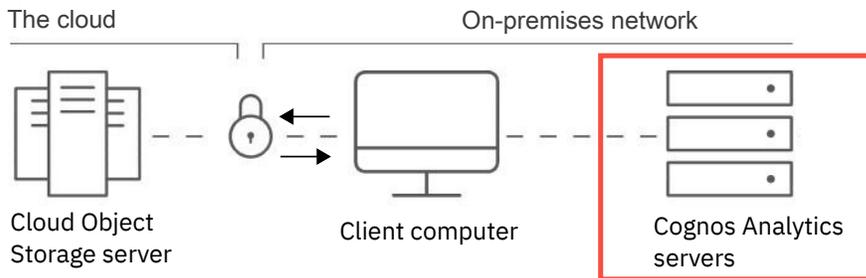
### Tips for Cognos Analytics administrators:

- When you select from the **Location** list, make a note of the region. You must select this same value later when you configure Cognos Analytics to add a location to your connection.
- In the **Access control** field, choose **Uniform**, so that all content in the bucket has the same permissions.
- In the **Advanced settings (optional) > Encryption** field, select **Google-managed key**, and then click **CREATE**.

## Creating a storage connection in Cognos Analytics

Create a storage connection in Cognos Analytics to integrate an existing cloud storage service with Cognos Analytics.

This is the second stage in configuring Cognos Analytics to save to cloud.



### Before you begin

You must set up a storage service with a Cloud Object Storage provider before you can configure Cognos Analytics to connect to it.

### Procedure

1. Click **Manage > Storage**.

The **Cloud storage** page appears. If any connections exist, they appear in the **Connection list**.

2. Click **Create connection** + .
3. Enter a name for your connection.
4. In the **Type** field, select the cloud object storage provider with which you created a connection.
5. Enter the access key ID and the secret access key.

**Tip:** These values were generated when you created your credentials in your cloud object storage account. For more information, see “Determining the access key ID and the secret access key” on page 267.

6. If you have an Amazon Cloud Object Storage connection with server side encryption, enter this customer master key (CMK) in the **Headers** field:

```
x-amz-server-side-encryption: AES256
```

Amazon supports many other customer master keys (CMKs). To view these keys, sign in to the AWS Management Console and open the AWS Key Management Service (AWS KMS) console at <https://console.aws.amazon.com/kms>.

For more information, see Protecting data using server-side encryption with Amazon S3-managed encryption keys (SSE-S3)

7. If you selected **Other** in the **Type** field, enter the MinIo service endpoint.

**Tip:** For more information, see “Determining the service endpoint (MinIO only)” on page 268

8. Click **Test** ▷.

-  **Test success** indicates that the connection is configured properly.
  -  **Test failed** indicates that the connection is not configured properly. Try [this solution](#).
9. Click **Create and continue**.

The connection is created and the wizard advances to the **Add location** page.

## What to do next

Your next step is to [add a location to the connection that you just created](#).

## Determining the access key ID and the secret access key

You must find out the access key ID and the secret access key for your storage provider before you can configure Cognos Analytics to connect to the storage service.

Choose the procedure for your storage object provider:

- [IBM](#)
- [Amazon](#)
- [MinIO](#)

### Procedure for IBM Cloud Object Storage

1. If you haven't yet done so, [create your service credentials](#).
  - a. Log in to the IBM Cloud console and navigate to your instance of Object Storage.
  - b. In the side navigation, click **Service Credentials**.
  - c. Click **New credential** and provide the necessary information. If you want to generate HMAC credentials, click on **Advanced Options** to reveal the 'Include HMAC Credential' option. Verify the option is selected before continuing.
  - d. Click **Add** to generate service credential.
2. Make a note of the values of the COS properties listed in the following table. You will need these values later when you configure Cognos Analytics to [connect to this IBM Cloud Object Storage connection](#).

<i>Table 89. IBM COS access key and secret access key</i>	
<b>Property in IBM COS service credentials</b>	<b>Related property when you configure Cognos Analytics</b>
apikey	<b>Access Key ID</b>
resource_instance_id	<b>Secret access key</b>

### Procedure for Amazon Simple Storage Service

1. [Create a new access key and secret access key](https://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html#create-aws-access-key) (https://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html#create-aws-access-key) as part of your service credentials.

**Tip:** If you previously created an access key but did not record the secret access key, you must create a new one and record the new secret access key.

2. Make a note of the values of the AWS properties listed in the following table. You will need these values later when you configure Cognos Analytics to [connect to this IBM Cloud Object Storage connection](#).

<i>Table 90. AWS access key and secret access key</i>	
<b>Property in Amazon Web Services (AWS) Management Console</b>	<b>Related property when you configure Cognos Analytics</b>
AWSAccessKeyId	<b>Access Key ID</b>
AWSecretKey	<b>Secret access key</b>

## Procedure for MinIO

In this example, we install MinIO on Windows and note the values that are required to configure Cognos Analytics:

1. Install MinIO server on a Windows computer.
2. Create a folder C:\my\_data\_folder.
3. In a command line window, cd to the directory where you installed MinIO server.
4. Type `minio.exe server C:\my_data_folder`.

A list of parameters for your MinIO instance appears in the command window.

5. To configure Cognos Analytics later, make a note of these parameters:
  - Access key
  - Secret access key
  - Endpoint

## Determining the service endpoint (MinIO only)

The service endpoint is a URL that is required when you configure Cognos Analytics to connect to a MinIO storage environment.

In the following example, we install MinIO on Windows and note the Endpoint value.

### Procedure

1. Install MinIO server on a Windows computer.
2. Create a folder C:\my\_data\_folder.
3. In a command line window, cd to the directory where you installed MinIO server.
4. Type `minio.exe server C:\my_data_folder`.

A list of parameters for your MinIO instance appears in the command window.

5. Make a note of the Endpoint value.

### What to do next

You will enter the Endpoint value in the **Service endpoint** field when you [create a MinIO connection](#) in Cognos Analytics.

## Managing the connection list

After you create one or more connections, view the connection list to check each connection's properties and status.

### Before you begin

You must have [created at least one connection](#).

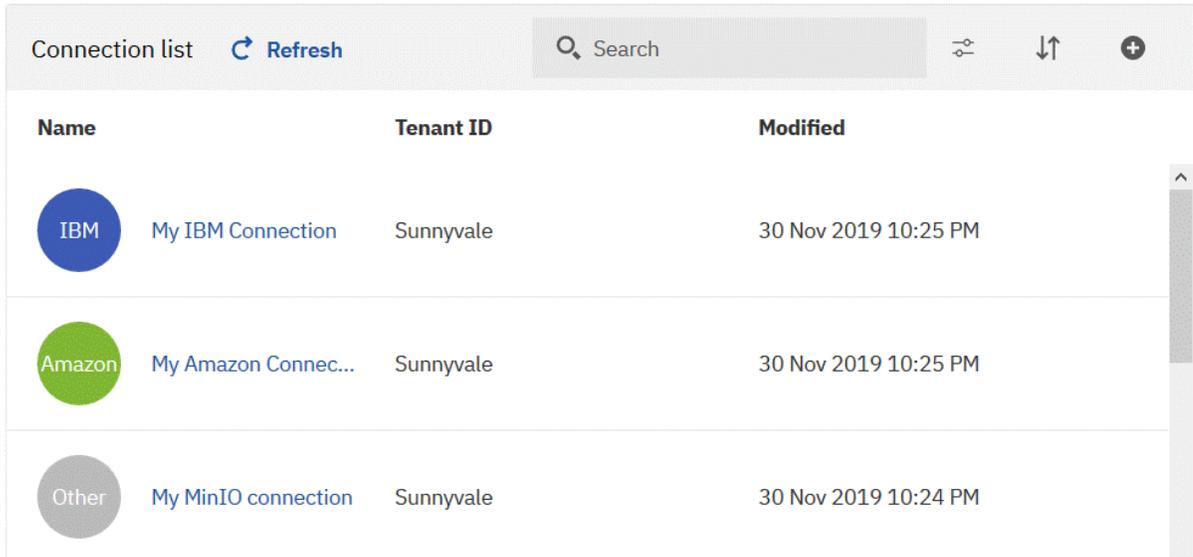
## Procedure

1. Click **Manage > Storage**.

The **Connection list** appears.

For example, see the following figure:

### Cloud storage



Name	Tenant ID	Modified
 My IBM Connection	Sunnyvale	30 Nov 2019 10:25 PM
 My Amazon Connec...	Sunnyvale	30 Nov 2019 10:25 PM
 My MinIO connection	Sunnyvale	30 Nov 2019 10:24 PM

**Important:** You may need to clear your browser's cache if the **Modified** date and time is not updated correctly after you click **Refresh**.

In Firefox, open a private window. In Chrome, open an incognito window.

2. At the end of the row for your connection, click the ellipsis icon  and then click **Properties**.

A panel opens for the connection, showing the **General** tab.

- To grey out the connection name in the list and make the connection temporarily unavailable, click **Advanced** and then select the **Disable this entry** check box.

**Tip:** The connection between the Cognos Analytics server and the cloud storage service is not broken. If you deselect the check box, users can resume using the connection.

- To change the name of your connection, click the Edit icon  at the top of the panel and type a new name.

3. Click the **Connection** tab.

- To reset the **Access key ID** and **Secret access key** fields, first update the security credentials for your cloud storage service. Then determine the key values that you need to enter.

**Important:** For MinIO storage environments only, you must also update the Service Endpoint field in your MinIO cloud storage environment. For more information, see [“Determining the service endpoint \(MinIO only\)”](#) on page 268.

- Click **Test** , and then click **Save** to ensure that any changes you made keep the connection up and running.

4. To remove the connection from the list, click the ellipsis icon  at the end of the row, and then click **Delete**.

**Note:** The storage service that you created in the cloud storage environment is not affected by the removal of the Cognos Analytics storage connection.

## Adding a location to a connection

Add a location to your connection that will serve as a container for reports that are saved to cloud. The location in Cognos Analytics maps to a bucket that you created in your Cloud Object Storage environment.

### Procedure

1. Click **Manage > Storage**.

The **Cloud storage** page appears.

2. Click the connection to which you want to add a location.

The **Location list** page appears.

**Tip:** If this message appears:  Error accessing cloud storage connection '*connection\_name*', try [this solution](#).

3. Click the Create location icon **+** or, if no locations exist yet, click **Add location**.

The **Add location** page appears.

4. Enter a name for your location.

5. In the **Select bucket** field, select a bucket that you created using your [Cloud Object Storage service](#).

6. If you want, enter a key prefix.

**Tip: Key prefix** is an optional field that acts like a folder in your cloud object storage environment. If you do not enter a key prefix value, your objects are saved at the root of your bucket.

- **If you enter a key prefix for an Amazon S3 bucket, and a user saves a report to that bucket:**

- The report is copied to a folder in the bucket in the Amazon S3 environment.
- The folder name is the same as the key prefix value.

- **Example**

A Cognos Analytics user saves the report `Product line revenue` to the cloud, and selects an AWS service and a bucket that was assigned the key prefix value `Revenue`. The user selects **PDF** and **Excel** formats and **English (New Zealand)** as the language.

**Result**

The report output files `Product line revenue-en-nz.xlsx` and `Product line revenue-en-nz.pdf` appear in the Amazon Management Console, in the location **`aws_service_name/ aws_bucket_name/Revenue`**.

- **If you enter a key prefix for an IBM COS bucket, and a user saves a report to that bucket:**

- **Note:** A folder is **not** created in the bucket in the IBM COS console. Instead, the report appears in the list of bucket objects with `key_prefix_value/` prepended to the report name.

- **Example**

A Cognos Analytics user saves the report `Product line revenue` to the cloud, and selects an IBM COS service and a bucket that was assigned the key prefix value `Revenue`. The user selects **PDF** and **Excel** formats and **English (New Zealand)** as the language.

**Result**

The report output files `Revenue/Product line revenue-en-nz.xlsx` and `Revenue/Product line revenue-en-nz.pdf` appear in the IBM COS console, in the location **`ibm_cos__service_name/ibm_cos_bucket_name`**.

- **If you enter a key prefix for an MinIO bucket, and a user saves a report to that bucket:**

- The report is copied to a folder in the bucket in the MinIO browser.
- The folder name is the same as the key prefix value.

7. Select the region.

**Important:** You must choose the same region that was used when you created your bucket in your cloud object storage environment. For more information, see [“Determining the region for your Cognos Analytics bucket”](#) on page 271.

8. Click **Test** .

-  **Test success** indicates that the location is configured properly.
-  **Test failed** indicates that the location is not configured properly. Try [this solution](#).

## What to do next

After you add a location successfully, Cognos Analytics users can save their report output in this cloud location. For more information, see [“Saving output to cloud”](#) on page 273.

## Determining the region for your Cognos Analytics bucket

For AWS or IBM storage types, you must ensure that the region you select in your Cognos Analytics location matches the region or location that you chose when you created a bucket in your cloud storage environment.

Choose the procedure for your storage object provider:

- [IBM](#)
- [Amazon](#)

**Note:** MinIO storage configuration does not contain a region value.

### Steps for IBM Cloud Object Storage

1. Go to your [IBM Cloud Resource List](https://cloud.ibm.com/resources) (<https://cloud.ibm.com/resources>).
2. Expand **Storage** and click on your Cloud Object Storage (COS) service.  
A list appears showing the buckets for your COS service.
3. In the row for the bucket you want, find the value in the **Location** column.
4. Make a note of the **Location** value.

**Tip:** You will enter this value in the **Region** field when you [add an IBM location in Cognos Analytics](#).

### Steps for Amazon Simple Storage Service

1. Go to your [list of S3 buckets in the AWS Management Console](https://s3.console.aws.amazon.com/s3/home). (<https://s3.console.aws.amazon.com/s3/home>).
2. In the row for the bucket you want, find the value in the **Region** column.
3. Make a note of the **Region** value.

**Tip:** You will enter this value in the **Region** field when you [add an Amazon location in Cognos Analytics](#).

## Using a key prefix

If you want, you can specify a key prefix when you configure a bucket in Cognos Analytics. If you plan on storing many reports on the cloud, a key prefix provides a method of sorting many report objects into different categories.

A key prefix can result in different file structures of saved report output, depending on which storage solution you are using:

- **If you enter a key prefix for an Amazon S3 bucket, and a user saves a report to that bucket:**
  - The report is copied to a folder in the bucket in the Amazon S3 environment.
  - The folder name is the same as the key prefix value.

### – Example

A Cognos Analytics user saves the report `Product line revenue` to the cloud, and selects an AWS service and a bucket that was assigned the key prefix value `Revenue`. The user selects **PDF** and **Excel** formats and **English (New Zealand)** as the language.

### Result

The report output files `Product line revenue-en-nz.xlsx` and `Product line revenue-en-nz.pdf` appear in the Amazon Management Console, in the location **`aws_service_name/ aws_bucket_name/Revenue`**.

### • If you enter a key prefix for an IBM COS bucket, and a user saves a report to that bucket:

- **Note:** A folder is **not** created in the bucket in the IBM COS console. Instead, the report appears in the list of bucket objects with `key_prefix_value/` prepended to the report name.

### – Example

A Cognos Analytics user saves the report `Product line revenue` to the cloud, and selects an IBM COS service and a bucket that was assigned the key prefix value `Revenue`. The user selects **PDF** and **Excel** formats and **English (New Zealand)** as the language.

### Result

The report output files `Revenue/Product line revenue-en-nz.xlsx` and `Revenue/Product line revenue-en-nz.pdf` appear in the IBM COS console, in the location **`ibm_cos__service_name/ibm_cos_bucket_name`**.

### • If you enter a key prefix for an MinIO bucket, and a user saves a report to that bucket:

- The report is copied to a folder in the bucket in the MinIO browser.
- The folder name is the same as the key prefix value.

## Managing the location list

After you create one or more locations, view the location list to check each location's properties and status.

### Before you begin

You must have created at least one location.

### Procedure

1. Click **Manage > Storage**.

The **Connection list** appears.

2. Click a connection.

The **Location list** appears.

For example, see the following figure:



Location list		Refresh		Search		↓↑		+	
Name	Bucket	Region	Key prefix			Modified			
My profit margin	profitmargin	us-south						30 Nov 2019 10:39 PM	
My revenue	revenue	us-south						30 Nov 2019 10:39 PM	

3. Click a location.

4. At the end of the row for your location, click the ellipsis icon and then click **Properties**.

A panel opens for the location, showing the **General** tab.

- To grey out the location name in the list and make the location temporarily unavailable, click **Advanced** and then select the **Disable this entry** check box.

**Tip:** The connection between the Cognos Analytics server and the cloud storage service is not broken. If you deselect the check box, users can resume using the location.

- To change the name of your location, click the Edit icon at the top of the panel and type a new name.

5. Click the **Location** tab.

- If you want to switch to a different bucket, select it from the pulldown menu.

**Important:** For IBM and Amazon storage environments only, you must then select the region that you selected when you created the bucket in your cloud storage environment. For more information, see [“Determining the region for your Cognos Analytics bucket”](#) on page 271.

- If you want to add or modify a key prefix, enter the value in the **Key prefix** field. For more information, see [“Using a key prefix”](#) on page 271.

- Click **Test** , and then click **Save** to ensure that any changes you made keep the location up and running.

6. To remove the location from the list, click the ellipsis icon at the end of the row, and then click **Delete**.

**Note:** The storage service that you created in the cloud storage environment is not affected by the removal of the Cognos Analytics storage connection.

## Testing saved outputs to cloud

To test that you enabled cloud storage correctly, perform these tasks:

1. [Save a report to the cloud](#)
2. [Confirm that the output was saved to the cloud](#)

### Saving output to cloud

Save a report to cloud as the **first** step in testing that you enabled cloud storage correctly.

## Before you begin

Before you can save report output to the cloud, you must first create a connection with a [Cloud Object Storage provider](#) and then second [create a storage connection in Cognos Analytics](#).

## Procedure

1. In a folder, for the report that you want to run, click the Action menu icon  and then click **Run as**.
2. Select an output format.
3. Select **Run in background**, click **Advanced**, and then follow these steps:
  - a) Select **Now** for when you want the report to run.
  - b) In the **Languages** field, select one or more output languages.
  - c) In the **Delivery** field, select the **Save to cloud** check box and then click **Done**.
  - d) If you want, change the report name.  
For example, append the current date and time to the name.
  - e) Click the **Connection name** field and select a connection that you configured in Cognos Analytics.
  - f) Click the **Location name** field and select a location that you configured in the connection.
  - g) Click **Done**.
4. Click **Run**.

## Results

The report is saved to the cloud location.

## What to do next

Your next step is to [confirm that the output was saved to cloud](#).

## Confirming that output was saved to cloud

Confirming that output was saved to cloud is the **second** step in testing that you enabled cloud storage correctly.

## Before you begin

Ensure that you [saved a report to the cloud](#).

## Procedure

1. In the application bar, click the Personal menu icon , and then click **My schedules and subscriptions**.
2. Click **Schedule**, click the Type icon , and then click **Past**.  
The status (**Succeeded** or **Failed**) of the report run is shown in a list and on a graph.  
If the report ran successfully, but [could not be saved to the cloud](#), you may need to specify S3 header information.
3. To see additional details about the report run, click the Action menu icon  next to the listing, and then click **View versions**.
4. Click the Open details icon  for the report version.  
Additional information appears, such as:
  - **Start time** of the report run
  - **End time** of the report run

- **Starting upload** message for each version
  - **Finished upload** message for each version
5. To view the output, go to your [cloud storage location](#) and navigate to the bucket or folder in which you saved your Cognos Analytics output.
- Tip:** If you want users to view their saved output on the cloud, you must assign them appropriate permissions to access the cloud storage location.

### What to do next

After you confirm that Cognos Analytics output can be saved successfully to your cloud location, inform other Cognos Analytics users that they can use this feature.

## Troubleshooting cloud storage

---

You may encounter problems when managing cloud storage in Cognos Analytics.

This section describes some common issues and their potential solutions.

### Error accessing cloud storage connection

You try to create a location, but this error message appears:

 Error accessing cloud storage connection '*connection\_name*'.

#### Solution

Try these steps:

- Check that your access key and secret access key [match the current values](#) of your Cloud Object Storage connection.
- Click **Test**  to test your connection.
- Clear your cache, or open a Private window (in Firefox) or Incognito window (in Chrome), restart Cognos Analytics, and then try again to add a location.
- Check that your Cloud Storage environment is operating properly.

### Test failed

You click **Test**  to test your connection or location, but this message appears:

 Test failed

#### Solution

Try these steps:

- If your failed test was for a new location, ensure that you selected the correct region. The region must match the one you selected when you created a bucket in your Cloud Object Storage environment. For more information, see [“Determining the region for your Cognos Analytics bucket”](#) on page 271.

**Tip:** If you think you know what the correct region should be, select that region and try the test again.

- If your failed test was for a new connection, check that your connection parameters were entered correctly.
- Clear your cache, or open a Private window (in Firefox) or Incognito window (in Chrome), restart Cognos Analytics, and then try again to add a location or connection.
- Check that your Cloud Storage environment is operating properly.

## Cannot upload file to cloud

You try to upload a file to a cloud storage location, but the message `Error uploading report_name` appears.

For example, you try to upload a file to an Amazon S3 storage service. The following message appears:

```
Error uploading report_name. Part number must be an integer between 1
and 10000, inclusive (Service: Amazon S3; Status Code: 400; Error Code:
InvalidArgument; Request ID: request_id)
```

This message can occur if the default size of data chunks delivered to the cloud during file uploads is too small.

### Solution

To prevent this issue, you can [adjust the chunk size of uploaded files](#).

## S3 headers not specified in connection

You try to save a report to a cloud storage location. The report runs successfully. However, when you view the past activities for the report, you notice this error message:

```
RSV-SRV-0112 Saving report output to cloud storage failed.
Response was 403 Forbidden. {"details":["Access Denied (Service: Amazon
S3; Status Code: 403; Error Code: AccessDenied; Request ID:
16DF5762BAC17033)"],"error":"COS-002","message":"Error accessing cloud storage
location '1'.*}
```

This message indicates that the Cloud Storage Location where you wanted your report to be saved is configured with server-side encryption. However, your COS location does not contain the required encryption key in the S3 header.

### Solution

To prevent this issue, you must edit your COS location connection and add the following S3 header name-value pair:

```
s3:x-amz-server-side-encryption: AES256
```

---

# Chapter 11. Cognos Analytics on Cloud On-Demand

Cognos Analytics on Cloud on-Demand is a version of Cognos Analytics on Cloud that is available to you digitally, via self-service. The product is updated to the latest version upon availability. This offering has two tiers: Standard and Premium.

## Who should use Cognos Analytics on Cloud On-Demand?

You may want to register for Cognos Analytics on Cloud On-Demand if you meet these criteria:

- You are willing to connect to data sources only when connected through a [Secure Gateway](#) or to one of the [supported on Cloud databases](#).
- Your organization uses only one namespace.
- You are willing to authenticate using IBMid or with an identity provider that is [federated to IBMid](#).
- You are not an existing On-Demand customer.
- You are willing to migrate all of your content in one move. You cannot perform partial imports.

## Functionality

Supported databases can use SSL connections via imported certificates that are stored in the cloud. For more information, see [“Securing your data server connection using a cloud-based certificate”](#) on page 31.

For a full list of functions and whether they are supported by Cognos Analytics on Cloud On-Demand, see [Cognos Analytics offerings](#).

## Limitations

You should be aware that the Cognos Analytics on Cloud On-Demand offering has the following limitations:

- If you are [migrating from Cognos Analytics on Cloud Hosted](#):
  - Your capability settings are not transferred.
  - Default Cognos groups and roles are migrated. However, they lose all capabilities that were assigned to them.
  - If your default Cognos groups and roles were used to secure content, that security is maintained.
- You cannot secure certificates.
- Cognos Analytics on Demand does not support the following:
  - Jobs
  - IBM Cognos Administration console
  - Default Cognos groups and roles. You can create new custom roles. However, you can use them only to secure content; you cannot change the capabilities of a user, group, or role.
  - Images and fonts
  - Secure File Transfer Protocol (SFTP)
  - Framework Manager
  - Power cubes and Transformer
  - Compatible query mode (CQM)

# Migrating to Cognos Analytics on Cloud On-Demand

---

If you are the administrator of Cognos Analytics on Cloud Hosted environment, you may want to migrate to a Cognos Analytics on Cloud On-Demand environment.

## Before you begin

Review information about the [intended audience](#), [functionality](#), and [limitations](#) of Cognos Analytics On-Demand.

**Important:** You must be a member of the Directory Administrators role to perform this task.

## About this task

Some Cognos data is not transferred during migration:

- Your capability settings are not transferred.
- Default Cognos groups and roles are migrated. However, they lose all capabilities that were assigned to them.
- If your default Cognos groups and roles were used to secure content, that security is maintained.

## Procedure

1. Contact your IBM sales representative to discuss whether a Cognos Analytics on Demand subscription is a good fit for your organization.

**Tip:** If you decide to proceed with the migration, remember that you will be working closely with your sales rep. You will be informed whenever there is something that you need to do. When you have a question, your sales rep is your primary resource!

2. If your organization does not already authenticate using IBMid, you must federate your identity provider to IBMid before migration begins.

For more information, see [IBMid Enterprise Federation \(https://www.ibm.com/docs/en/ief\)](https://www.ibm.com/docs/en/ief).

3. Ensure that you receive an invitation to your on Demand subscription and that you complete these tasks:

- [Accept your invitation](#) as the on Demand subscription administrator.
- [Invite all of your users](#) to join the on Demand subscription.

**Note:** The users do not need to accept the invitations immediately. However, they must all be invited so that the IBM team can validate their IBMIDs.

4. In your Cognos Analytics Hosted environment, remove any content and user profiles that you don't want exported to your On-Demand environment.

5. If you want to import your samples to on Demand, rename the Samples folder.

6. Create a .csv file that contains information about every user in your namespace.

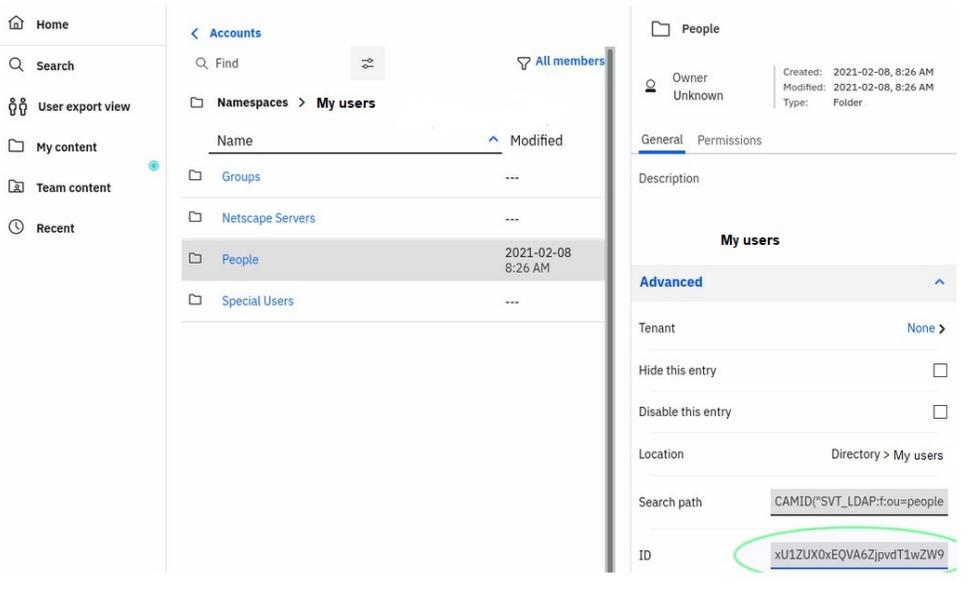
- a) Obtain the file `user-export-extension.zip` from your sales rep and copy it to your computer.
- b) Select **Manage > Customization** and then click the **Extensions** tab.

- c) Click the Upload extension icon  , navigate to the file `user-export-extension.zip`, and then click **Open**.

The name appears in the list of extensions.

- d) Log out and then log back in to Cognos Analytics for the extension to take effect.

The **User export view** category appears in the navigation bar.



- e) Click **User export view**, and then navigate to **Accounts > Namespaces > your\_namespace\_folder > People**
- f) In the People panel, under **your\_namespace\_folder**, copy the value in the **ID** field.
- g) Paste the **ID** value into the **Namespace ObjectID** field.

The **User export view** category appears in the navigation bar.



- h) Click **Query Users** to review the list of users.
    - Tip:** Remove or modify any users, as required.
  - i) Click **Download CSV** and save the .csv file to your computer.
  - j) Send the .csv file to the IBM team.
  - k) Remove the **User export view** extension after you are finished using it.
7. Create a deployment of your current environment:
- a) In **IBM Cognos Administration**, on the **Configuration** tab, click **Content Administration**.
  - b) On the toolbar, click the **New Export** icon .
  - c) Name the archive.

**Specify a name and description - New Export wizard**

Specify a name and location for the deployment specification. You can also specify a description.

**Name:**

**Description:**

**Screen tip:**

**Tenant:** None [Set...](#)

**Location:**  
 Administration  
[Select another location...](#)

- d) Select both **Select the entire content store** and **Include user account information** and then click **Next**.

**Choose a deployment method - New Export wizard**

Choose a deployment method.

**Deployment method:**

Select public folders, directory and library content  
 Select tenants  
 Select the entire Content Store  
 Include user account information

- e) Set an encryption password that you will give to the IBM team so that they can import the content, and then click **Next**.

**Specify a deployment archive - New Export wizard**

Select from the existing deployment archives or type a new deployment archive name. Select whether to encrypt the content of the archive.

**Deployment archive**

The location of the deployment archive is set using the deployment files location in IBM Cognos Configuration.

Entries: 1 - 3

	Name
<input type="radio"/>	IBM_Cognos_Audit
<input type="radio"/>	IBM_Cognos_Notebook_Samples
<input type="radio"/>	Samples_for_Install_11_1_7

**New archive:**

full content store deployment

**Encryption**

You can encrypt the content of the archive by setting a password. This password is required to decrypt the archive during import.

Encrypt the content of the archive

[Set the encryption password...](#)

Cancel < Back Next > Finish

- f) Review the summary information and click **Next**.
- g) Under **Action**, select **Save and run once** and then click **Finish**.

**Select an action - New Export wizard**

Select whether you want to run, schedule, or save only, when the wizard closes.

**Action:**

Save and run once

Save and schedule

Save only

Cancel < Back Next > Finish

A .zip deployment file is created in *installation\_location*/deployment.

- h) Copy the .zip deployment file and send it to the IBM team.

**Tip:** The IBM team will import this deployment to your On Demand environment.

8. If the IBM team discovers assets in your **Team content** folder without valid owners, they will send you a list of the invalid owners and ask you how to proceed.

If this happens, proceed as follows:

- a) Open the list in an editor.
  - b) Next to each invalid user name, enter the name of a valid user to whom the invalid user's content can be reassigned.
  - c) Send the list back to the IBM team.
9. After the IBM team informs you that the migration is complete, re-establish your data source connections by creating a Secure Gateway or by connecting to a supported database on the cloud.

# Managing your On-Demand subscription (for Subscription administrators)

If you are a designated Subscription administrator for IBM Cognos Analytics on Demand, you receive an email invitation to use the on Demand version. You can add and remove users to the subscription, assign users, upgrade your subscription, and manage other subscription details.

## Accepting an invitation to join a Cognos Analytics on Cloud on-Demand subscription

After you accept an email invitation to join an IBM Cognos Analytics on Demand subscription, you can log in to the subscription.

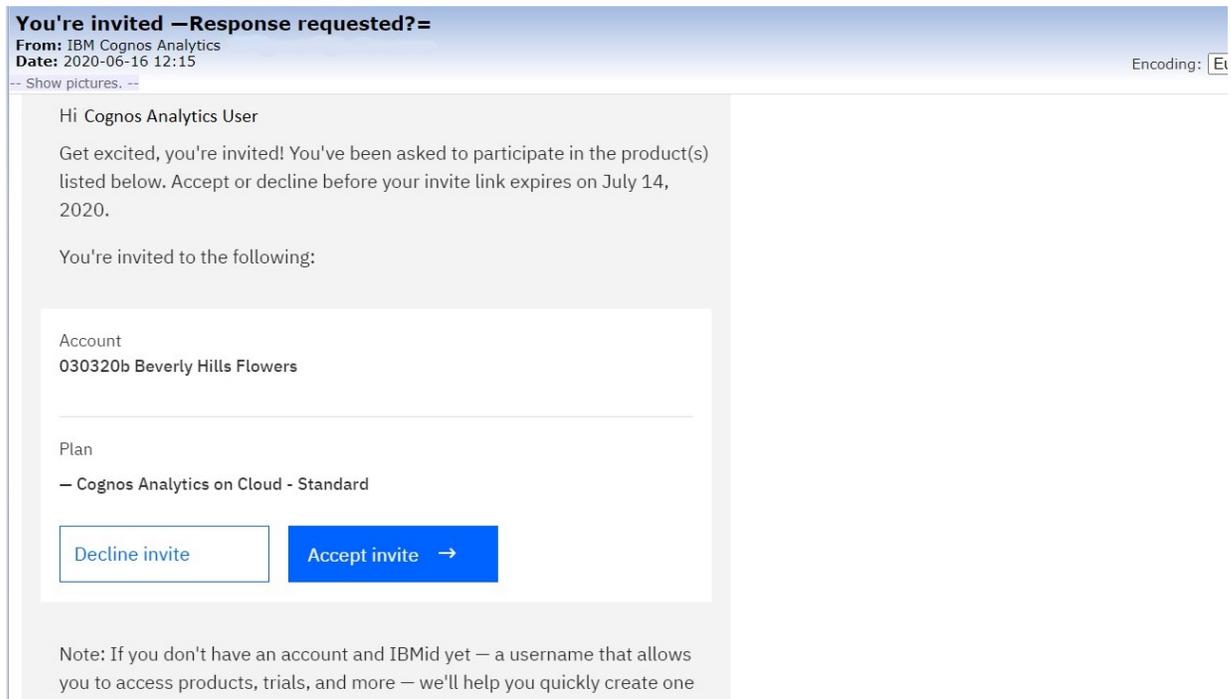
**Note:** The steps in this task are *mostly* the same for the two on Demand subscription roles:

- [Subscription administrators](#)
- [Licensed users](#)

If you receive an email from **IBM Cognos Analytics <noreply@us.ibm.com>** inviting you to use IBM Cognos Analytics on Demand, follow these steps:

### Procedure

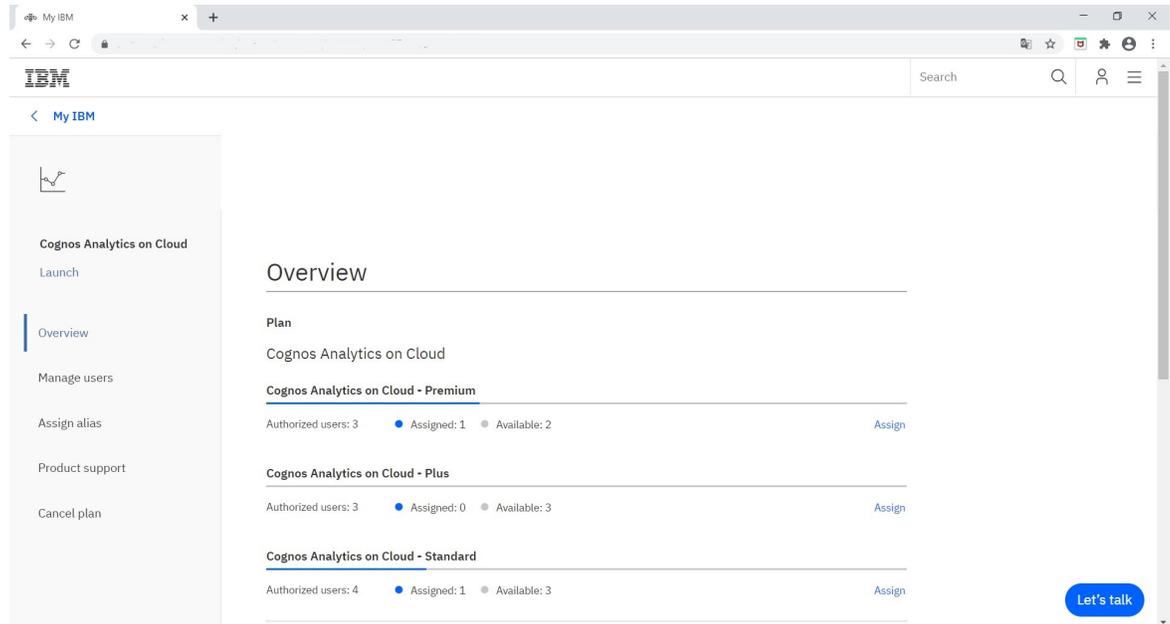
1. Open the invitation email and click **Accept invite**.



2. Log in with your IBM ID, if you have one. Otherwise, [create your IBM account now \(https://www.ibm.com/account/profile\)](https://www.ibm.com/account/profile).  
The IBM Cognos Analytics **Welcome** page appears.
3. If you are a License user, you can start using Cognos Analytics right away. For more information, see the *Getting Started Guide*.
4. If you want to view details about your subscription (if you are a License user) or manage the subscription (if you are a Subscription administrator), do the following:
  - a) Click the Personal menu icon  in the application bar.
  - b) Click **Manage product subscription**.

The **Overview** page for your IBM Cognos Analytics subscription appears.

- If you are a Subscription administrator, the **Overview** page looks like this:

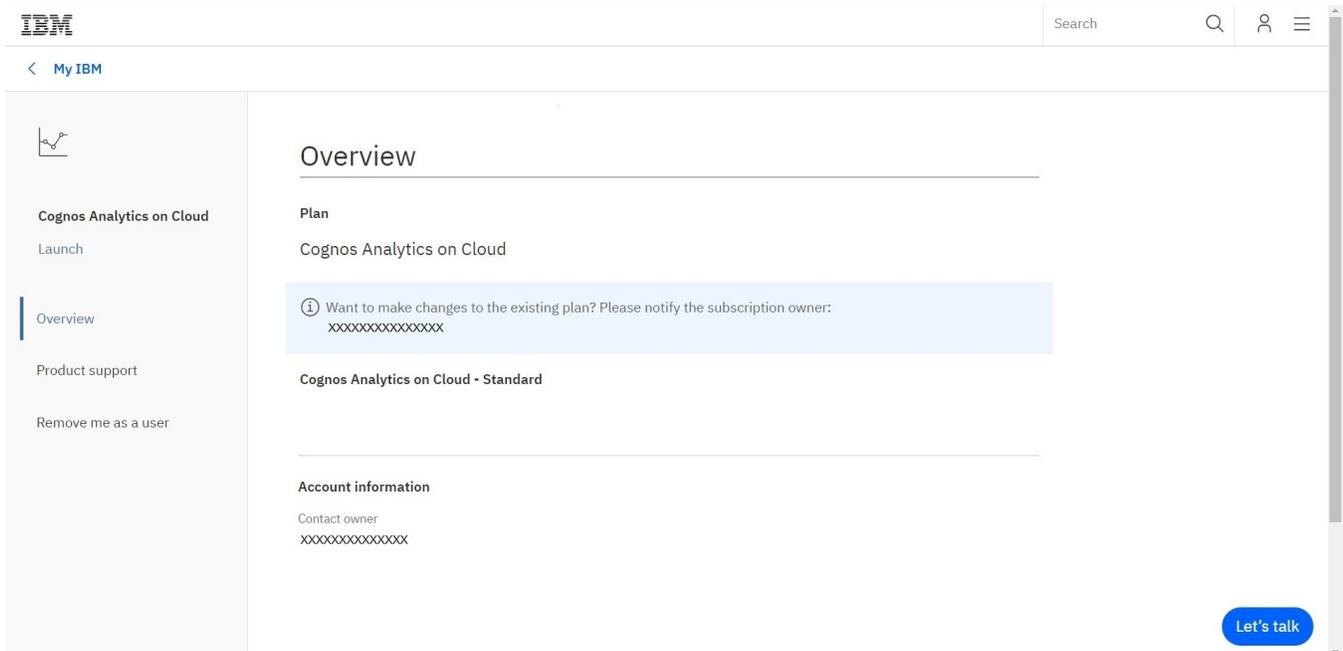


Three subscription levels appear:

- **Cognos Analytics on Cloud - Premium**
- **Cognos Analytics on Cloud - Plus**
- **Cognos Analytics on Cloud - Standard**

**Note:** To help you plan your user assignments, note the number of seats already **Assigned** and the number of seats still **Available** that are shown for the subscription you choose.

- If you are a License user, the **Overview** page looks like this:



**Note:** The License user does not see any subscription level information. As they are not a Subscription administrator, the License user cannot make any subscription changes or invite other users.

## Logging in to My IBM dashboard

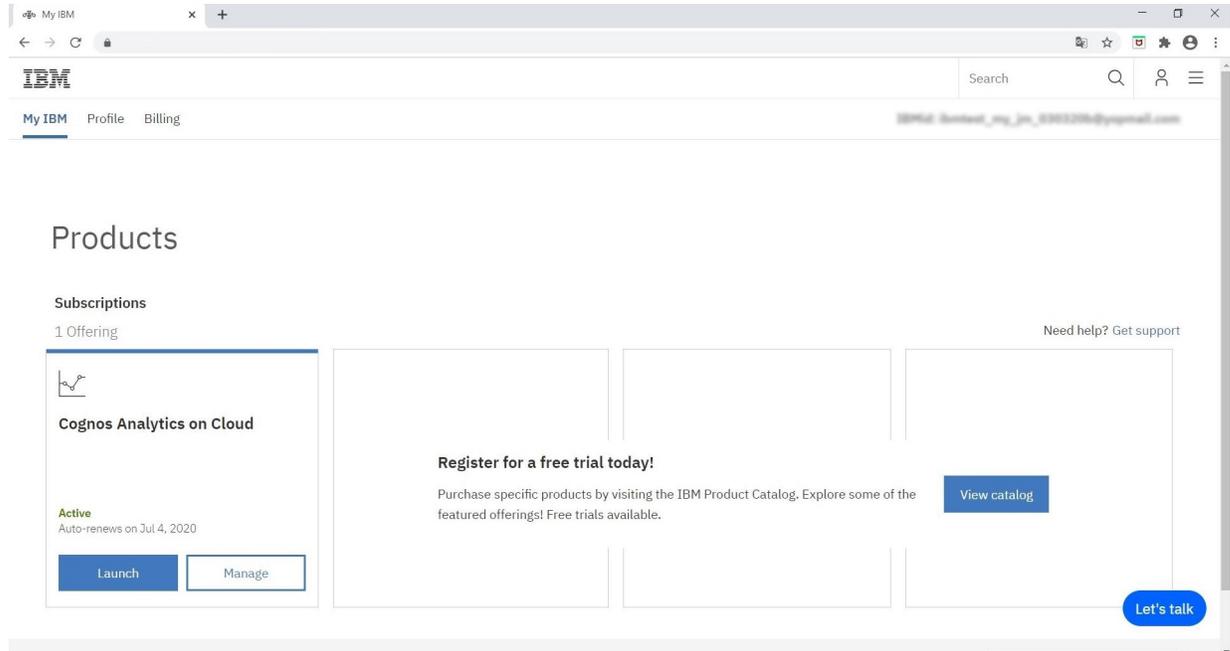
If you previously accepted the an email invitation and want to make changes to your subscription, you can log in to your My IBM Dashboard **Overview** page.

Follow these steps:

### Procedure

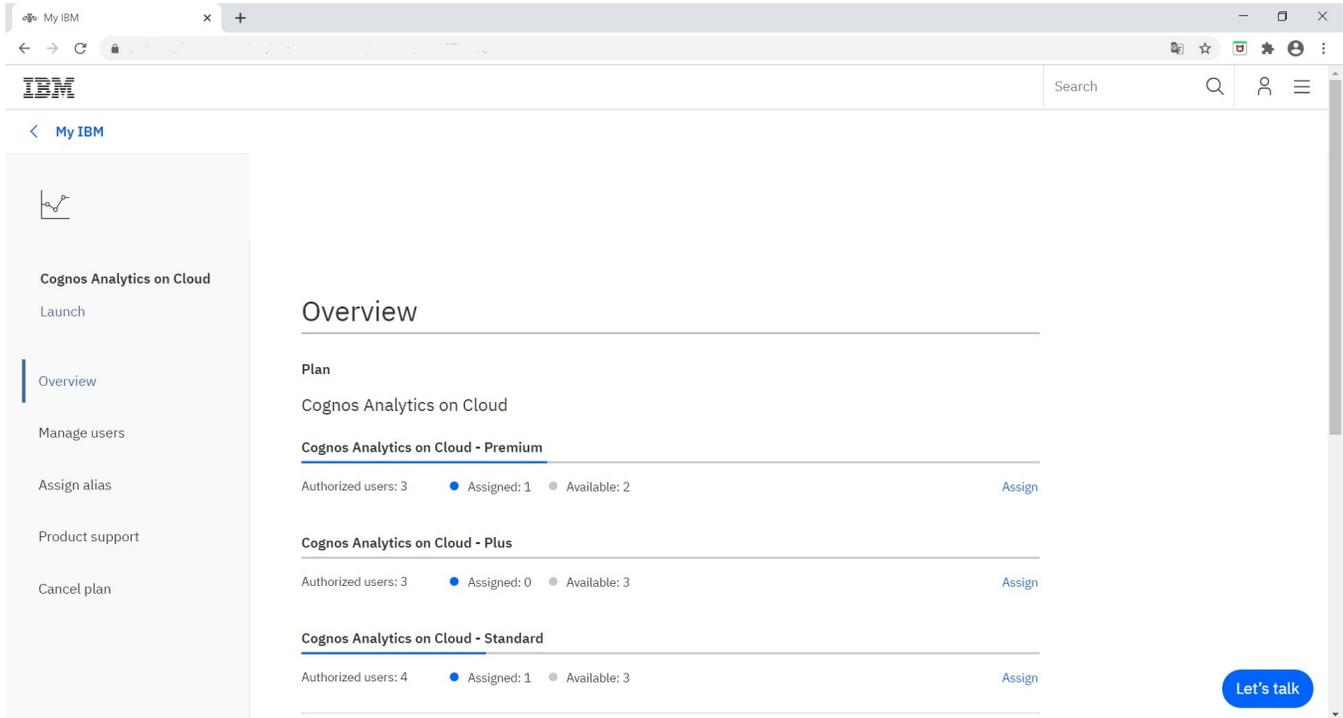
1. Go to your [My IBM dashboard](https://myibm.ibm.com/dashboard) (https://myibm.ibm.com/dashboard).
2. Log in to your IBM account, if you have one. Otherwise, [create your IBM account](https://www.ibm.com/account/profile) now (https://www.ibm.com/account/profile).

Your IBM dashboard appears, including a tile for your Cognos Analytics on Cloud subscription:



3. In the tile for your IBM Cognos Analytics on Cloud product, click **Manage**.

The **Overview** page for your IBM Cognos Analytics subscription appears:



Three subscription levels appear:

- **Cognos Analytics on Cloud - Premium**
- **Cognos Analytics on Cloud - Plus**
- **Cognos Analytics on Cloud - Standard**

**Note:** To help you plan your user assignments, note the number of seats already **Assigned** and the number of seats still **Available** that are shown for the subscription you choose.

## On-Demand subscription roles

There are two types of subscription roles in Cognos Analytics on Cloud On-Demand: subscription administrators and license users.

### Subscription administrator role

As the Subscription administrator, you can make the following changes to your registered Cognos Analytics on Cloud On-Demand plan:

- Add or remove users to the **Standard** or **Premium** subscription.
- Assign users to one of these role combinations:
  - Subscription administrator role
  - License user role
  - Both the subscription administrator role and the license user role
- Send an email to users inviting them to use Cognos Analytics on Cloud On-Demand.
- Cancel the Cognos Analytics on Cloud On-Demand plan for users.

### License user role

License users can use Cognos Analytics on Cloud On-Demand with the functionality that is defined for their subscription level. For example, if you registered them for a Standard subscription, License users will not be able to create reports. If you want the users to be able to create reports, you must upgrade them to a Premium subscription.

The following table shows the Cognos Analytics functionality that is available for the Standard and Premium subscription levels:

Functionality	Standard	Premium
Dashboarding	Yes	Yes
Stories	Yes	Yes
Exploration	No	Yes
AI Assistant	Yes	Yes
Mobile app	Yes	Yes
Reporting: Create or Edit reports	No	Yes
Reporting: Run reports (in html, csv, Excel, and other formats)	No	Yes
Reporting: Schedule reports and jobs	No	Yes
Reporting: Save report output in Cognos	No	Yes
Reporting: Set report bursting	No	No
Reporting: Receive burst reports	No	No
Reporting: View saved report output (1)	Yes	Yes
Reporting: Receive reports sent by email (2)	Yes	Yes
Reporting: View and interact with <a href="#">active reports</a>	Yes	Yes

**Note:** Please note the following clarifications:

1. Viewing the saved report output is not the same as running a report. Standard users can view a report output file (html, csv, and so on) if it was saved by a Premium user in **Team content**.
2. Receiving reports by email is not the same as receiving burst reports. For example, the Premium users can choose the **Send report by email** delivery option, and add standard users' emails to the list of recipients.

The License users can perform these tasks:

- Remove themselves from the subscription.
- Launch and use Cognos Analytics on Demand.
- In Cognos Analytics on Demand, [create custom groups and roles](#) in the Cognos namespace to which content can be secured.

**Important notes about Cognos namespace groups and roles:**

- The two Cognos Analytics on Demand subscription roles (Subscription administrators and License users) serve a different purpose than the Cognos namespace roles.
- In Cognos Analytics on Demand, the [standard built-in groups and roles](#) in the Cognos namespace do not exist.

## Adding users to your On-Demand subscription

If you are a Subscription administrator for IBM Cognos Analytics on Demand, you can add users to your subscription. During this task, you assign each user to the Subscription administrator role, the License user role, or both.

**Important notes about Cognos namespace groups and roles:**

- The two *on Demand subscription roles* (Subscription administrators and License users) serve a different purpose than *Cognos namespace roles*.

- In Cognos Analytics on Demand, the Standard built-in groups and roles in the Cognos namespace do not exist.

## About this task

After you complete this task, an email is sent to the user(s) inviting them to use IBM Cognos Analytics on Demand.

## Procedure

1. Log in to your My IBM Dashboard.
2. In the navigation pane, click **Manage users**.

The Manage Users page appears:

The screenshot shows the 'Manage users (2)' page in the My IBM dashboard. The page has a navigation pane on the left with 'Manage users' selected. The main content area has a title 'Manage users (2)' and two buttons: '+ Add new user' and '+ Add multiple users'. Below these are tabs for 'License users (2)', 'Subscription administrators (1)', and 'Pending invitations (0)'. A search bar and a filter dropdown are present. A table lists two users: one with role 'License user' and status 'Active', and another with role 'Subscription administrator + License user' and status 'Active'. An 'Export user file' button is on the right. A 'Let's talk' button is at the bottom right.

3. If you want to add a single user, follow these steps:
  - a) Click **Add new user**.

My IBM

IBM

Search

< My IBM

Overview

Manage users

Assign alias

Product support

Cancel plan

First name:  
Delete

Last name:  
User

Email or IBMid:

Role:

Subscription administrator  
Can add, remove, and manage users within Products and Services.

License user

Cognos Analytics on Cloud - Premium  
(2 of 3 available)

Cognos Analytics on Cloud - Plus  
(3 of 3 available)

Cognos Analytics on Cloud - Standard  
(3 of 4 available)

Let's talk

b) Enter the first name, last name, and email of the user.

c) Select one or both of these check boxes:

- **Subscription administrator**

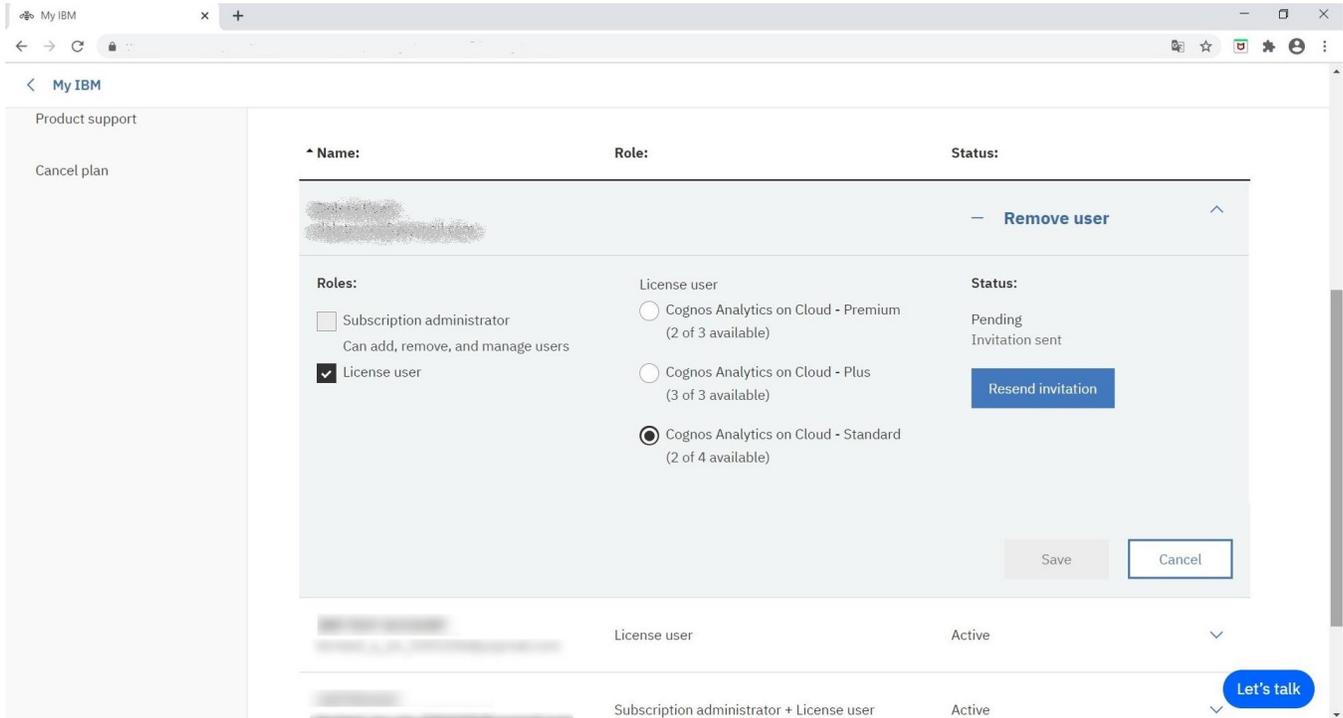
**Tip:** It's good practice to have at least two Subscription administrators.

- **License user** for one of these subscriptions:

- **Cognos Analytics on Cloud - Premium**
- **Cognos Analytics on Cloud - Plus**
- **Cognos Analytics on Cloud - Standard**

d) Click **Submit**.

e) Click the down chevron icon  at the end of the row containing the user's name to expand the user's information.



In the figure above, notice that the user **Status** now listed as **Pending**, as the invitation has not been accepted yet. Also, you have the option of resending the invitation if it was not received or it has expired.

4. If you want to add several users at once, follow these steps:
  - a) Click **Add multiple users**.
  - b) Click **Use this CSV file to upload multiple users**.
  - c) Edit the template `add-multi-users.csv` to list each user's name, email address, and license role(s).
  - d) Save the file.
  - e) Click **Select file** and then browse to the file you just edited.
  - f) Click **Upload**.

**Tip:** You may need to wait a few minutes for the subscription to be updated with the new users.

## Results

When you are done, the list of users is refreshed on the **Manage users** page.

An email is sent to all of the users inviting them to use IBM Cognos Analytics on Cloud. A Licensed user receives the same email invitation that you received and accepted as the Subscription administrator.

After users accept the invitation, the number of **Assigned seats** and the number of **Available seats** shown on the **Overview** page are updated accordingly.

## Removing a user from the subscription

If you are a Subscription administrator for IBM Cognos Analytics on Demand, you can remove users from your subscription.

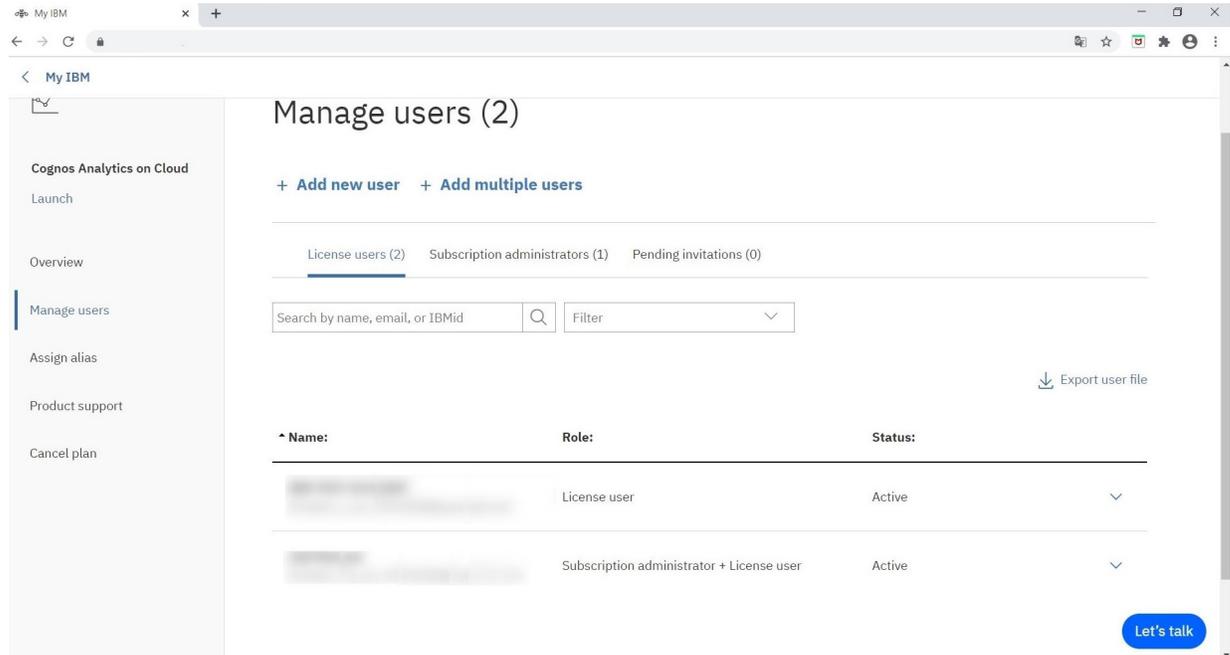
When a user is removed, any public content they created will remain. However, any content in the **My Content** folder will be lost. Adding a user back to the subscription will not restore their **My Content**.

For each user you want to remove, follow these steps:

## Procedure

1. Log in to your My IBM Dashboard.
2. In the navigation pane, click **Manage users**.

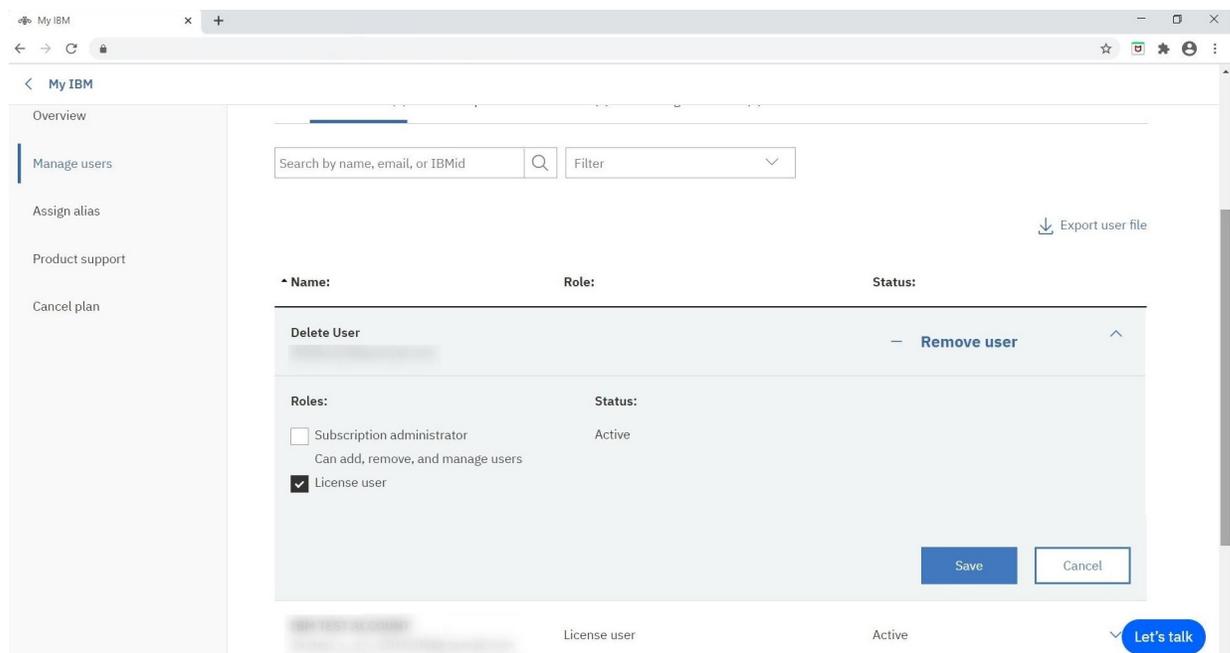
The Manage Users page appears:



3. Locate the user.

### Tips:

- Search on partial text in the user's name, email, or IBM ID.
  - Click **License users**, **Subscription administrators**, or **Pending invitations** to filter on that category.
  - Click **Filter** to filter on the user's status.
4. Click the down chevron icon  at the end of the row containing the user's name to expand the user's information.

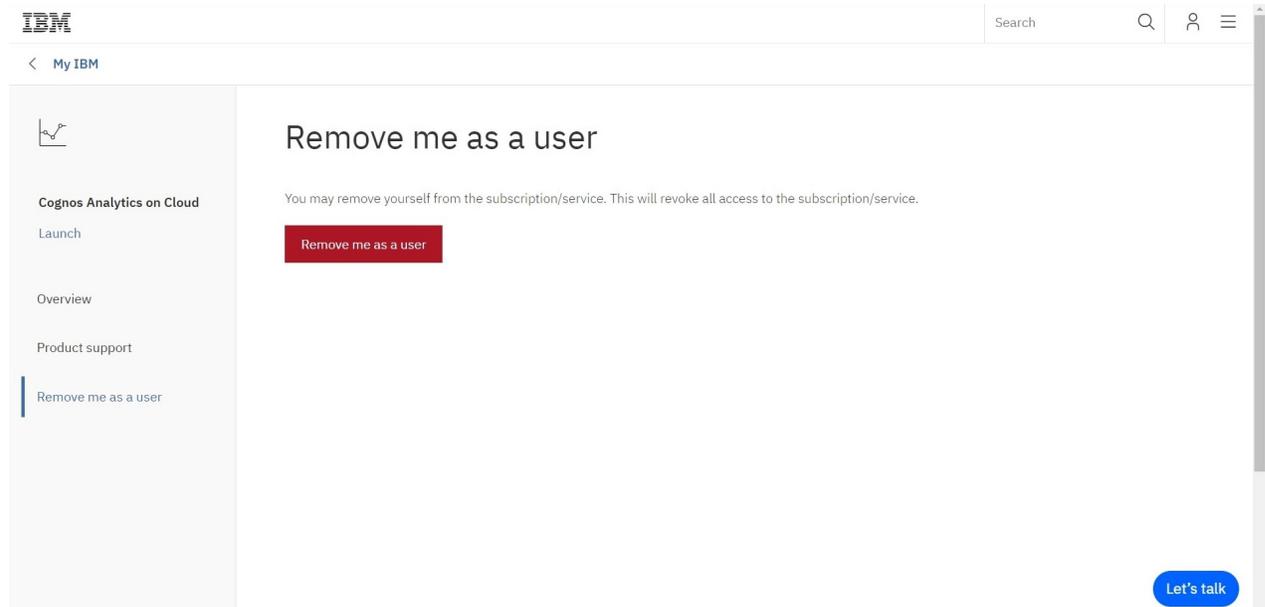


5. If you want to remove the user from your subscription, click **Remove user**.
6. If you want to change the role of the user, change the check box selections in the **Roles** section.  
**Note:** If you leave both the **Subscription administrator** and the **License user** check boxes unselected, the user will be removed from the subscription.
7. Click **Save**.

## Results

The user is removed from the subscription or their role is updated, depending on what you selected.

**Note:** Users can also remove themselves from the subscription by selecting **Remove me as a user** in the navigation menu their my dashboard menu. See the following figure:



## Upgrading your trial subscription

If you have an IBM Cognos Analytics Cloud Trial subscription, you can upgrade at any time to a plan that provides you with a richer user experience.

**Note:** The Trial subscription provides the same capabilities as the Premium offering, so keep that in mind when you upgrade.

### Procedure

1. Go to your [My IBM dashboard](https://myibm.ibm.com/dashboard) (https://myibm.ibm.com/dashboard).
2. Log in to your IBM account.
3. In the tile for IBM Cognos Analytics on Cloud, click **Manage**.

The **Overview** page for your **IBM Cognos Analytics Trial** subscription appears:

4. Click **Upgrade** or scroll down to view details about available IBM Cognos Analytics **On Demand** or **Enterprise** solutions.

5. Click **Purchase now** or **Contact us** to proceed with your upgrade.

## Securing your content (for On-Demand License users)

If you are a designated License user for IBM Cognos Analytics on Demand, you can secure your Cognos Analytics content. You can accomplish this in Cognos Analytics on Demand by assigning permissions to custom groups and roles that you created in the Cognos namespace folder.

### Custom groups and roles in the Cognos namespace

Groups  and roles in the Cognos namespace folder 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.

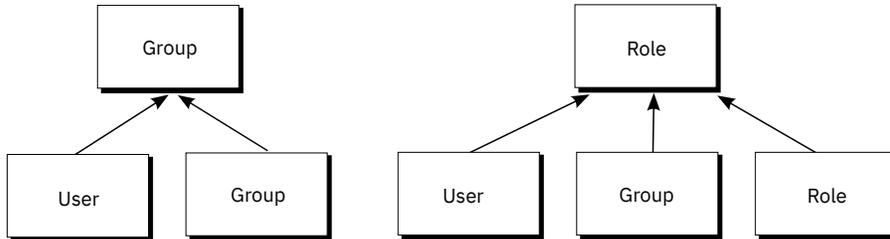


Figure 8. Structure of groups and roles

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.

## Procedure

1. Create custom groups and roles in the Cognos namespace folder.

**Tip:** You cannot change the capabilities of a user, group, or role. Capabilities are determined by the user's on Demand subscription level.

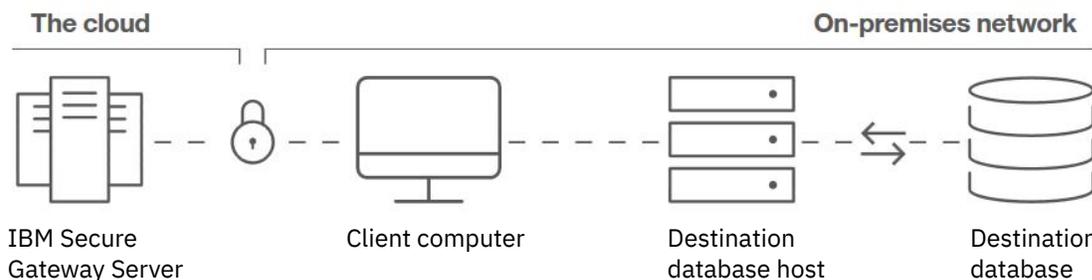
2. Decide which groups or roles should have access to your content.
3. assign group or role permissions to your selected content.

## IBM Secure Gateway (On-Demand only)

Use IBM Secure Gateway to maintain an encrypted connection between an on-premises Secure Gateway Client and the Secure Gateway Servers that IBM maintains on Cloud. This allows you to use IBM Cognos Analytics on Demand to securely consume your on-premises data.

### Secure Gateway at a glance

First, you install the Secure Gateway Client in your on-premises network and configure an encrypted (TLS v1.2) bi-directional connection with the on Cloud Secure Gateway server. Next, you establish a secure connection between the Secure Gateway Client and an on-premises database. This on-premise database is called the "destination database". Your on-premises data can then be securely accessed and manipulated by Cognos Analytics on Demand.



**Note:** IBM Secure Gateway is only available for use with Cognos Analytics on Demand. IBM Secure Gateway is not supported for Cognos Analytics on Cloud - Hosted users. For more information, see Chapter 7, "Tenant administration," on page 131.

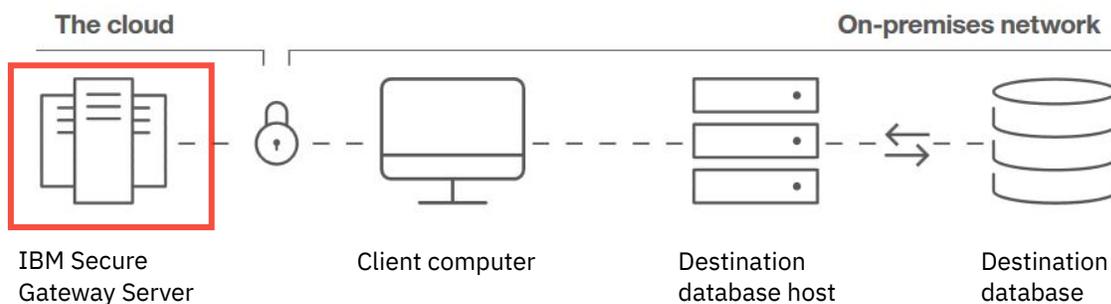
## For more info

For more information about IBM Secure Gateway, see the following resources:

- [About Secure Gateway](https://cloud.ibm.com/docs/services/SecureGateway?topic=securegateway-about-sg) (https://cloud.ibm.com/docs/services/SecureGateway?topic=securegateway-about-sg)
- [Frequently Asked Questions](https://cloud.ibm.com/docs/services/SecureGateway?topic=securegateway-sg-faq) (https://cloud.ibm.com/docs/services/SecureGateway?topic=securegateway-sg-faq)
- [Troubleshooting](https://cloud.ibm.com/docs/services/SecureGateway?topic=securegateway-troubleshooting) (https://cloud.ibm.com/docs/services/SecureGateway?topic=securegateway-troubleshooting)

## Creating a Secure Gateway instance

Creating a Secure Gateway instance is the **first** step in establishing a connection between the IBM Secure Gateway server and your on-premises data.



## Procedure

1. Click **Manage** > **Secure Gateway**.

- If no Secure Gateway instances exist yet, the **Secure Gateway** page appears.
- If other gateways exist, the **Secure Gateway list** appears.

2. Launch the **Connect to an on-premises database** wizard.

- If you are on the **Secure Gateway** page, click **Create**.
- If you are on the **Secure Gateway list** page, click the Add Gateway button **+**.

3. Enter a name for the gateway.

**Note:** You can ignore the token expiration value for now. It refers to the security token that will be generated for your new gateway.

4. Click **Create**.

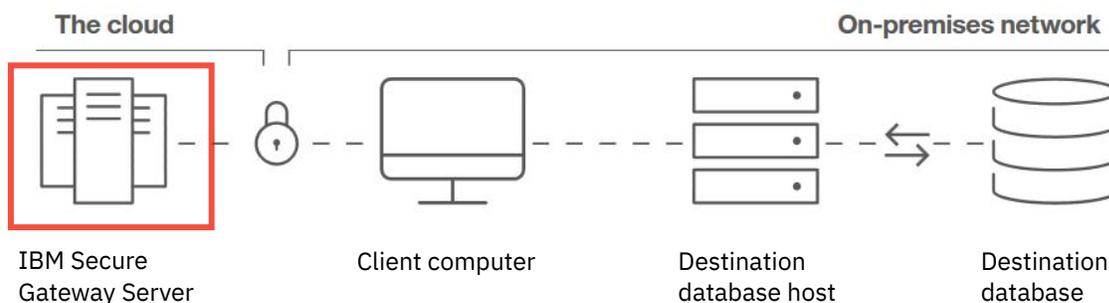
The gateway instance is created and the wizard advances to the next page.

## What to do next

Your next step is to [install and configure the Secure Gateway Client](#).

## Viewing the Secure Gateway list

After you create one or more Gateways, view the Secure Gateway list to check each gateway's properties and status.



### Before you begin

You must have created at least one Secure Gateway instance.

### Procedure

1. Click **Manage > Secure Gateway.**

The **Secure Gateway list** appears.

**Important:** You may need to clear your browser's cache in these cases:

- if the message below appears, and you have not yet hit the maximum number of gateways allowed for your user license type:

You have exceeded the maximum number of secure gateways.

- if the **Gateway connection** value was not refreshed

In Firefox, open a private window. In Chrome, open an incognito window.

2. Check the **Gateway connection** value for your gateway:

- If the value is  **Connected**, you are ready to add a destination database.

- If the value is  **Not connected**, you must:

- a. Install the Secure Gateway Client.
- b. Configure the Secure Gateway Client to connect to your gateway.

- If the value is  **Token expired**, you must refresh your token:

- a. At the end of the row for your gateway, click the ellipsis icon .
- b. Click **Properties.**
- c. Click **Refresh security token.**

A new security token is generated for your secure gateway.

- If the value is  **Invalid**, the gateway cannot be used. At the end of the row for your gateway, click the ellipsis icon , click **Delete** and then create a new gateway.

3. Check the **Status** value for your gateway:

- If it is  **Enabled**, your gateway is available for connection to a destination database.
- If it is  **Disabled**, your gateway is not available.

**Tip:** You can enable the gateway in step “4” on page 296.

4. At the end of the row for your gateway, click the ellipsis icon  and then click **Properties**.

The **Secure Gateway properties** page appears, showing information such as:

- the **Gateway ID** and the **Security token**. Use these values to [configure your Secure Gateway Client](#).
- whether there is a connection with a Secure Gateway Client
- the gateway status

**Tip:** Click this field to toggle between **Enabled** and **Disabled**.

- The **Secure Gateway client** list. To expand a Secure Gateway Client connection, click the chevron button  next to the name of the client host.

## What to do next

To [view the Destinations list](#), click the gateway name.

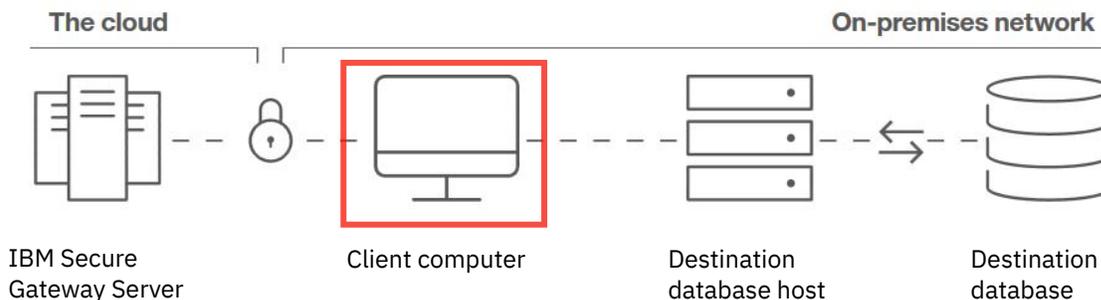
## Installing and configuring the Secure Gateway Client

Installing and configuring the Secure Gateway Client is the second step in establishing a connection between the IBM Secure Gateway server and your on-premises data.

**Note:** If you are viewing the **Add client** page on the wizard, but already installed Secure Gateway Client, do the following:

1. Select **I have already installed the client** and click **Next**.
2. Proceed to [“Adding a destination”](#) on page 304.

Install and configure the Secure Gateway Client so that it can establish connections with both the IBM Secure Gateway on Cloud server and with an on-premises database that will use the Secure Gateway.



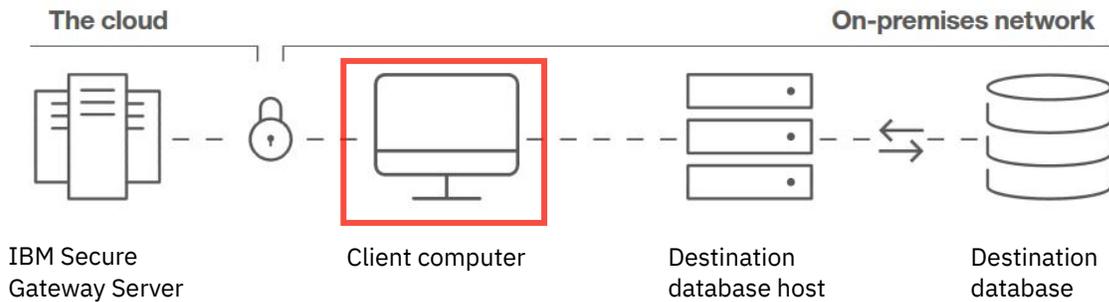
## Installation requirements

For information about system and network requirements, see [Requirements to run the Client](https://cloud.ibm.com/docs/services/SecureGateway?topic=securegateway-client-requirements) (<https://cloud.ibm.com/docs/services/SecureGateway?topic=securegateway-client-requirements>).

## Installing Secure Gateway Client using IBM Installer

You can run the IBM Installer to install Secure Gateway Client on several different platforms:

- AIX
- Ubuntu
- Windows
- Red Hat
- Macintosh

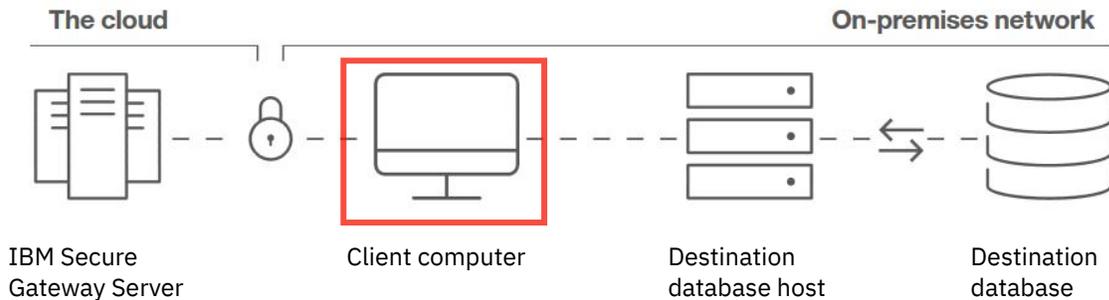


### ***Installing on Windows using IBM Installer***

On Windows, use the IBM Installer to install IBM Secure Gateway Client.

**Note:** If you are viewing the **Add client** page on the wizard, but already installed Secure Gateway Client, do the following:

1. Select **I have already installed the client** and click **Next**.
2. Proceed to [“Adding a destination”](#) on page 304.



### **Before you begin**

Install the Secure Gateway into your IT environment where your corporate security policy allows. This would typically be in a protected yellow zone or DMZ where your company can institute the appropriate security controls to protect on-premises assets. Always follow your corporate security policies and instructions when you install the Secure Gateway client.

### **Procedure**

1. Ensure that you [created a Secure Gateway instance](#).
2. Select **IBM Installer** and then click **Next**.
3. Under **Operating system**, select **Windows**.
4. Click **Download client**.
5. Follow the prompts to install the IBM client.
6. Copy  the **Gateway ID** and **Security token** values into a text file for later use.

**Tip:** You will need these values when you configure the client.

7. Click **Next**.

The Secure Gateway Client is installed and configured and the wizard advances to the next page.

### **What to do next**

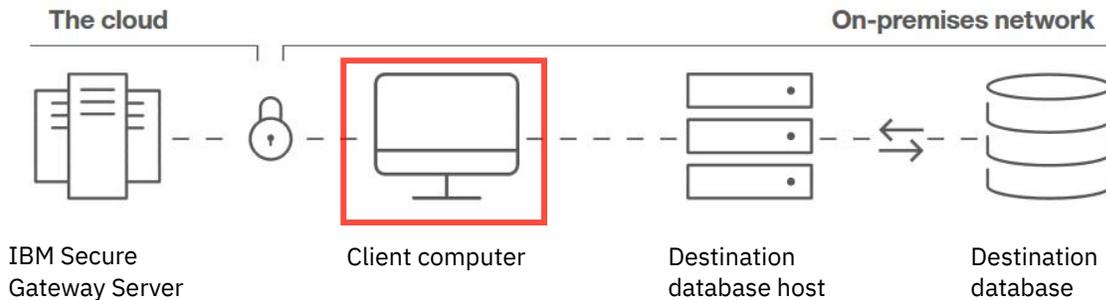
Your next step is to [add an on-premises destination database](#).

## Installing on AIX using IBM Installer

On AIX, use the IBM Installer to install IBM Secure Gateway Client.

**Note:** If you are viewing the **Add client** page on the wizard, but already installed Secure Gateway Client, do the following:

1. Select **I have already installed the client** and click **Next**.
2. Proceed to [“Adding a destination”](#) on page 304.



## Before you begin

Install the Secure Gateway into your IT environment where your corporate security policy allows. This would typically be in a protected yellow zone or DMZ where your company can institute the appropriate security controls to protect on-premises assets. Always follow your corporate security policies and instructions when you install the Secure Gateway client.

## Procedure

1. Ensure that you [created a Secure Gateway instance](#).
2. Select **IBM Installer** and then click **Next**.
3. Under **Operating system**, select **AIX**.
4. Click **Download client**.
5. Follow the prompts to install the IBM client.
6. Copy  the **Gateway ID** and **Security token** values into a text file for later use.

**Tip:** You will need these values when you configure the client.

7. Click **Next**.

The Secure Gateway Client is installed and configured and the wizard advances to the next page.

## What to do next

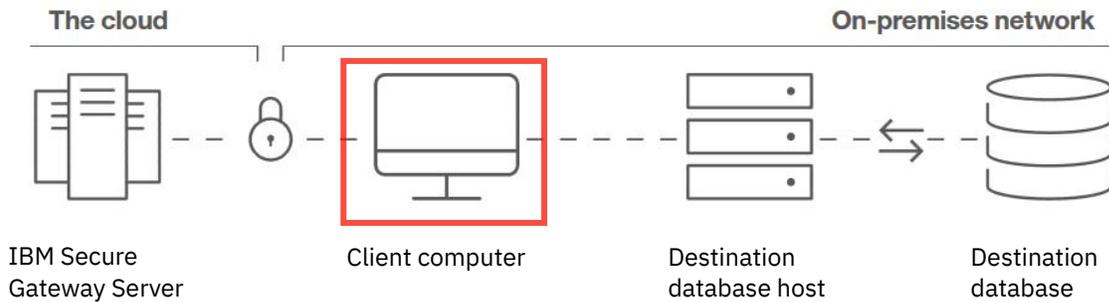
Your next step is to [add an on-premises destination database](#).

## Installing on Ubuntu using IBM Installer

On Ubuntu, use the IBM Installer to install IBM Secure Gateway Client.

**Note:** If you are viewing the **Add client** page on the wizard, but already installed Secure Gateway Client, do the following:

1. Select **I have already installed the client** and click **Next**.
2. Proceed to [“Adding a destination”](#) on page 304.



### Before you begin

Install the Secure Gateway into your IT environment where your corporate security policy allows. This would typically be in a protected yellow zone or DMZ where your company can institute the appropriate security controls to protect on-premises assets. Always follow your corporate security policies and instructions when you install the Secure Gateway client.

### Procedure

1. Ensure that you [created a Secure Gateway instance](#).
2. Select **IBM Installer** and then click **Next**.
3. Under **Operating system**, select **Ubuntu**.
4. Click **Download client**.
5. Follow the prompts to install the IBM client.
6. Copy  the **Gateway ID** and **Security token** values into a text file for later use.

**Tip:** You will need these values when you configure the client.

7. Click **Next**.

The Secure Gateway Client is installed and configured and the wizard advances to the next page.

### What to do next

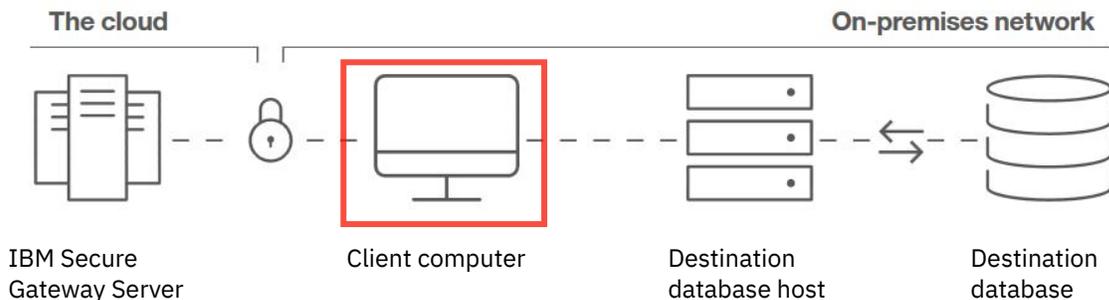
Your next step is to [add an on-premises destination database](#).

### Installing on Red Hat using IBM Installer

On Red Hat, use the IBM Installer to install IBM Secure Gateway Client.

**Note:** If you are viewing the **Add client** page on the wizard, but already installed Secure Gateway Client, do the following:

1. Select **I have already installed the client** and click **Next**.
2. Proceed to [“Adding a destination”](#) on page 304.



## Before you begin

Install the Secure Gateway into your IT environment where your corporate security policy allows. This would typically be in a protected yellow zone or DMZ where your company can institute the appropriate security controls to protect on-premises assets. Always follow your corporate security policies and instructions when you install the Secure Gateway client.

## Procedure

1. Ensure that you [created a Secure Gateway instance](#).
2. Select **IBM Installer** and then click **Next**.
3. Under **Operating system**, select **Red Hat**.
4. Click **Download client**.
5. Follow the prompts to install the IBM client.
6. Copy  the **Gateway ID** and **Security token** values into a text file for later use.

**Tip:** You will need these values when you configure the client.

7. Click **Next**.

The Secure Gateway Client is installed and configured and the wizard advances to the next page.

## What to do next

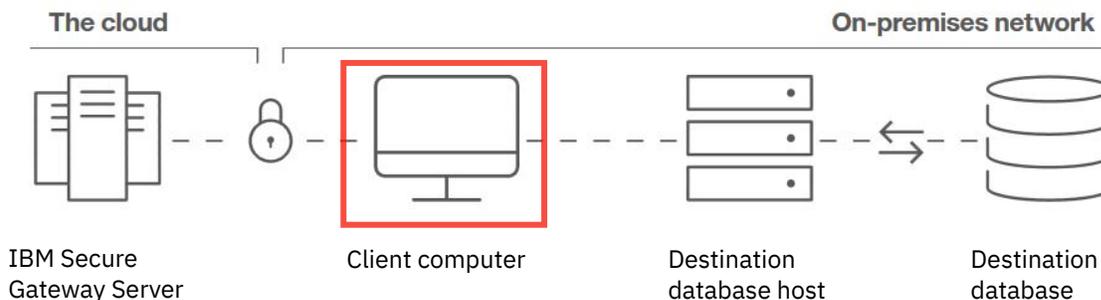
Your next step is to [add an on-premises destination database](#).

### *Installing on Macintosh using IBM Installer*

On Macintosh, use the IBM Installer to install IBM Secure Gateway Client.

**Note:** If you are viewing the **Add client** page on the wizard, but already installed Secure Gateway Client, do the following:

1. Select **I have already installed the client** and click **Next**.
2. Proceed to [“Adding a destination”](#) on page 304.



## Before you begin

Install the Secure Gateway into your IT environment where your corporate security policy allows. This would typically be in a protected yellow zone or DMZ where your company can institute the appropriate security controls to protect on-premises assets. Always follow your corporate security policies and instructions when you install the Secure Gateway client.

## Procedure

1. Ensure that you [created a Secure Gateway instance](#).
2. Select **IBM Installer** and then click **Next**.
3. Under **Operating system**, select **Macintosh**.
4. Click **Download client**.
5. Follow the prompts to install the IBM client.

6. Copy  the **Gateway ID** and **Security token** values into a text file for later use.

**Tip:** You will need these values when you configure the client.

7. Click **Next**.

The Secure Gateway Client is installed and configured and the wizard advances to the next page.

## What to do next

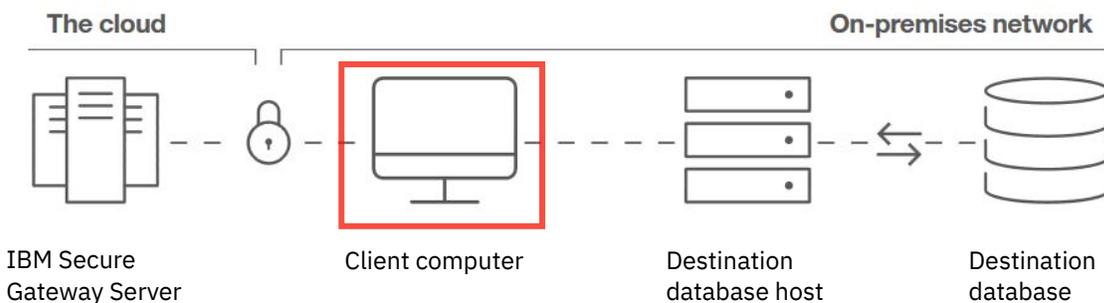
Your next step is to [add an on-premises destination database](#).

## Installing a Docker image that contains the Secure Gateway Client

Instead of using the IBM installer to install Secure Gateway Client, you can install a Docker image that contains the Secure Gateway Client.

**Note:** If you are viewing the **Add client** page on the wizard, but already installed Secure Gateway Client, do the following:

1. Select **I have already installed the client** and click **Next**.
2. Proceed to [“Adding a destination”](#) on page 304.



## Procedure

1. Ensure that you [created a Secure Gateway instance](#).
2. Select **Install Docker** and follow the prompts.

For more information, see [About Docker CE \(https://docs.docker.com/install/\)](https://docs.docker.com/install/).

**Tip:** On Linux, you can add `-h `hostname`` to your Docker bash shell. This will return the name of the system that Docker is hosted on, rather than the Docker ID.

3. Open a command window.
4. Copy  and run the Docker pull command.
5. Copy  and run the Docker run command with security token.
6. Click **Next**.

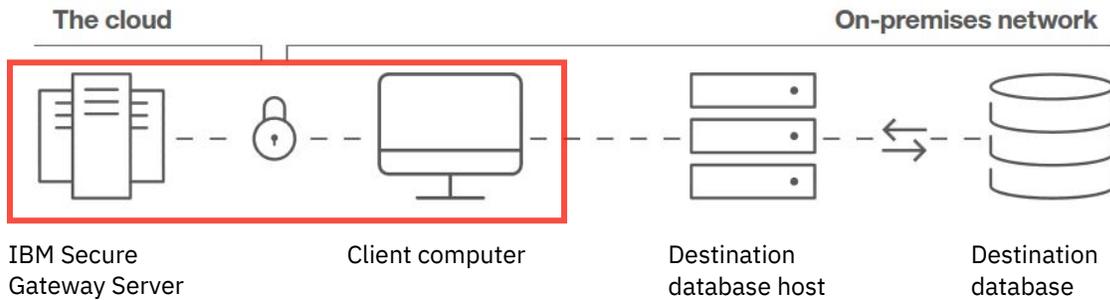
The Secure Gateway Client is installed and configured and the wizard advances to the next page.

## What to do next

Your next step is to [add an on-premises destination database](#).

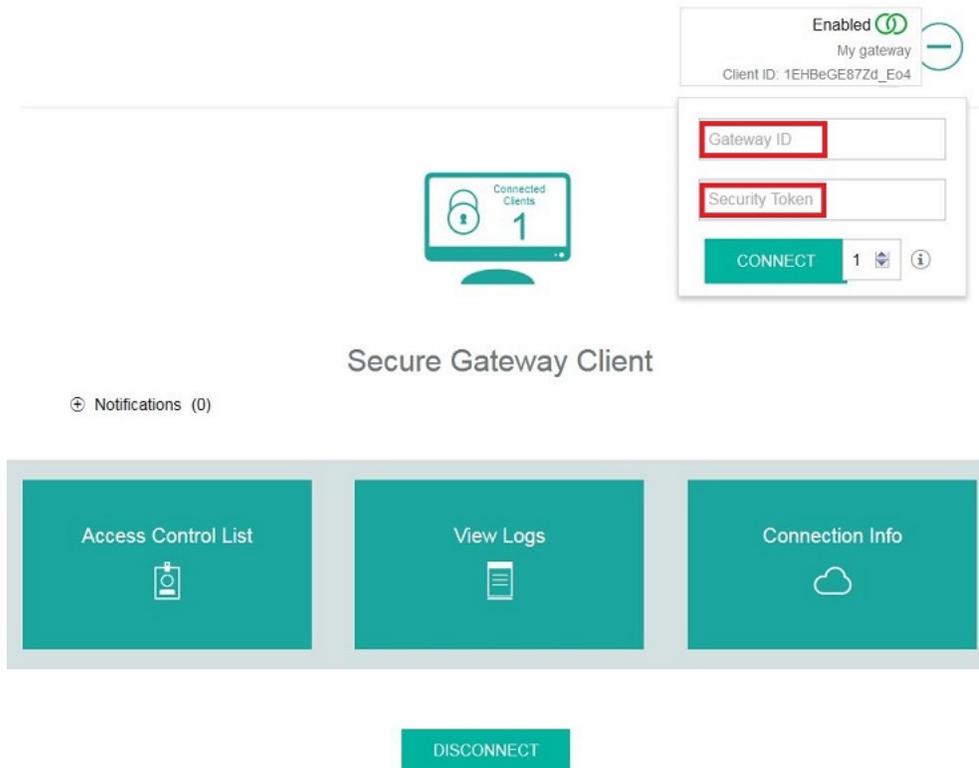
## Configuring Secure Gateway Client

Configure your Secure Gateway Client to connect to your Secure Gateway instance.



### Procedure

1. Start the Secure Gateway Client that you installed on your on-premises computer.
2. In the upper-right corner of the Secure Gateway Client window, click the plus sign button **+**.  
You are prompted for the **Gateway ID** and the **Security Token**.



3. Enter the **Gateway ID** and **Security Token** values from the [Properties page](#) when you view the **Secure Gateways list**.
4. Click **CONNECT**.
5. Go to the **Secure Gateways list** page,.  
The status shows as **Not connected**.
6. Click **Refresh**.

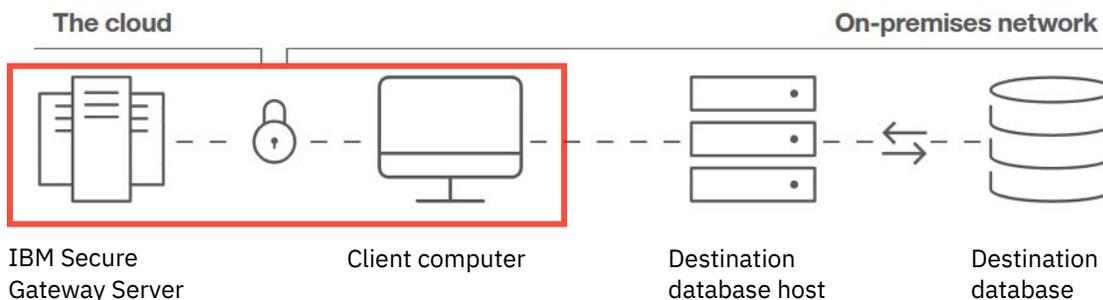
The status changes to **Connected**. This confirms that your Secure Gateway client is connected to your Secure gateway instance on the cloud.

## What to do next

You can now [connect to a destination](#) or view the properties of your Secure Gateway Client.

## Viewing the Secure Gateway Client properties

After you create a Secure Gateway instance and connect one or more Secure Gateway Client instances to it, you can view the Secure Gateway properties. This allows you to check on the gateway-client connection or troubleshoot issues.



## Before you begin

You must have [created at least one Secure Gateway instance](#) and [configured at least one Secure Gateway Client connection](#).

## Procedure

1. Click **Manage > Secure Gateway**.

The **Secure Gateway list** appears.

2. At the end of the row for your gateway, click the ellipsis icon **⋮** and then click **Properties**.

The **Secure Gateway properties** page appears. At the bottom, is a list of all **Secure Gateway client** connections to the current gateway.

3. To expand a Secure Gateway Client connection, click the chevron icon **>** next to the name of the client host.

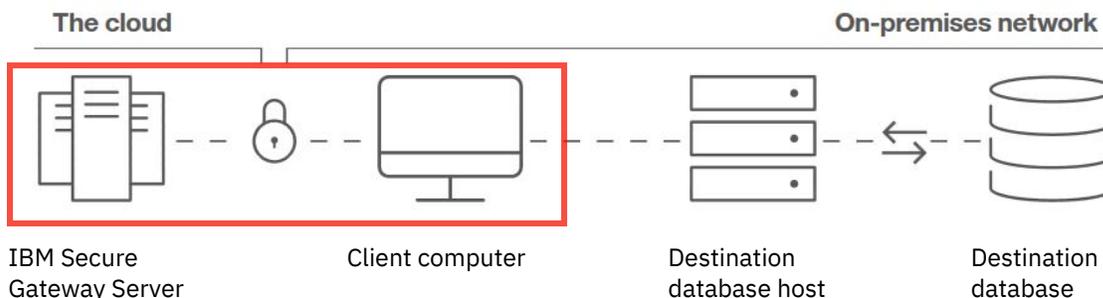
Client properties appear, such as the its connection status and the client ID.

4. To [check the performance](#) of your Secure Gateway client-server connection, click **Latency test**.
5. To [troubleshoot client-server connection issues](#), click **View client logs**.

## Testing latency

You can run a latency test on your Secure Gateway client-server connection. This test measures how long it takes for data to travel back and forth between your local Secure Gateway Client and the on-cloud Secure Gateway server.

For more information, see [Understanding latency](https://cloud.ibm.com/docs/infrastructure/direct-link?topic=direct-link-understanding-latency) (<https://cloud.ibm.com/docs/infrastructure/direct-link?topic=direct-link-understanding-latency>).



## Procedure

1. Click **Manage > Secure Gateway**.

The **Secure Gateway list** appears.

**Tip:** If you just completed your connection, but the **Gateway connection** value for your gateway is  **Not connected**, click **Refresh** to update the value to  **Connected**.

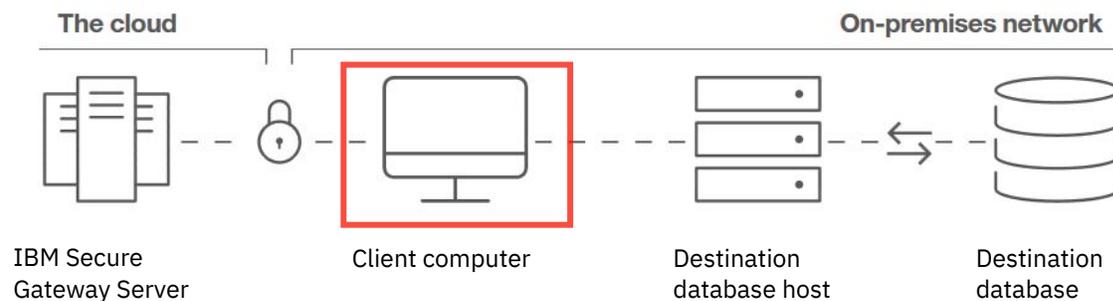
2. At the end of the row for your gateway, click the ellipsis icon  and then click **Properties**.
3. At bottom of the **Secure Gateway properties** page, under **Secure Gateway client**, expand the name of the computer where you installed Secure Gateway Client.
4. Click **Latency test**.

## Results

The Server-Client Latency and the Client-Server Latency times are displayed, in milliseconds.

### Client logs

Client logs record events related to the connection between IBM Secure Gateway Client and the IBM Secure Gateway server.



## Viewing log messages

To view the log messages, follow these steps:

1. Click **Manage > Secure Gateway**.

The **Secure Gateway list** appears.

**Tip:** If you just completed your connection, but the **Gateway connection** value for your gateway is  **Not connected**, click **Refresh** to update the value to  **Connected**.

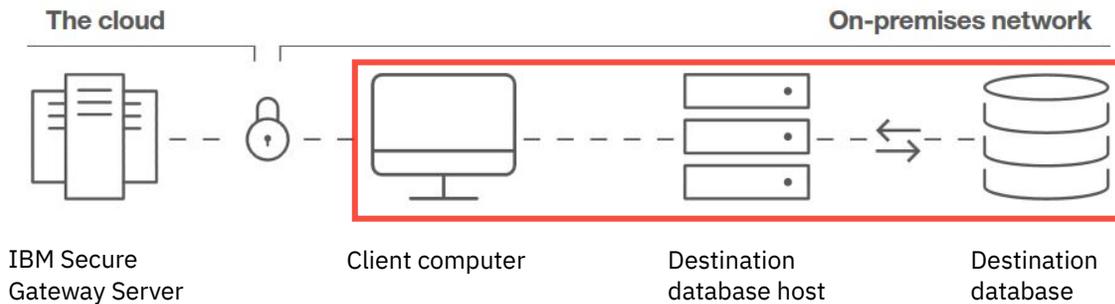
2. At the end of the row for your gateway, click the ellipsis icon  and then click **Properties**.
3. At bottom of the **Secure Gateway properties** page, under **Secure Gateway client**, expand the name of the computer where you installed Secure Gateway Client.
4. Click **View client logs**.

If a log message is unclear, consult with your administrator about possible actions that you should take.

## Adding a destination

Adding a destination is the **third** step in establishing a connection between the IBM Secure Gateway server and your on-premises data.

Add a destination to define the on-premises database that you will associate with your gateway.



## Procedure

1. Ensure that you [installed and configured the IBM Secure Gateway Client](#).  
If you clicked **Next** after installing and configuring the Secure Gateway Client, the **Add destination** page appears.
2. If you previously installed and configured the Secure Gateway Client and then exited the wizard, follow these steps:
  - a) Click **Manage > Secure Gateway**.
  - b) On the **Secure Gateway list** page, click your gateway.
  - c) On the **Destination list** page, click the Add destination button **+**.

The **Add destination** page appears.

3. Enter a name for your destination.

**Tip:** Include the database type in the name.

4. Enter the computer host name and port number for your database.
5. Click **Next**.

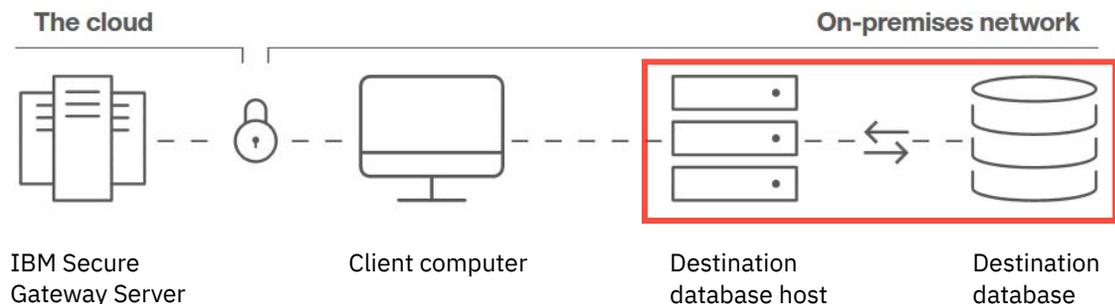
The destination is added and will appear on the destination list the next time you [view it](#).

## What to do next

Your next step is to [specify valid destination databases that can be accessed by the Secure Gateway](#).

## Viewing the Destinations list

After you create one or more Destinations, view the Destinations list to check each Destination's properties and status.



## Before you begin

You must have [added at least one Destination](#).

## Procedure

1. Follow the [steps to view the Secure Gateway list](#).

2. In the Secure Gateway list, click the gateway name.

The **Destinations list** appears.

3. Check the **Destination connection** value for your destination:

**Important:** You may need to clear your browser's cache before the **Destination connection** value is refreshed. In Firefox, open a private window. In Chrome, open an incognito window.

- If the value is  **Connected**, you are connected to the destination host.
- If the value is  **Blocked by ACL**, click the **Blocked by ACL** link to [configure the Access Control List](#) for your destination.
- If it is  **Invalid**, there are two possibilities:
  - a. The Secure Gateway service may be temporarily unavailable. In this case, the destination connection is still valid, and will show as  **Connected** after the service becomes available. If your destination connection originally was valid, check the Destinations list later. You can then confirm that the Destination connection value is no longer Invalid and that the Secure Gateway service is therefore running again.
  - b. The destination cannot be used. At the end of the row for your destination, click the ellipsis icon  , click **Delete** and then [add a new destination](#).

4. Check the **Status** value for your destination:

- If it is  **Enabled**, your destination is available for connection to a Secure Gateway.
- If it is  **Disabled**, your destination is not available.

**Tip:** You can enable the destination in step “5” on [page 306](#).

5. At the end of the row for your destination, click the ellipsis icon  and then click **Properties**.

The **Destination properties** page appears, showing information such as:

- the Destination host name and port number. Use this value when you [create a data server connection on the destination computer](#).
- the Destination status

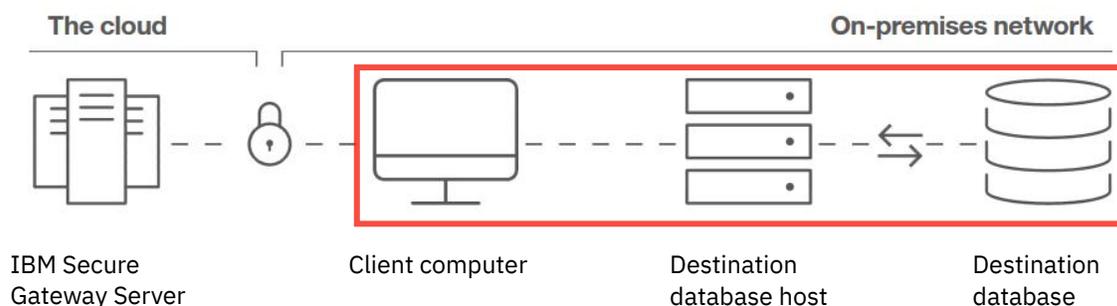
**Tip:** Click this field to toggle between **Enabled** and **Disabled**.

- The **Data server connection list**. Click the chevron button  to list any data server connections that you [already created](#).

## Connecting to an on-premises destination database

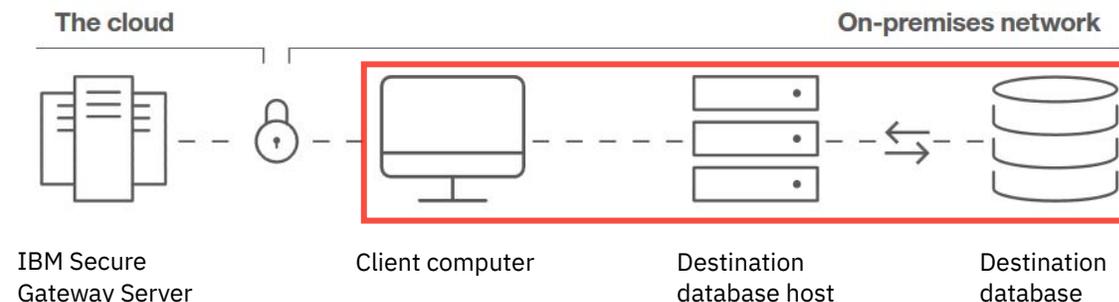
Connecting to an on-premises destination database is the **fourth** step in establishing a connection between the IBM Secure Gateway server and your on-premises data.

Connect the Secure Gateway Client to a destination database to allow on-premises data to be shared securely with Cognos Analytics on Cloud on Demand.



## Specifying which databases can be accessed

Edit the IBM Secure Gateway Access Control List (ACL) to identify your on-premises database as a valid destination database for your Secure Gateway instance. This will allow you to securely access your on-premises data in IBM Cognos Analytics on Demand.



The ACL is a file in which you list the names and port numbers of computers that are permitted to host your on-premises data via the Secure Gateway.

For more detailed information, see [Access Control List \(https://cloud.ibm.com/docs/services/SecureGateway?topic=securegateway-acl\)](https://cloud.ibm.com/docs/services/SecureGateway?topic=securegateway-acl).

## Editing the Access Control List

If you want to use the command line interface (**Option 1**), follow these steps:

1. Open a command window.
2. Run the following command:

```
acl allow database_hostname:port_number
```

where *database\_hostname* is the name of the computer that hosts the database and *port\_number* is the port number of the database.

3. In the **Connect to an on-premises database** wizard, click **OK**.

If you want to use the Secure Gateway Client interface (**Option 2**), follow these steps:

1. Start the Secure Gateway Client on your local computer.
2. Click **Access Control List**.
3. Under **Allow access**, enter the destination computer's name and port number.
4. In the **Connect to an on-premises database** wizard, click **OK**.

## What to do next

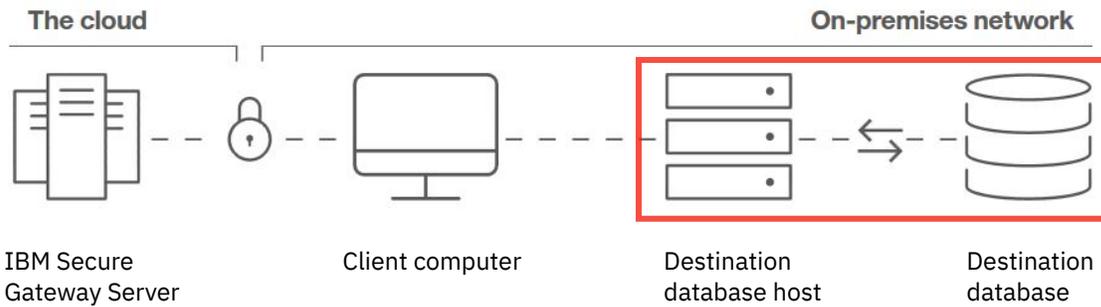
Your next step is to [create a data server connection on the destination computer](#).

**Tip:** You may already have set up a data server connection that you can use for your destination database.

## Creating a data server connection on the destination computer

A data server connection specifies the parameters that are needed to connect to the destination database for your Secure Gateway.

**Note:** Only relational databases can be used for Secure Gateway data server connections.



Each data server can have one or more connections. The connection names must be unique.

For information about data server connections that are not used as Secure Gateway destinations, see [“Data servers” on page 29](#).

## Procedure

1. Click **Manage > Data server connections**.
2. In the **Data server connections** pane, click the **Add data server** icon .
3. Select the data server type from the list of supported types.

**Tip:** You must select a relational data server type.

4. In the field **New data server connection**, type a unique name for the connection.
5. Beside **Connections details**, click **Edit** and enter the connection details for the type of connection that you are creating.

Specify the JDBC URL. You can view the syntax and example URL under connection details. You might need to ask the database administrator for more details, or check the database vendor documentation.

**Important:** The JDBC URL must contain only one host name and only one static port number.

6. In the **Edit *dataserver\_type* connection** pane, under **Secure Gateway destination**, select the Gateway and Destination names that you created.
7. Under **Authentication method**, specify how to access the data server.

You can select one of the following options.

### Connect anonymously or Integrated security

Choose the **Connect anonymously** option when anonymous access to the data server is allowed.

### Prompt for the user ID and password

Choose this option when the user must be prompted for database credentials with each use.

### Use an external namespace

Choose this option to secure the connection against a namespace that is configured for Cognos Analytics. Use the drop-down menu to select one of the available namespaces.

### Use the following signon

Choose this option to assign a signon for the connection.

Select the signon from the drop-down list, or create a new signon by clicking the add icon  . In the **New data server connection** window on the **Credentials** tab, type a user ID and password.

To restrict the signon to particular users, roles, or groups, on the **Permissions** tab, click the add icon , and specify the access permissions for the signon.

## Results

The new connection name is displayed in the **Data server connections** panel. To edit the data server connection, including adding or modifying its signon, click the connection name.

## What to do next

You are now ready to use Cognos Analytics on Demand with your on-premises data.

For more information, see the *Cognos Analytics Data Modeling Guide*.



---

# Index

## A

- access permissions
  - capabilities [159](#)
  - granting or denying [143](#)
  - ownership of entries [143](#)
  - secured functions and features [159](#)
  - setting [144](#)
  - users [140](#)
- actions
  - permissions [140](#)
- activities
  - managing [115](#)
- Administration
  - secured functions and features [148](#)
- Analysis Studio
  - secured functions and features [148](#)
- audit logging [98](#)
- authentication
  - IBMid [14](#)
  - prompts [144](#)
- authentication providers
  - namespaces [13](#)
  - OpenID Connect [14](#)

## B

- bidirectional languages [136](#)
- bootstrap.properties file [103](#)

## C

- cancel entry run [129](#)
- capabilities
  - secured functions [148](#)
- Cloudera Impala
  - JDBC driver [74](#)
- Cognos Viewer
  - secured functions and features [148](#)
- color palettes [254](#)
- connection parameters [61](#)
- connections
  - data servers [29](#)
  - Planning Analytics [78](#)
- connections to data servers
  - Cloudera Impala [74](#)
- content language [136](#)
- Content Manager
  - initial access permissions [159](#)
- content stores
  - backup [21](#)
- current
  - activities [129](#)
  - entries [129](#)
- customizing
  - Cognos Analytics [211](#)
  - tenants [135](#)

## D

- data modules [77](#)
- data servers
  - Cloudera Impala [74](#)
  - connection parameters [61](#)
  - creating connections [29](#)
  - Denodo [74](#)
  - end of support [74](#)
  - loading metadata [69](#)
  - multiple connections [72](#)
  - Pivotal Greenplum and HDB [74](#)
  - Planning Analytics [29](#), [78](#)
  - troubleshooting connections [72](#)
  - unknown data types [73](#)
  - updates by release [77](#)
- data sets
  - creating [83](#)
- data sources
  - securing against multiple namespaces [144](#)
- defaults
  - user profiles [256](#)
- deleting
  - user profiles [112](#), [257](#)
- Denodo
  - supported versions [74](#)
- denying access [143](#)
- deploying
  - content store [21](#)
- Detailed Errors
  - secured functions and features [148](#)
- diagnostic logging
  - troubleshooting Cognos service startup problems [103](#)
- dispatchers
  - setting routing rules [111](#)
- distributing content
  - tenant sender [136](#)

## E

- end of support
  - data servers [74](#)
- enriching packages [80](#)
- entries
  - cancel run [129](#)
  - current [129](#)
  - past [128](#)
  - scheduling [115](#)
  - suspend run [129](#)
  - upcoming [127](#)
- Event Studio
  - secured functions and features [148](#)
- execute permissions [139](#)
- external namespaces [13](#)

## F

- features [148](#)
- files
  - uploading [87, 89, 93](#)
- folders
  - maximum number of users [1](#)
- functions [148](#)

## G

- Glossary
  - object capabilities [190](#)
  - secured functions and features [148](#)
- granting access [143](#)
- groups
  - creating [5](#)
  - managing [5](#)
  - modifying settings after installation [146](#)

## I

- IBM Cognos
  - namespace [1](#)
- IBM Cognos Series 7 namespace [13](#)
- IBMId
  - setting up [14](#)

## J

- JDBC drivers
  - Cloudera Impala [74](#)

## L

- licenses
  - usage report [195](#)
- Lineage
  - object capabilities [190](#)
  - secured functions and features [148](#)
- logging
  - log files [98](#)
  - types [98](#)
- logging on
  - multiple namespaces [144](#)

## M

- metadata
  - loading [69](#)
- Mobile
  - secured functions and features [148](#)
- multitenancy
  - assigning content to tenants [132](#)
  - containment rules [131](#)
  - tenant administration [131](#)
  - tenant ID [133](#)
  - tenants [131](#)

## N

- namespaces

- namespaces (*continued*)
  - authentication providers [13](#)
  - IBM Cognos [1](#)
  - multiple [1, 144](#)

## O

- object capabilities
  - Glossary [190](#)
  - Lineage [190](#)
  - setting up [194](#)
- OpenID Connect
  - adding groups [17](#)
  - adding users [14, 16](#)

## P

- packages
  - enriching metadata [80](#)
- palettes
  - global [254](#)
  - system [254](#)
- past
  - activities [128](#)
  - entries [128](#)
- permissions
  - actions [140](#)
  - execute [139](#)
  - granting or denying [143](#)
  - parent/child [144](#)
  - read [139](#)
  - secured functions and features [148](#)
  - set policy [139](#)
  - traverse [139](#)
  - write [139](#)
- permissions and permitted actions
  - Cognos Workspace
    - reports, report parts, folders, workspaces [141](#)
- Pivotal Greenplum and HDB
  - stalled queries [74](#)
- Planning Analytics
  - creating connections [29](#)
  - creating data modules [78](#)
- predefined entries [209](#)
- product language [136](#)
- profiles
  - user [256](#)

## Q

- Query Studio
  - secured functions and features [148](#)

## R

- read permissions [139](#)
- reporting
  - license usage [195](#)
- roles
  - creating [5](#)
  - managing [5](#)
  - modifying settings after installation [146](#)
  - predefined [209](#)

routing rules [111](#)  
routing tags  
    setting server groups [111](#)

## S

schedules  
    entries [115](#)  
    manage upcoming activities [127](#)  
Scheduling  
    secured functions and features [148](#)  
secured features [148](#)  
secured functions  
    Administration [148](#)  
    Analysis Studio [148](#)  
    Cognos Viewer [148](#)  
    Detailed Errors [148](#)  
    Event Studio [148](#)  
    Generate CVS Output [148](#)  
    Generate PDF Output [148](#)  
    Generate XLS Output [148](#)  
    Generate XML Output [148](#)  
    Glossary [148](#)  
    Lineage [148](#)  
    Mobile [148](#)  
    My Data [148](#)  
    Query Studio [148](#)  
    Reporting [148](#)  
    Scheduling [148](#)  
secured functions and features  
    initial access permissions [159](#)  
security  
    access permissions [139](#)  
    access to content [1](#)  
    authentication [1](#), [13](#)  
    functions and features [148](#)  
    modifying settings after installation [146](#)  
    predefined entries [209](#)  
    setting up [146](#)  
server groups  
    setting [111](#)  
    setting routing rules [111](#)  
session logging [98](#)  
set policy permissions [139](#)  
setting  
    access permissions [144](#)  
sources  
    data modules [77](#)  
    data sets [82](#)  
    packages [80](#)  
    uploaded files [87](#)  
suspend  
    entries [129](#)

## T

tenant ID  
    public object [133](#)  
tenant sender [136](#)  
tenants  
    creating [131](#)  
    customizing [135](#)  
    deleting [138](#)

tenants (*continued*)  
    disabling [137](#)  
    enabling [137](#)  
    terminating active user sessions [137](#)  
time zone [136](#)  
traverse  
    permissions [139](#)  
troubleshooting  
    data server connections [72](#)  
troubleshooting Cognos service startup problems [103](#)

## U

unknown data types  
    warnings [73](#)  
upcoming activities [127](#)  
uploaded files  
    best practices [92](#)  
    data types used [93](#)  
uploading files [89](#)  
user profiles  
    copying [258](#)  
    default [256](#)  
users  
    best practices for grouping users [1](#)  
    classes and permissions [140](#)  
    creating in Cognos Analytics [6](#), [282](#), [284–286](#), [289](#), [291](#),  
    [292](#)  
    deleting profiles [112](#), [257](#)  
    managing [6](#), [282](#), [284–286](#), [289](#), [291](#), [292](#)  
    profiles [256](#)

## W

write permissions [139](#)





