Administer Qlik Sense Enterprise on Windows

Qlik Sense®
February 2023

Contents

Contents

Contents

Contents

Contents
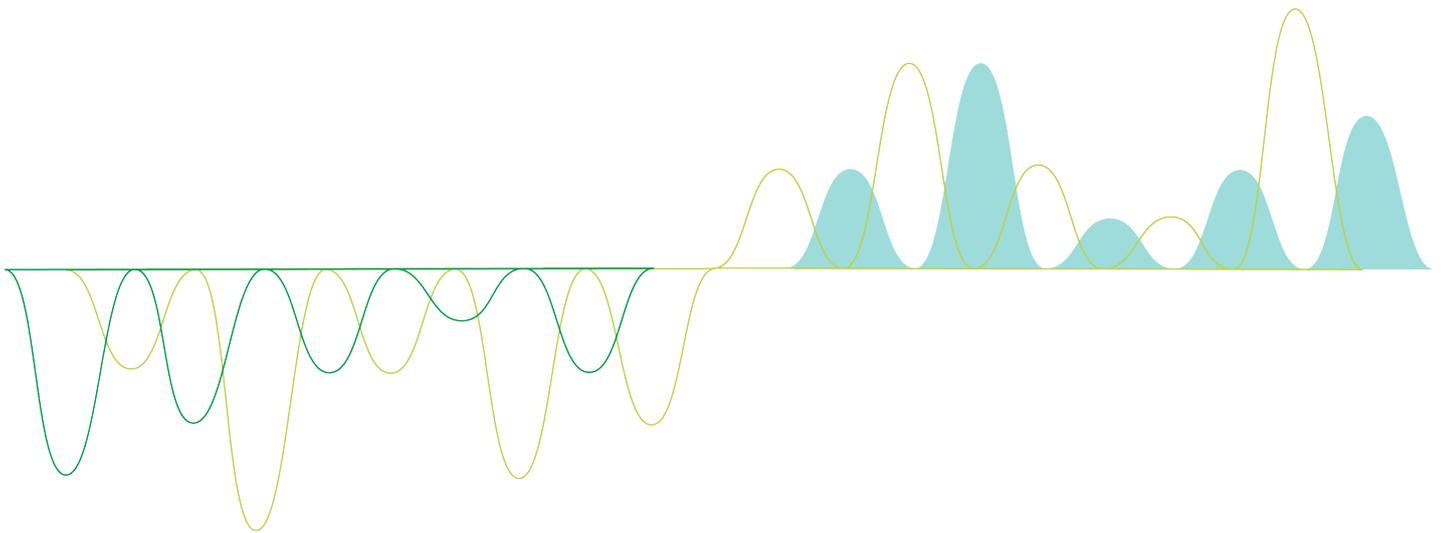
1 Managing a Qlik Sense Enterprise on Windows site

The QMC is a web-based application for configuring and administrating your Qlik Sense Enterprise on Windows site. In the QMC, you can, among other things, do the following:

- Manage licenses
- Manage access types
- Configure nodes
- Manage data connections
- Manage content security (by security rules)
- Manage tasks and triggers
- Synchronize users

> *In a multi-node installation, you manage the whole Qlik Sense Enterprise on Windows site from the QMC on the central node. You can access the QMC from rim nodes, but requests from the QMC towards the repository are routed to the repository on the central node.*

The QMC provides you with a set of very powerful tools to create different access patterns for different QMC administrators and for the different user groups that access the hub:

- Security rules
- Admin roles
- Custom properties

> *For some useful tips regarding how to work with the QMC, see QMC performance – best practices (page 444).*

1.1 Important concepts in the QMC

Apps

You can create and publish apps to streams from the Qlik Sense hub, if you have the appropriate access rights. Apps can also be published from the QMC. To publish an app that is created in a Qlik Sense Desktop installation, you must first import it from the QMC. The security rules applied to the app, stream, or user, determine who can access the content and what the user is allowed to do. The app is locked when published. Content can be added to a published app through the Qlik Sense hub in a server deployment, but content that was published with the original app cannot be edited. Apps can only be deleted from the apps overview page of the QMC.

Associated items

The resources in the QMC have an associative structure. This makes it easy for you to navigate between the different resources in the QMC. Because of the associative structure of the QMC, you can select a resource in more than one way. For example, you can select an app either from the apps overview or from the **Associated items** for the stream that the app belongs to. Similarly, you can select a task either from the tasks overview or from the **Associated items** for the app that the task belongs to.

Audit

On the QMC audit page, you can query for resources and users, and audit the security rules, load balancing rules, or license rules that have been defined in the Qlik Sense system.

Custom properties and QMC tags

In the QMC, you can create customized properties that you can connect to resources. The main purpose of custom properties is to use them in the security rules. You can also create and connect QMC tags that can be used for filtering on the overview page of a resource. Tags cannot be used in the security rules.

Application example for custom properties:

- **Grouping streams by department**
  Create a custom property called *Departments* with values appropriate to your organization. Apply the custom property to your streams and you can then apply security rules to streams according to their *Departments* property instead of managing security rules for individual streams.

> *Group memberships are uploaded to the central repository when you create and synchronize a user directory connector. This means that you can apply security rules to group memberships instead of defining and applying custom properties to users.*

Data connections

You can manage security rules for all data connections from the QMC. Users can create data connections from Qlik Sense but the sharing of data connections (security rules) is managed from the QMC.

Multiple selections

You can select several resources from the overview. By doing this, you can edit or delete multiple resources at the same time. This makes your QMC administration work more efficient.

Publish to stream

You can create and publish apps to streams from the Qlik Sense hub, if you have the appropriate access rights. Apps can also be published from the QMC. To publish an app that is created in a Qlik Sense Desktop installation, you must first import it from the QMC. The security rules applied to the app, stream, or user, determine who can access the content and what the user is allowed to do. The app is locked when published. Content can be added to a published app through the Qlik Sense hub in a server deployment, but content that was published with the original app cannot be edited.

By default, Qlik Sense includes two streams: **Everyone** and **Monitoring apps**.

> *All authenticated users have read and publish rights to the **Everyone** stream and all anonymous users read-only rights.*

> *Three of the predefined admin roles (RootAdmin, ContentAdmin, and SecurityAdmin), have read and publish rights to the Monitoring apps stream.*

Security rules

Content security is a critical aspect of setting up and managing your Qlik Sense Enterprise on Windows system. The QMC enables you to centrally create and manage security rules for all your Qlik Sense resources. Security rules define what a user is allowed to do with a resource, for example read, update, create, or delete.

By design, security rules are written to include, not exclude, users. Users who are not included in security rules are denied access. Therefore, security rules must be created to enable users to interact with Qlik Sense content, data connections, and other resources.

> *The QMC includes pre-defined administrator roles, including the RootAdmin user who has full access rights to the Qlik Sense Enterprise on Windows system, which allows the RootAdmin user to set up security rules.*

Access types

There are two license models: the serial and control number and the signed license key. These models define the terms of your license and the access types that you can allocate to users. With a signed license key, you need internet access (direct or through a proxy) to access the cloud-based license backend, for user assignments, analytic time consumption, and product activations.

There are two major license types: one based on access types, and one based on tokens.

- Access types licenses are the Professional and Analyzer Users licenses (user-based) and Analyzer Capacity licenses (capacity-based). With a Professional and Analyzer Users license you can allocate professional access and analyzer access. With an Analyzer Capacity license you can allocate analyzer capacity access, where consumption is time based (analyzer time).
- With a Qlik Sense Token license you use tokens to allocate access passes to users. You can allocate user access and login access.

An access type allows users to access the hub and apps within a Qlik Sense Enterprise on Windows site.

> *If you want to set up Qlik Sense Enterprise SaaS, please contact your Qlik representative or Qlik Support to obtain a valid license for the setup.*

Each access type provides the Qlik Sense user with a certain type of access to Qlik Sense apps. A user with no access type cannot see any streams.

> *Application access only grants access to app objects in mashups, and not to the Qlik Sense hub or streams.*

Users

All user data is stored in the Qlik Sense Repository Service (QRS) database. You create user directory connectors in the QMC to be able to synchronize and retrieve the user data from a configured directory service. When a user logs in to Qlik Sense or the QMC, the user data is automatically retrieved. You can change the authentication method that handles the authentication of the Qlik Sense users.

Resource owners

The creator of a resource (for example, an app or a stream) is by default the owner of the resource. You can change the ownership for resources in the QMC.

1.2   Resource workflow

The following illustration gives an overview of the workflow of the resources.
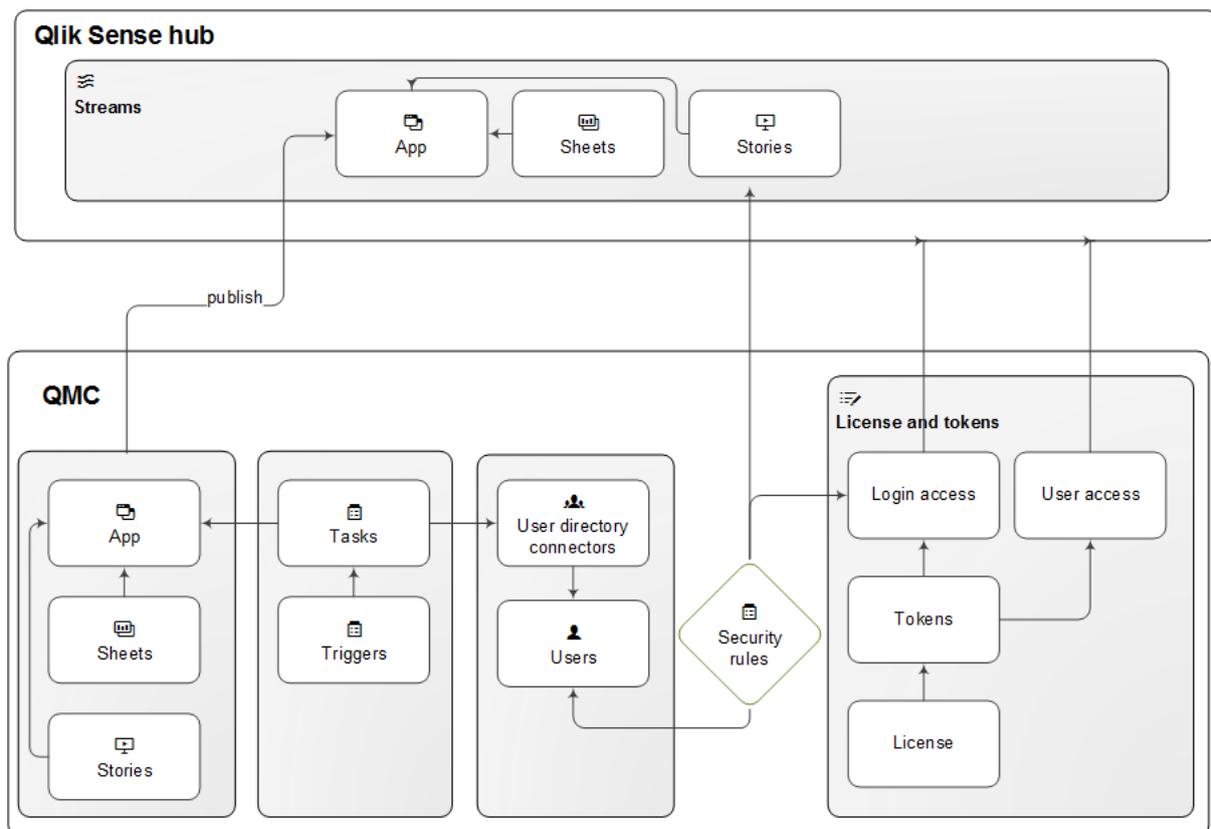
Resource overview and workflow for a token-based license

The apps, sheets, and stories are created from the Qlik Sense hub. Apps are published to streams from the Qlik Sense hub or from the QMC.

Tasks are available for apps and user directory connectors. The reload task is used to fully reload the data in an app from the source. The user sync task is applied to a user directory connector to synchronize the users from a user directory. Triggers can execute tasks.

A stream security rule is applied to the stream and affects the access rights for the users.

Token-based license: The site license provides for a number of tokens that are allocated to access types. Users are given access to streams and apps on the hub by login access or user access. A security rule is applied to the login access to specify which users the login access is available for.

User-based license: The site license provides for a number of professional and analyzer access allocations. Users are given access to streams and apps on the hub by their access.

> *The hub is not a part of the QMC. The hub is where Qlik Sense apps and sheets are opened and managed.*

1.3   Starting the QMC

A new session is started when you log in to the Qlik Management Console (QMC). You can start from one of the following situations:

- If the Internet browser tab with your previous session is still open you should see a **Login** dialog in the middle of the page. Click the **Login** button to start a new session.

- Otherwise, start the QMC from the Qlik Sense program group in the **Start menu** or enter the address of the QMC in the address field of your Internet browser.
    - By default, the QMC address is *https://<QPS server name>/qmc*.
    - Unencrypted communication is allowed if the proxy property **Allow HTTP** is selected. This means that both https (secure communication) and http (unencrypted communication) are allowed. Then the QMC address is *https://<QPS server name>:Service listen port HTTP/qmc* (where *https* can be replaced by *http*).

    > *You may be prompted to enter your user name and password.*

> *For non-Windows users, a login window will open in your browser. The **User name** should be entered in the format DOMAIN\user.*

The QMC opens at the **Start** page.

Starting the QMC for the first time after installation

The first time you access the QMC after a Qlik Sense installation you must activate the license.

Do the following:

1. Enter the address of the QMC in the address field of your Internet browser.
   The QMC opens at the **Site license** page.

   > *You may be prompted to enter your user name and password.*

2. Activate your license.
   This makes you the root administrator for the Qlik Sense site that is assigned to the RootAdmin role.
   There are two license models: the serial and control number and the signed license key. These models
   define the terms of your license and the access types that you can allocate to users. With a signed
   license key, you need internet access (direct or through a proxy) to access the cloud-based license
   backend, for user assignments, analytic time consumption, and product activations.
   There are two major license types: one based on access types, and one based on tokens.

   - Access types licenses are the Professional and Analyzer Users licenses (user-based) and
     Analyzer Capacity licenses (capacity-based). With a Professional and Analyzer Users license you
     can allocate professional access and analyzer access. With an Analyzer Capacity license you can
     allocate analyzer capacity access, where consumption is time based (analyzer time).
   - With a Qlik Sense Token license you use tokens to allocate access passes to users. You can
     allocate user access and login access.

   An access type allows users to access the hub and apps within a Qlik Sense Enterprise on Windows
   site.

   > *If you want to set up Qlik Sense Enterprise SaaS, please contact your Qlik representative or
   > Qlik Support to obtain a valid license for the setup.*

> *With a signed license key, license information can be viewed in the QMC after the license key is
> entered and saved using **Apply**.*

You have now started the your first QMC session. The next step is to allocate user access or professional
access to yourself.

Managing user access (page 317)

Managing professional access (page 307)

Logging out from the QMC

You can either logout from the QMC manually or be automatically logged out. Automatic logout occurs when
you have been inactive in your QMC session for longer than a predefined time limit. This time limit is set per
virtual proxy in the **Virtual proxy edit** page.

Do the following:

1. Click **username▼** in the top right of the page.
   Logout is displayed in the drop-down list.

2. Click **Logout**.
   The QMC welcome page is shown including a **Login** button.

> *Clicking **Login** on the welcome page will open the QMC start page. You may be prompted to enter your user name and password.*

1.4   Navigating in the QMC

Because of the associative structure of the QMC, you can select a resource in more than one way. For example, you can select an app either from the apps overview or from the **Associated items** for the stream that the app belongs to. Similarly, you can select a task either from the tasks overview or from the **Associated items** for the app that the task belongs to.

You can use the back and forward buttons of your Internet browser to move between the pages in the QMC. It is also possible to type the URL in the address field. For example, type *https://<QPS server name>/qmc/Users* to open the users overview page. Also, you can bookmark QMC pages in your Internet browser.

> *If you manage a certain resource often, it is a good idea to bookmark the page, for example, bookmark the apps overview page.*

You can save views that you often use as custom filters in the QMC. This lets you quickly access the data you need.

Keyboard shortcuts in the QMC

Qlik Sense supports keyboard accessibility. You can use keyboard controls to navigate the Qlik Management Console (QMC) and the Multi-Cloud Setup Console (MSC).

> *Keyboard shortcuts are expressed assuming that you are working in Windows. For Mac OS use Cmd instead of Ctrl.*

Qlik Management Console

Main actions

Shortcuts and their actions

Shortcut	Action
Esc	Close a filter dialog
Up arrow	Scroll up in tables

Shortcuts and their actions

Shortcut	Action
Down arrow	Scroll down in tables
Tab	Move to the next field on an edit page
Shift+Tab	Move to the previous field on an edit page
Esc	Close a dialog box
Ctrl+C	Copy selected text to clipboard
Ctrl+H	Open the Qlik Sense help
Ctrl+V	Paste last copied text from clipboard
Ctrl+X	Cut selected text and copy to clipboard
Ctrl+Z	Undo action (copy, paste, cut)
Ctrl+Y	Redo action (copy, paste, cut)
Backspace	On PC: Go back in navigation. On Mac: Delete selected item.

In tables

> The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.

Shortcuts and their actions

Shortcut	Action
Ctrl+A	Select all rows in the table
Esc	Deselect all selected rows
S	Open the **Search** popover
C	Open the Column selector
R	Refresh the table

On overview pages

Shortcuts and their actions

Shortcut	Action
Enter	Edit the selected rows
Delete	Delete the selected rows

On edit pages

Shortcuts and their actions

Shortcut	Action
Esc	Undo all changes, equivalent to clicking **Cancel**
Ctrl+S	Save and apply all the changes, equivalent to clicking **Apply**

In confirmation dialogs

Shortcuts and their actions

Shortcut	Action
Esc	Cancel
Enter	OK

Multi-Cloud Setup Console

Console

Shortcuts and their actions

Shortcut	Action
Left and right arrows	Navigate between menu tiles
Enter/Space bar	Select object

Deployments

Shortcuts and their actions

Shortcut	Action
Tab	Move to the next field
Up and down arrows	Navigate between list items
Enter/Space bar	Select object

UI icons and symbols

A symbol can be used in more than one context. Here is a list of the icons and symbols used throughout the Qlik Management Console (QMC) user interface.

UI icons

Icon	Meaning
⊕	Create new
⧉	Apps
Ⅱ◦	Content libraries
▰	Data connections
▰	Analytic connections
▱	App objects
≋	Streams
▤	Tasks
●	Users
☁	App distribution status/Cloud distribution
⛨	Audit
≔	Security rules
⛨	Custom properties
▦	License management
✦	Extensions
●	Tags
⊦	On-demand apps service
●	User directory connectors
≋	Monitoring apps
▤	Service cluster
▤	Nodes
⚙	Engines
▯	Printing
⤫	Proxies
⤫	Virtual proxies
▣	Schedulers

☰	Repositories
⤓	Distribution policies
↻	Load balancing rules
⚷	Certificates
🔗	Task chain
🔗	Task chain
•••	Task status: Never started, Skipped, Reset
↻	Task status: Triggered, Started, Abort initiated, Aborting, Retrying
⧗	Task status: Queued
⊗	Task status: Aborted
✓	Task status: Success
✕	Task status: Failed, Error
👁	Read access (by security rule)
✎	Update and/or Write and/or Edit access (by security rule)
⊗	Delete access (by security rule), Logout, Cancel, Close, Exit
🗃	Other access (by security rule), for example Create, ChangeOwner and/or Export
▼	Filter
?	Help
ⓘ	Information
◇	Information
🔒	Locked
🔓	Unlocked
🔍	Search
↩	Undo
⚙	Settings
▲	Arrow up
▼	Arrow down

◀	Arrow left
▶	Arrow right
🔖	Custom filters

The QMC start page

The start page in the Qlik Management Console (QMC) contains all the resources that you can manage in the Qlik Sense site. The resources you can manage depend on your access rights.
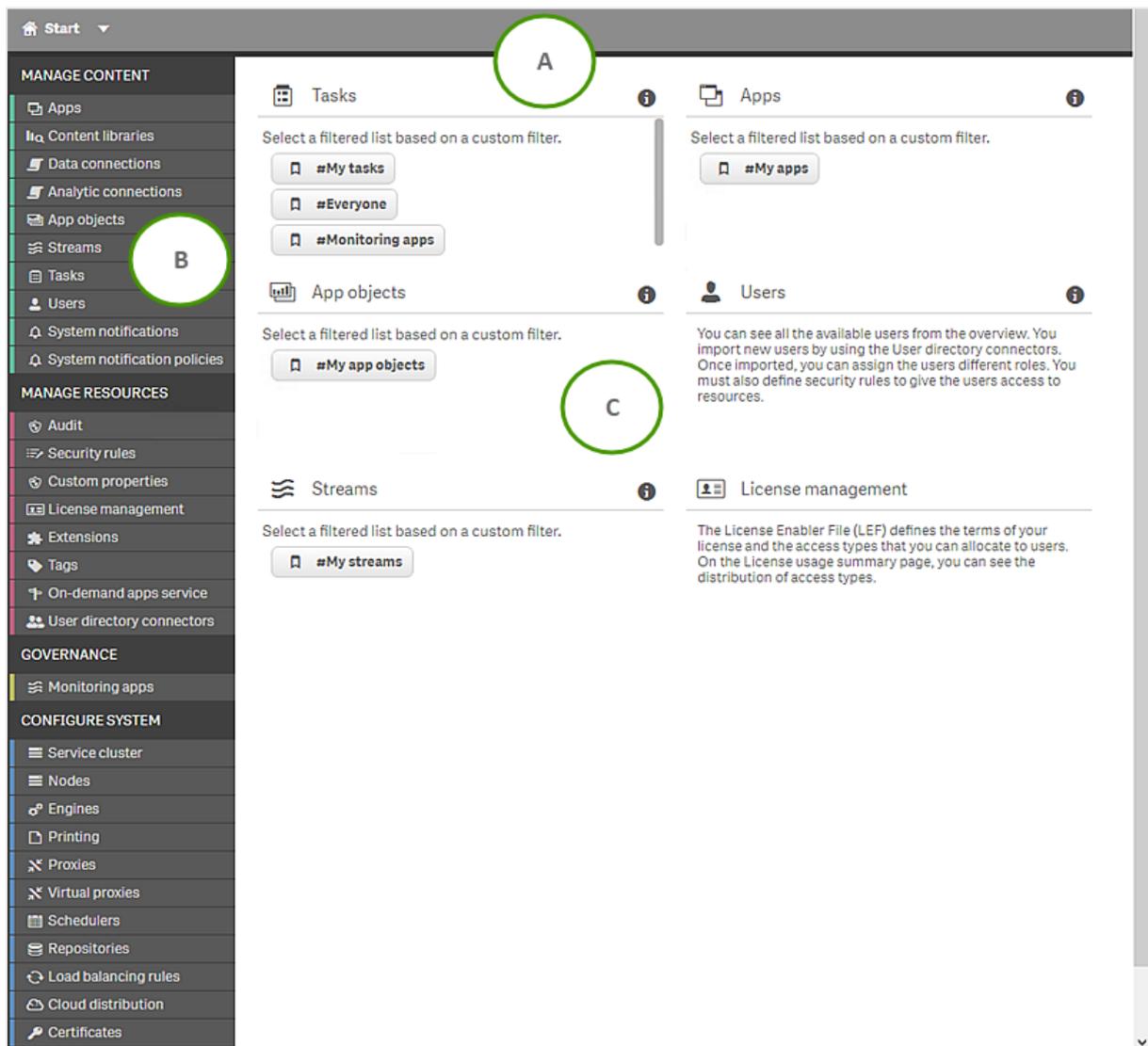
The QMC start page

The QMC start page interface legend descriptions

Legend letter	Description
A	The top bar is displayed from all pages to enable you to navigate the QMC efficiently. The following is possible: Click **Start** to access the QMC start page. Click ▼ next to **Start** to display a drop-down list of all resources. This enables you to select another resource without first having to access the start page. Click **Help** to access the (QMC) help. The top right corner displays who is logged in to the (QMC). Click the drop-down ▼ next to the login name and click **Logout** in the dialog to log out.
B	The left panel contains all QMC resources in groups. If any of the Qlik Sense services are down, the number of services that are not running is displayed with a numeral.
C	The basic resources are also available from the middle of the start page. Custom filters are listed for each resource. A number sign (#) indicates a predefined custom filter. Click a custom filter to go to the saved table view. Click to see information about the resource.

Resource overview page

When you select a resource from the start page, the resource overview is displayed. The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

By default, the overview page shows the most commonly used columns. You can add or remove columns in the column selector. In the table header bar, click to open the column selector. In the **Actions** menu, you can clear filters and search, select and deselect all rows, and toggle wrapping.
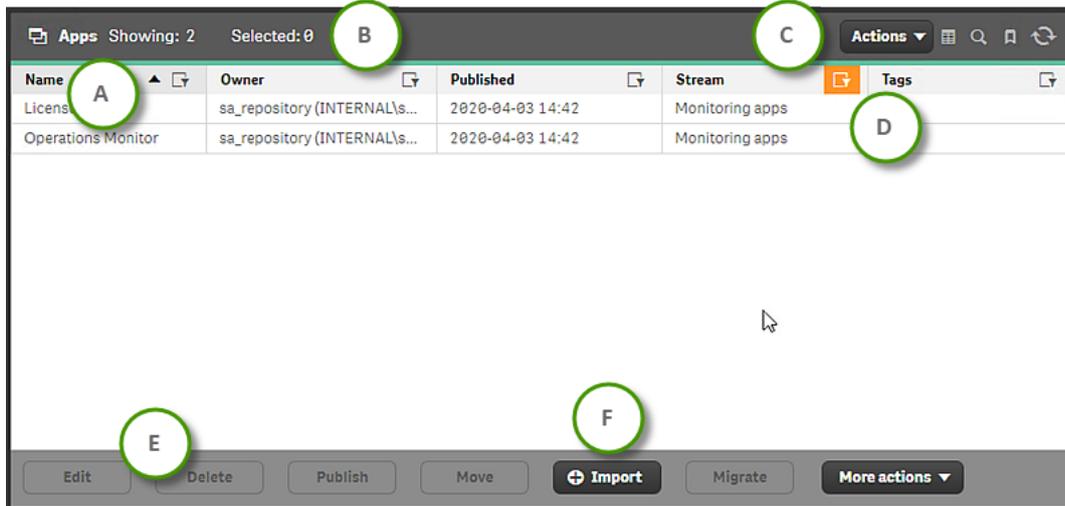
Apps overview page

Apps overview page legend descriptions

Legend letter	Description
A	Click a column heading to sort that column ascending ▼ or descending ▲. Click ⌐▼ next to sorting to display the filter dialog for the column. Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌐▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.
B	In the table header, to the left, a summary of the status of the current data set is displayed. **Total**: shows the total number of resources. **Showing**: shows the number of resources currently displayed. **Selected**: shows the number of selected resources.

C	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.
	*The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
	Click ⊞ to open the **Column selector**, where you can select which columns to display in the overview. Click ↰ to reset to default columns.
	Click ⎀ to open the **Custom filters** menu, where you can select, create, and delete custom filters. When a custom filter is applied, the button is highlighted.
	Click ↻ to refresh the data in the table. If there have been changes to the data, the button is highlighted.
D	You can create tags and apply them to resources so that you can search and manage the QMC content efficiently.
E	The action bar at the bottom of the page contains different action buttons depending on the selected resource type. For example, select an app in the overview and click **Edit** to open the **App edit** page.
	When you do not have update rights for the selected items, **Edit** is replaced by **View**.
	If you do not have delete rights for the selected items, **Delete** is disabled. If a resource is deleted, all load balancing rules and security rules associated with that resource are deleted automatically.
F	Click ⊕ in the action bar to create a new instance of a resource.
	In this example, click ⊕**Import** to open the **Import app** dialog.
	New rows are added to the bottom of the table. This is because the sort order is saved in the cache. Use sort or filter to trigger a full table reload.

Selections

The selection you previously made is still active when you display a resource overview, even if you have worked on another resource type in between.

Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.

Resource edit page

You edit resources from the edit page. You must have update right to be able to edit. If you do not have update rights you can view the page but you cannot edit. In this example you see the **Edit app** page.
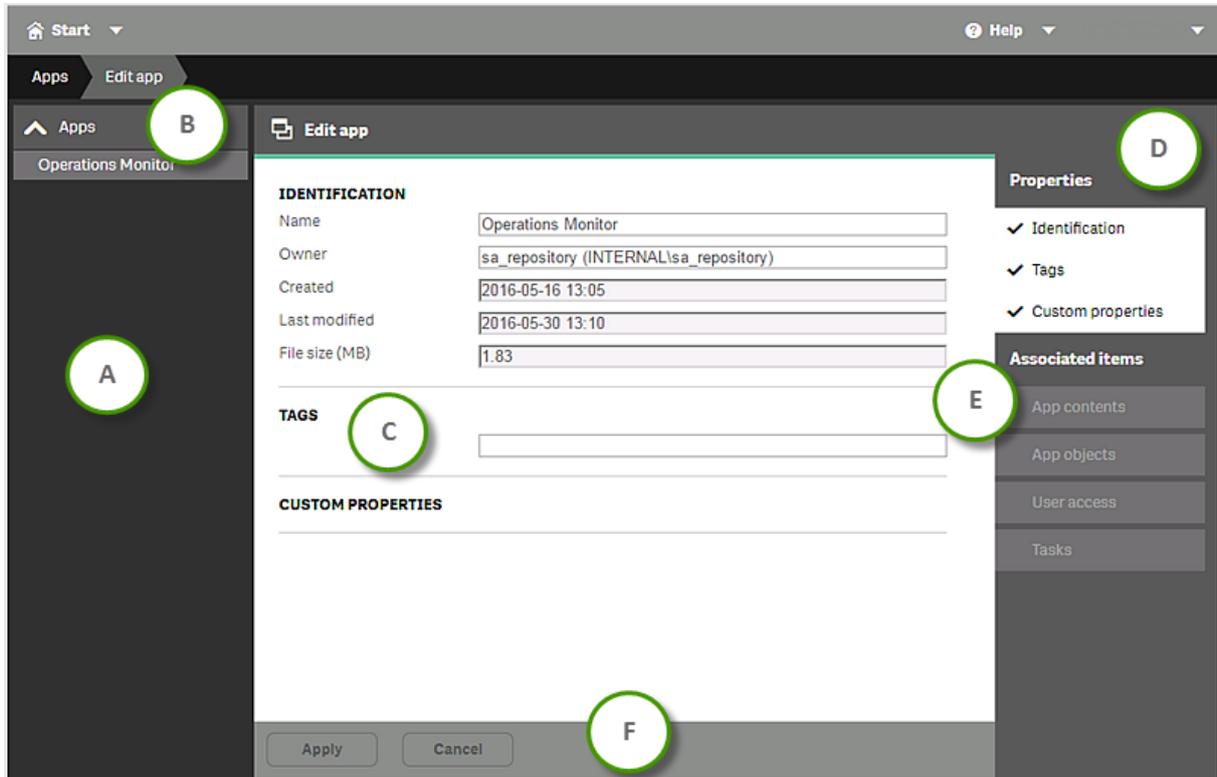
Example: The Edit app page

Edit app interface legend descriptions

Legend letter	Description
A	The selections panel, to the left, displays the resources you are currently editing. You can edit several resources at the same time to manage the QMC content efficiently.
B	Click **Apps** to return to the overview page where you can change your selection.
C	The edit page displays the properties that you select from the property groups in the right panel. If you select several items from the overview and they have different values for a specific field, *Multiple values* is displayed as the field value. Clicking ↰ next to a field cancels the changes in that field. If the communication with the QRS fails, the edit page is locked. Use the top bar to leave the page.
D	The **Properties** section displays the property groups containing the properties for the resource. You can display or hide properties on the edit page.
E	The **Associated items** section shows what items that are associated with this particular resource.

F	The action bar at the bottom of the page contains the **Apply** and **Cancel** buttons. Clicking **Cancel** resets all field values. **Apply** is disabled if a mandatory field is empty. The unsaved changes dialog is displayed if you leave the edited page without clicking **Apply**. Choose **Continue** to leave the edit page and undo all your changes or **Cancel** to stay on the edit page. If the communication with the QRS fails when you click **Apply**, an error message is displayed. You can continue editing or try clicking **Apply** again.

Searching and filtering in the QMC

You can use the in-built search tool to search in most tables in the QMC. You can perform simple searches quickly, and also create more advanced searches with several search criteria, arranged into subgroups. The search can be combined with column filtering to further limit the resulting list. You can save a filtered table view as a custom filter.

Search options

The following four options are available when you open search.

Search options

Search option	Description
A	Select an attribute to search on.
B	Select a condition for the search. In most cases, the conditions are **=**, **!=**, **Contains**, **Starts with**, and **Ends with**. In columns related to time, you have the conditions **Since**, **Before**, and **After**.
C	Click and select one of the available values, or type a string.
D	Add an additional search condition.

Simple search

Do the following:

1. To the right in the table header, click 🔍.
   Search is opened.
2. In the first drop-down list, select which attribute to search on.
3. In the second drop-down list, select a condition for the search.

---

4. Click the third list and select one of the available options, or type a string.
5. Click **Search**.

The table shows the matching items.

> ℹ️ *You clear search and filters by clicking ⊗ in the table header.*

Advanced search

When you want to make more advanced searches, you can combine several conditions of search criteria. The conditions are connected either with OR or AND. You can adjust the logical relationship between the rows by using **Group**, **Join**, or **Split**. By default, the rows are grouped.

Example:

The following search consists of four conditions.

The first condition is separated from the other conditions through the **Split** option.

The second condition is connected to the third and fourth conditions through a **Join**, and the third and fourth conditions, in turn, are grouped.

There are three ways in which these conditions can be met:

*   The first condition is met.
*   The second condition is met, in conjunction with condition three.
*   The second condition is met, in conjunction with condition four.

Filtering

Filtering can be used on its own or together with search. You can filter on multiple columns simultaneously.

Do the following:

1. Click ▼ in the column heading.
   The filter dialog for the column is displayed.
2. In the filter dialog, type a string to filter on. If available, you can instead select a predefined value.
3. Click outside of the filter dialog (or press Esc) to close the dialog.
   The ⬓▼ icon indicates that a filter is applied to the column.

The table shows the matching items.

Managing custom filters in table views

Custom filters help you easily find the content that you want to work with. For example, you might need to look at a specific set of tasks every day. Filter the tasks and then save the table view as a custom filter. Next time, use the custom filter to go directly to your set of tasks. An additional benefit is that only the items included in the filter are loaded, which reduces load time.

You can save the following settings in a custom filter:

- Search filters
- Column filters
- Sort order
- Sort column
- Column definition (which columns to show and the column width)

You create and manage custom filters for all resources from the **Custom filters** menu on the resource overview page.

Predefined custom filters

On the QMC start page you can use predefined custom filters. These are denoted by a number sign (#).

- **#My apps**, **#My app objects**, and **#My streams** show objects that you own.
- **#My tasks** shows tasks associated with apps that you own.
- The **Tasks** overview has one custom filter for each stream. They show tasks that are connected to the apps that are published to that stream.

Predefined custom filters have no settings for column layout. They only define filters and sort order. Update a predefined custom filter if you want to save a specific layout.

You can temporarily delete a predefined custom filter, but it is re-created when you refresh the browser.

Applying custom filters

When you apply a custom filter, the custom filter icon is highlighted. The currently applied custom filter has a check mark in the **Custom filters** menu. This is reset once you make any changes to the table.

If the custom filter that you apply includes filters, only a subset of the table data is loaded.

Do the following:

1. On the resource overview page, click to open the **Custom filters** menu.
2. Click **Use** next to the custom filter you want to apply.

> *For apps, app objects, tasks, and streams, custom filters are available on the QMC start page.*

Creating custom filters

You create a custom filter by first making the necessary edits to the table and then saving the result.

Do the following:

1. Go to the resource overview page.
2. Filter, sort, or make any column adjustments to save in a custom filter.
3. Click to open the **Custom filters** menu.
4. Type a name for the new custom filter and add a description.
5. Click .

Deleting custom filters

Do the following:

1. On the resource overview page, click to open the **Custom filters** menu.
2. Click next to the custom filter you want to delete.

> *The option **Clear** does not delete anything, it only removes the applied custom filter.*

Updating custom filters

You can update any custom filter with the current layout, filters, and sort order.

Do the following:

1. On the resource overview page, click to open the **Custom filters** menu.
2. Click **Update** next to the custom filter you want to update.

The selected custom filter will be updated with the new settings.

The custom filters user interface
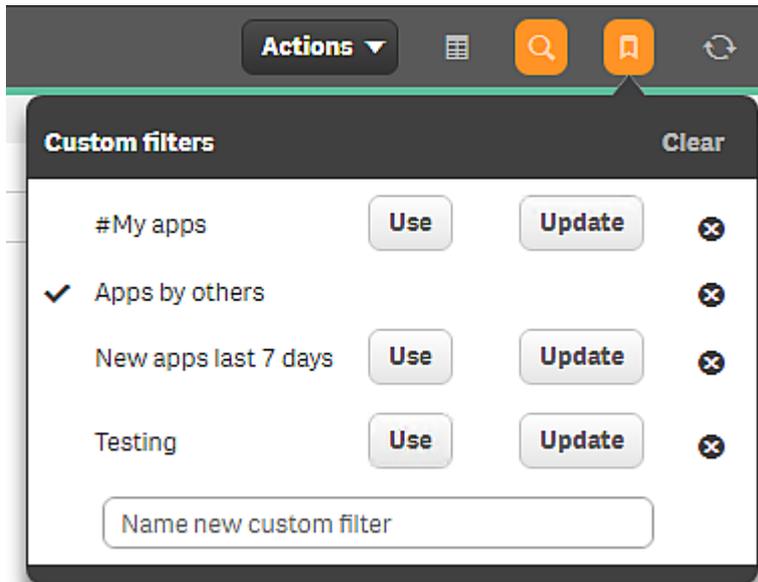
In the following user interface, the custom filter **Apps by others** is in use. Click **Clear** to clear the current filter. Nothing is deleted.

To apply a different filter, click **Use** for that filter. If you click **Update** that custom filter is updated with the current settings.

Delete a filter by clicking ⊗.

Example: Creating a custom filter for apps owned by others

This filter will only show apps created by other users.

Do the following:

1. On the QMC start page, click **Apps**.
   The apps overview section is opened.

2. Click 🔍 to open the search.

3. In the first list, select **Owner**.

4. In the second list, select **!=**.

5. In the text box, enter your user name.

6. Click **Search**.
   Now only apps owned by others are displayed.

7. Click 🔖 to open the **Custom filters** menu.

8. Name the new custom filter *Apps by others*.

9. Click ➕.
   Your new custom filter is saved and a check mark indicates that it is currently in use.

Example: Updating a custom filter

In this example you will update the predefined custom filter **#My apps** to sort apps by size.

Do the following:

1. On the QMC start page, select the custom filter **#My apps**.
   The apps section is opened and the custom filter is applied. Only your apps are shown.
2. Click ▦ to open the column selector and select **File size (MB)**.
3. Click the **File size (MB)** header to change the sorting order.
4. Click ⊓ to open the **Custom filters** menu.
5. On the row for **#My apps**, click **Update**.
6. The **#My apps** filter is updated and a check mark indicates that it is currently in use.

1.5   QMC resources overview

All resources that are available in the Qlik Management Console (QMC) are described briefly in the following table.

QMC resource descriptions

Resource	Description
▱ Apps	A Qlik Sense app is a task-specific, purpose-built application. The user who creates an app is automatically designated as the owner of the app. An app can be reused, modified, and shared with others.
	You can create and publish apps to streams from the Qlik Sense hub, if you have the appropriate access rights. Apps can also be published from the QMC. To publish an app that is created in a Qlik Sense Desktop installation, you must first import it from the QMC. The security rules applied to the app, stream, or user, determine who can access the content and what the user is allowed to do. The app is locked when published. Content can be added to a published app through the Qlik Sense hub in a server deployment, but content that was published with the original app cannot be edited.
▮Q Content libraries	A content library is a storage that enables the Qlik Sense users to add shared contents to their apps.
	The user who creates the content library automatically becomes the owner of that library. The library and the library objects can be shared with others through security rules defined in the QMC.

Data connections	Data connections enable you to select and load data from a data source. All data connections are managed centrally from the QMC. Data connections are created in the Qlik Sense data load editor. The user who creates a data connection automatically becomes the owner of that connection and is, by default, the only user who can access the data connection. The data connection can be shared with others through security rules defined in the QMC.
	When you import an app developed on Qlik Sense Desktop, existing data connections are imported to the QMC. When you export an app from a server, existing data connections are not exported with the app.
	If the name of a data connection in the imported app is the same as the name of an existing data connection, the data connection will not be imported. This means that the imported app will use the existing data connection with an identical name, not the data connection in the imported app.
Analytic connections	With analytic connections you are able to integrate external analysis with your business discovery. An analytic connection extends the expressions you can use in load scripts and charts by calling an external calculation engine (when you do this, the calculation engine acts as a server-side extension (SSE)). For example, you could create an analytic connection to R, and use statistical expressions when you load the data.
App objects	You can manage the following app objects: • Sheets • Stories The user who creates an app is automatically designated as the owner of the app and its app objects. The app objects are published when the app they belong to is published. The users can add private app objects to the apps and share them by publishing the app objects from Qlik Sense.

≋ **Streams**	A stream enables users to read and/or publish apps, sheets, and stories. Users who have publish access to a stream create the content for that specific stream. The stream access pattern on a Qlik Sense site is determined by the security rules for each stream. By default, Qlik Sense includes two streams: **Everyone** and **Monitoring apps**.
	An app can be published to only one stream. However, if you duplicate the app to create a copy, you can publish the copy to another stream. Apps can be moved between streams.
	In the hub, streams with no apps—either empty streams or streams that do not show apps due to the existing security rules for a user—will not appear. After you publish an app, move it from another stream, or delete it, the list of streams will update dynamically and the stream will appear in the hub or be hidden depending on whether it contains at least one app. Changes outside of the hub, for example in QMC, will not trigger an update to the stream list in the hub.
	*All authenticated users have read and publish rights to the **Everyone** stream and all anonymous users read-only rights. Three of the predefined admin roles (RootAdmin, ContentAdmin, and SecurityAdmin), have read and publish rights to the Monitoring apps stream.*
▦ **Tasks**	Tasks are used to perform a wide variety of operations and can be chained together in just any pattern. The tasks are handled by the Qlik Sense Scheduler Service (QSS). There are four types of tasks:
	- Reload - User synchronization - External program - Distribution
	Execution of a task is initiated by a trigger or manually from the tasks overview page. You can create additional triggers to execute the task, and there are two types of triggers:
	- Scheduled - Task event
👤 **Users**	Users are imported from a user directory via a user directory connector in the QMC.

⌂ **System notifications**	You can create custom notifications to be pushed to users through the Qlik Sense Mobile Client Managed app on their mobile devices.
	System notifications and System notification policies features are available only on Qlik Sense Enterprise on Windows installations licensed with a signed key. For more information on licenses, see: Qlik Sense licenses documentation.
⌂ **System notification policies**	You create system notification policies to determine to which users a system notification is distributed. By creating a system notification policy, you can customize the pool of users or groups of users that receive the notification on their mobile devices.
	System notifications and System notification policies features are available only on Qlik Sense Enterprise on Windows installations licensed with a signed key. For more information on licenses, see: Qlik Sense licenses documentation.
⛨ **Audit**	On the QMC audit page, you can query for resources and users, and audit the security rules, load balancing rules, or license rules that have been defined in the Qlik Sense system.
⊞✎ **Security rules**	The Qlik Sense system includes an attribute-based security rules engine that uses rules as expressions to evaluate what type of access users should be granted for a resource.
⛨ **Custom properties**	You create a custom property to be able to use your own values in the security rules. You define one or more values for the custom property, and use these in the security rule for a resource.

🪪 **License management**	There are two license models: the serial and control number and the signed license key. These models define the terms of your license and the access types that you can allocate to users. With a signed license key, you need internet access (direct or through a proxy) to access the cloud-based license backend, for user assignments, analytic time consumption, and product activations. There are two major license types: one based on access types, and one based on tokens. • Access types licenses are the Professional and Analyzer Users licenses (user-based) and Analyzer Capacity licenses (capacity-based). With a Professional and Analyzer Users license you can allocate professional access and analyzer access. With an Analyzer Capacity license you can allocate analyzer capacity access, where consumption is time based (analyzer time). • With a Qlik Sense Token license you use tokens to allocate access passes to users. You can allocate user access and login access. An access type allows users to access the hub and apps within a Qlik Sense Enterprise on Windows site. ℹ️ *If you want to set up Qlik Sense Enterprise SaaS, please contact your Qlik representative or Qlik Support to obtain a valid license for the setup.*
🧩 **Extensions**	Extensions can be several different things: A widget library, a custom theme, or a visualization extension, used to visualize data, for example, in an interactive map where you can select different regions.
🏷️ **Tags**	You create tags and apply them to resources to be able to search and manage the environment efficiently from the resource overview pages in the QMC.
🪧 **On-demand apps**	Selection and template apps, as well as on-demand apps are published to streams from the QMC.

👪 **User directory connectors**	The user directory connector (UDC) connects to a configured directory service to retrieve users. The UDCs supplied with the Qlik Sense installation are Generic and Advanced LDAP, Active Directory, ApacheDS, ODBC, Access (via ODBC), Excel (via ODBC), SQL (via ODBC), and Teradata (via ODBC).
	ℹ️ *No UDC is required for a local user to log on to Qlik Sense. However, for the local user to be able to access apps, you need to allocate access. With a user-based license, you can use professional or analyzer access rules. With a token-based license, you can use user or login access rules to allocate access. Alternatively, a local user can first log on to be recognized as a user, and then be allocated tokens.*
	You create new user directory connectors in the QMC.
≋ **Monitoring apps**	A stream that contains the governance apps License Monitor and Operations Monitor that present data from the Qlik Sense log files.
≣ **Service cluster**	On a multi-node site, the service cluster stores configurations, such as persistence type, database connection, and static content folder, for all nodes. All nodes are linked to the service cluster so that the settings can be unified.
≣ **Nodes**	A node is a server that is using the configured Qlik Sense services. There is always a central node in a deployment and nodes can be added for different service configurations. There is always a repository on every node.
	A Qlik Sense site is a collection of one or more server machines (that is, nodes) connected to a common logical repository or central node.
	ℹ️ *In a Shared Persistence multi-node installation, you can make one or more nodes failover candidates. In the case of a central node failure, a failover candidate will assume the role of central node.*
	ℹ️ *In a multi-node installation, you manage the whole Qlik Sense Enterprise on Windows site from the QMC on the central node. You can access the QMC from rim nodes, but requests from the QMC towards the repository are routed to the repository on the central node.*
⚙️ **Engines**	The Qlik Sense Engine Service (QES) is the application service that handles all application calculations and logic.
🗎 **Printing**	The Qlik Sense Printing Service (QPR) manages the export and printing of objects to PDF or image files.

⤢ **Proxies**	The Qlik Sense Proxy Service (QPS) manages the Qlik Sense authentication, session handling, and load balancing.
⤢ **Virtual proxies**	One or more virtual proxies run on each Qlik Sense Proxy Service (QPS), making it possible to support several sets of site authentication, session handling, and load balancing strategies on a single proxy node.
⌚ **Schedulers**	The Qlik Sense Scheduler Service (QSS) manages the scheduled tasks (reload of Qlik Sense apps or user synchronization) and task chaining. Depending on the type of Qlik Sense deployment, the QSS runs as manager, worker, or both on a node.
🗄 **Repositories**	The Qlik Sense Repository Service (QRS) manages persistence and synchronization of Qlik Sense apps, licensing, security, and service configuration data. The QRS attaches to a Qlik Sense Repository Database and is needed by all other Qlik Sense services to run and to serve Qlik Sense apps. In addition, the QRS stores the Qlik Sense app structures and the paths to the binary files (that is, the app data stored in the local file system).
↻ **Load balancing rules**	The load balancing defines the nodes' access rights to resources.
☁ **Cloud distribution**	The following sections are available if you have a license with multi-cloud: • **App distribution status**: Monitor the distribution of apps. • **Distribution policies**: Determine whether a published app can be distributed to deployments in Qlik Sense Enterprise SaaS. To be distributed, a published app must have a distribution policy connected to it. • **Deployment setup**: Configuring a deployment in Qlik Sense Enterprise on Windows.
🔑 **Certificates**	Qlik Sense uses certificates for authentication. A certificate provides trust between nodes within a Qlik Sense site. The certificates are used within a Qlik Sense site to authenticate communication between services that reside on multiple nodes.
ⓘ **Custom banner messages**	Publish custom banner messages in the hub to announce and inform users about important information. Choose from four banner styles—Standard (green), Information (blue), Warning (yellow), and Error (red)—to indicate the type of message displayed, and set the length of time that the banner will appear in the hub. The default duration is 10 seconds.
Log collector	With the log collector, you can collect and export log files from a period that you define. The logs facilitate troubleshooting for Qlik Support.

Apps

A Qlik Sense app is a task-specific, purpose-built application. The user who creates an app is automatically designated as the owner of the app. An app can be reused, modified, and shared with others.

You can create and publish apps to streams from the Qlik Sense hub, if you have the appropriate access rights. Apps can also be published from the QMC. To publish an app that is created in a Qlik Sense Desktop installation, you must first import it from the QMC. The security rules applied to the app, stream, or user, determine who can access the content and what the user is allowed to do. The app is locked when published. Content can be added to a published app through the Qlik Sense hub in a server deployment, but content that was published with the original app cannot be edited.

You can also duplicate, reload, import, export, or delete an app from the QMC.

The **Apps** overview lists all the available apps. The apps are shown as links. Click a link to open the app in the hub. You cannot be sure that all the apps that are shown can be opened in the hub. Security rules applied to the hub may prevent you from opening the app. Unpublished apps can only be opened if you are the app owner. If you don't have access rights to the app, you will still be redirected to the hub where a message is displayed that access is denied.

Limitation: If you try to open an app through a virtual proxy which isn't the default virtual proxy, the app is still opened using the default proxy.

The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

> 💡 *You can adjust the column width by dragging the header border.*

App properties

Property	Description
Name	The name of the app.
Owner	The owner of the app.
Published	The date that the app was published.
Stream	The stream that the app is published to.
Tags	The tags that are connected to the app.
Target app ID	The app ID of the published original app that you have duplicated. When you create a copy of a published app and want to replace the original app, the target app ID is used to identify it.
Description	The app description, if any.

Property	Description
File size (MB)	The file size of the app. *The app file size displayed in the QMC differs from the file size on disk. This is because the size in the QMC only includes data objects, such as fields, tables, and document properties, and not visualizations, bookmarks, measures, etc, that are also included in the .qvf file.*
Last reload	When the app was last reloaded.
ID	The app ID.
Created	The date and time when the app was created.
Last modified	This field is updated under the following conditions: • Change of app title. • Change of app description. • Change of app thumbnail. • Publishing of app. • Moving of app between streams. • Reload of app data. This field is not updated under the following conditions: • Change of sheets, visualizations, stories, and bookmarks. • Change in visualization settings. • Change in app options.
Modified by	By whom the app was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌧	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌧ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*

Property	Description
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↩ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.
Edit	Edit the selected apps. The number next to **Edit** indicates the number of items in your selection that you are allowed to edit.When you do not have update rights for the selected items, **Edit** is replaced by **View**.
View	View the selected apps. When you do not have update rights for the selected items, **Edit** is replaced by **View**.
Delete	Delete the selected apps. The number next to **Delete** indicates the number of items that will be deleted.If you do not have delete rights for the selected items, **Delete** is disabled.
Publish	Publish the selected apps.
➕ **Import**	Import a new app.
More actions > **Export**	Export the selected app.
More actions > **Duplicate**	Duplicate the selected app.
More actions > **Reload now**	Reload the selected app. *In a multi-node site, where the Qlik Sense Scheduler Service (QSS) on the central node runs as manager and the QSSs on the rim nodes run as workers, the task might fail the first time it is triggered through **Reload now**. This is because the task has not yet been synced from the manager QSS to the worker QSSs. The second time the action is performed, the task will work.*

Property	Description
More actions > Create new reload task	Create a new reload task.
More actions > Trigger distribution	Trigger distribution of the selected app. *In a multi-node site, where the Qlik Sense Scheduler Service (QSS) on the central node runs as manager and the QSSs on the rim nodes run as workers, the task might fail the first time it is triggered through **Trigger distribution**. This is because the task has not yet been synced from the manager QSS to the worker QSSs. The second time the action is performed, the task will work.*
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.

App: associated items

The tables in this document show the fields available for the **Contents** and **Security rules** property groups.

By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

You can adjust the column width by dragging the header border.

App contents

App contents is available from **Associated items** when you edit apps. The overview contains a list of app contents (images) associated with the selected apps.

App contents properties

Property	Description
File name	The name of the app content file.
Location	The location of the app content. Example: *%RepositoryRoot%\AppContent\[App ID]\[App content file]*
URL path	The path to the app content. Example: */AppContent/[App ID]/[App content file]*.
File size (KB)	The size of the app content file.

Property	Description
App	The app that the app content belongs to.
ID	The ID of the app content.
Created	Date and time when the app content was created.
Last modified	Date and time when the app content was last modified.
Modified by	By whom the app content was modified.

App objects

App objects is available from **Associated items** when you edit apps. The overview contains a list of app objects associated with the selected apps.

App object properties

Property	Description
Name	The name of the app object.
Type	The type of app object: sheet or story.
Owner	The owner of the app object.
Approved	The status of the app object: • **Not approved**: The app object is not approved because it was added to a published app. • **Approved**: The app object is approved because it belonged to the app when the app was published.
Published	The status of the app object: • **Not published**: The app object is not published to a stream. • **Published**: The app object is published to a stream. There are two alternatives: The app object itself has been published from Qlik Sense, or the app that the app object belongs to, has been published from Qlik Sense or from the Qlik Management Console.
Last modified	Date and time when the app object was last modified.
App	The app that the app object belongs to.
Tags	The app object tags.
ID	The ID of the app object.
Created	Date and time when the app object was created.
Modified by	By whom the app object was modified.

If you make a selection in the overview and click **Edit** in the action bar, the app object edit page is displayed.

User access

User access is available from **Associated items** when you edit a resource.

The preview shows a grid of the target resources and the source users who have access to the selected items.

Depending on rights, you can either edit or view a user, a resource, or an associated rule.

Tasks

Tasks is available from **Associated items** when you edit apps. The overview contains a list of tasks associated with the selected apps.

Task properties

Property	Description
Name	The name of the task.
Type	The type of task.
App	The name of the app associated with the task.
Enabled	Status values: **Yes** or **No**.
Status	The task status.
Tags	The name of the app associated with the task.
Partial reload	Load only data recently changed.
Max retries	The maximum number of reload retries.
ID	The ID of the task.
Created	Date and time when the task was created.
Last modified	Date and time when the task was last modified.
Modified by	By whom the task was modified.
Custom properties	Custom properties, if any, are listed here.

If you make a selection in the overview and click **Edit** in the action bar, the task edit page is displayed.

App contents

A Qlik Sense app is a task-specific, purpose-built application. The user who creates an app is automatically designated as the owner of the app. An app can be reused, modified, and shared with others.

When importing an app to a server, or exporting an app from a server, related content that is not stored in the .qvf file, such as images, is also moved. The related content is stored in a separate folder: *%ProgramData%\Qlik\Sense\Repository\AppContent\<App ID>*. Each app has its own app content folder, with the app ID as the folder name.

> *Content that is uploaded to the AppContent folder is only available for that specific app. If you want content to be available for other apps, use the **Content libraries**.*

Uploading an image to the app content folder

On the **App contents** page in the QMC, you can upload files (images) for use in a specific app. The files are saved in the app content folder.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the app that you want to upload images to and click **Edit**.
4. On the **App edit** page, under **Associated items**, select **App contents**.
5. Click ⊕ **Upload**.
   A file selection dialog is displayed.
6. Click the button for selecting the files to upload, select the files and click **Upload**.

The files are uploaded and displayed in the **App contents** list.

> *The Qlik Sense Repository Service scans for script tags in XML files uploaded to AppContent or Content Library.*

Deleting an image in the app content folder

On the **App contents** page in the QMC, you can delete files (images) from an app. The files are deleted from the app content folder.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the app that you want to delete images from and click **Edit**.
4. On the **App edit** page, under **Associated items**, select **App contents**.
5. In the **App contents** list, select the files that you want to delete.
   (The URL paths contain the file names.)
6. Click **Delete**.
   A confirmation dialog is displayed.
7. Click **OK**.

Content libraries

A content library is a storage that enables the Qlik Sense users to add shared contents to their apps.

The user who creates the content library automatically becomes the owner of that library. The library and the library objects can be shared with others through security rules defined in the QMC.

The **Content library** overview lists all the content libraries in the Qlik Sense site.

The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

💡	*You can adjust the column width by dragging the header border.*

The **Content library** fields and values

Field	Value
Name	The name of the content library.
Owner	The owner of the content library.
Tags	The tags that are connected to the content library.
ID	The ID of the content library. By default, not displayed.
Created	The date and time when the content library was created.
Last modified	The date and time when the content library was last modified.
Modified by	By whom the content library was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
�	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. ℹ️ *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.

🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.
Edit	Edit the selected content libraries. When you do not have update rights for the selected items, **Edit** is replaced by **View**.
View	View the selected content libraries. When you do not have update rights for the selected items, **Edit** is replaced by **View**.
Delete	Delete the selected content libraries. If you do not have delete rights for the selected items, **Delete** is disabled.
Upload	Upload library objects to the selected content library. ⓘ *The Qlik Sense Repository Service scans for script tags in XML files uploaded to AppContent or Content Library.*
➕ **Create new**	Create a new content library.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

💡 *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

Content library: associated items

The tables in this document show the fields available for the **Contents** and **Security rules** property groups.

By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

💡 *You can adjust the column width by dragging the header border.*

Contents

Contents is available from **Associated items** when you edit a content library.

The overview contains a list of the contents that are associated with the selected content library.

The **Contents** property group fields

Property	Description
File name	The name of the object file.
Location	The location where the object is saved: *\Content\<Content library name>\<file name>*.
URL path	The object's URL path: */content/<Content library name>/<file name>*.
File size (KB)	The file size in kilobytes.
ID	The ID of the object.
Created	The Date and time when the object was created.
Last modified	The Date and time when the object was last modified.
Modified by	By whom the object was modified.

Content cache-controls

There are potential security risks with cached content. Browsers may store a local cached copy of content received from web servers. Some browsers cache content accessed via HTTP/HTTPS. If sensitive information in application responses is stored in the local cache, this information can be retrieved by other users who have access to the same computer at a future time.

With content cache-controls, you can modify the cache behavior of the browser to prevent such risks.

The **Content cache-control** property group fields

Property	Description
name	Name of the content cache-control.

Property	Description
regex filter	Regular expression to filter out matching URLs to which the cache settings are applied:
	`(.*?)` - matches everything
	`(resources|appcontent)` - matches requests containing "resources" OR "appcontent" in the URI, for example:
	/resources/hub/img/core/static/Default_thumbnail_app.svg
	/appcontent/126610c6-1a6f-4d1b-8126-a7fbb040b44d/Icon_License_grey.png
	For repository use the standard `System.Text.RegularExpressions.Regex` class. The comparison is made by :
	`regex = new Regex(contentCacheControl.Filter)`
	`regex.IsMatch(httpRequest.RawUrl);`
	For hub it is the standard nodejs RegExp:
	`regex = new RegExp(contentCacheControl.Filter)` `regex.test("/api/hub" + res.req.originalUrl);`
maxAge	Maximum age for cached content to be included. The default value 3600 (seconds) can be edited.
cachePolicy	**Public, max-age**: The cached response is sent without revalidation.
	Public, must-revalidate, max-age=0: Requires a cache to revalidate stale responses before using a cached response.
	Private, max-age: The cached response is sent without revalidation. All or part of the response message is intended for a single user and must not be cached by a shared cache.
	Private, must-revalidate, max-age=0: A normally uncacheable response is cacheable, but requires a cache to revalidate stale responses before using a cached response. All or part of the response message is intended for a single user and must not be cached by a shared cache.
	No-store: The response cannot be reused.
ID	ID of the object.
Created	Date and time when the object was created.
Last modified	Date and time when the object was last modified.
Modified by	By whom the object was modified.

Before modifying the cache-controls

Please note the following before modifying cache control headers:

- It is generally not recommended to manually alter the cache-control headers.
- Make sure that you understand how the browser caching behavior is affected by the changes.
- Prior to applying any changes in a production environment, evaluate the risks of the changes.

Linking a new content cache-control

The cache-control has no owner. It has a mandatory reference to a content library and will only affect resources in that library that match the regular expression in the **regex filter** setting.

Do the following:

1. In the QMC, open **Content libraries**.
2. Double-click the content library to which you want to add content cache-controls.
3. Under **Associated items**, open **Content cache-controls**.
4. Click **Link new content cache control**.
5. Fill in the fields.
   name and **regex filter** are mandatory. **maxAge** is stated in seconds and can be edited.
6. Click **Add**.

See also: *Configuring content cache-controls (page 512)*

User access

User access is available from **Associated items** when you edit a resource.

The preview shows a grid of the target resources and the source users who have access to the selected items.

Depending on rights, you can either edit or view a user, a resource, or an associated rule.

Security rules

Security rules is available from **Associated items** when you edit a content library. The overview contains a list of the security rules that are associated with the selected content library.

The **Security rules** property group contains the user condition properties.

User condition properties

Property	Description
Name	The name of the security rule.
Description	The description of what the rule does.
Resource filter	The ID for the rule.
Actions	The permitted actions for the rule.
Disabled	Status values: **Yes** or **No**.
Context	The security rule context (**QMC**, **Hub**, or **Both**).
Type	The security rule type (**Default**, **Read only**, or **Custom**).
Conditions	The security rule conditions.

Property	Description
ID	The ID of the security rule.
Created	Date and time when the security rule was created.
Last modified	Date and time when the security rule was last modified.
Modified by	By whom the security rule was modified.

> *If you make a selection in the overview and click **Edit** in the action bar, the edit security page is displayed.*

Data connections

Data connections enable you to select and load data from a data source. All data connections are managed centrally from the QMC. Data connections are created in the Qlik Sense data load editor. The user who creates a data connection automatically becomes the owner of that connection and is, by default, the only user who can access the data connection. The data connection can be shared with others through security rules defined in the QMC.

When you import an app developed on Qlik Sense Desktop, existing data connections are imported to the QMC. When you export an app from a server, existing data connections are not exported with the app.

> *If the name of a data connection in the imported app is the same as the name of an existing data connection, the data connection will not be imported. This means that the imported app will use the existing data connection with an identical name, not the data connection in the imported app.*

> *To give access to the data connection to other users than the owner, edit the connection or go the **Security rules** page.*

The **Data connections** overview lists all the available data connections.

By default, the QMC contains two data connections: ArchivedLogsFolder and ServerLogFolder. These are the data connections for the two monitoring apps, License Monitor and Operations Monitor, which are installed together with the QMC. For users with admin roles (root, security, content, and deployment), the data connections are available in the data load editor in the Qlik Sense hub.

The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

> *You can adjust the column width by dragging the header border.*

Field descriptions

Field	Description
Name	The name of the data connection.
Owner	The owner of the data connection.
Tags	The tags that are connected to the data connection.
Connection string	The connection string for the data connection. Typically, includes the name of the data source, drivers, and path.
Type	The type of data connection. Standard data connections include ODBC, OLEDB, and Folder.
User ID	The user ID that is used in the connection string.
ID	The ID of the data connection. By default, not displayed.
Created	The date and time when the data connection was created.
Last modified	The date and time when the data connection was last modified.
Modified by	By whom the data connection was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⧨	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⧨ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. ⓘ *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↩ to reset to the default columns.

⌕	Search – both basic and more advanced searches.
	Searching and filtering in the QMC (page 25)
↻	Refresh the page.
Edit	Edit the selected data connections.
Delete	Delete the selected data connections.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

> *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

Data connection: associated items

The tables in this document show the fields available for the **Contents** and **Security rules** property groups.

By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

> *You can adjust the column width by dragging the header border.*

User access

User access is available from **Associated items** when you edit a resource.

The preview shows a grid of the target resources and the source users who have access to the selected items.

Depending on rights, you can either edit or view a user, a resource, or an associated rule.

Security rules

Security rules is available from **Associated items** when you edit data connections. The overview contains a list of the security rules that are associated with the selected data connections.

The **Security rules** property group contains the user condition properties.

User condition properties

Property	Description
Name	The name of the security rule.
Description	The description of what the rule does.
Resource filter	The ID for the rule.
Actions	The permitted actions for the rule.

Property	Description
Disabled	Status values: **Yes** or **No**.
Context	The security rule context (**QMC**, **Hub**, or **Both**).
Type	The security rule type (**Default**, **Read only**, or **Custom**).
Conditions	The security rule conditions.
ID	The ID of the security rule.
Created	Date and time when the security rule was created.
Last modified	Date and time when the security rule was last modified.
Modified by	By whom the security rule was modified.

If you make a selection in the overview and click **Edit** in the action bar, the security rule edit page is displayed.

Analytic connections

With analytic connections you are able to integrate external analysis with your business discovery. An analytic connection extends the expressions you can use in load scripts and charts by calling an external calculation engine (when you do this, the calculation engine acts as a server-side extension (SSE)). For example, you could create an analytic connection to R, and use statistical expressions when you load the data.

Analytic connections support up to 200 parameters.

The **Analytic connections** overview lists all the available analytic connections. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

> *For the **Analytic connections** to appear on the start page, it is a prerequisite that the virtual proxy used for accessing the QMC has a load balancing server. On the **Edit virtual proxy** page, under **Load balancing**, make sure that there is a server node for load balancing.*

Analytic connection properties

Property	Description
Name	Name of the analytic connection. Must be unique and must not start with numbers. Mapping/alias to the plugin that will be used from within the expressions in the app using the plugin functions, for example, SSEPython for a Python plugin or R for an R plugin.
Host	Host of the analytic connection, for example, *localhost* if on the same machine or *mymachinename.qlik.com* if located on another machine.
Port	Port to use when connecting (integer).

Property	Description
Certificate file path	The full path to the certificate: *C:\ProgramData\Qlik\Sense\Repository\Exported Certificates\<server name>*. The path should point to the folder containing both the client and server certificates and keys. This path just points to the folder where the certificates are located. You have to make sure that they are actually copied to that folder. The names of the three certificate files must be the following: *root_cert.pem*, *sse_client_ cert.pem*, *sse_client_key.pem*. Only mutual authentication (server and client authentication) is allowed. *It is optional to set the certificate file path, but the connection is insecure without a path.*
Reconnect timeout (seconds)	Default value: 20
Request timeout (seconds)	Default value: 0
ID	ID of the analytic connection.
Created	Date and time when the analytic connection was created.
Last modified	Date and time when the analytic connection was last modified.
Modified by	By whom the analytic connection was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌄	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌄ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*

Property	Description
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. ⓘ *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
◯	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.
Edit	Edit the selected connection.
Delete	Delete the selected connection.
⊕ **Create new**	Create a new connection.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

App objects

The **App objects** overview lists app objects in the Qlik Sense site.

You can manage the following app objects:

- Sheets
- Stories

The user who creates an app is automatically designated as the owner of the app and its app objects. The app objects are published when the app they belong to is published. The users can add private app objects to the apps and share them by publishing the app objects from Qlik Sense.

The app objects overview lists all the available app objects. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

> 💡 *You can adjust the column width by dragging the header border.*

App object properties

Property	Description
Name	The name of the app object.
Type	The type of app object: sheet or story.
Owner	The owner of the app object.
Approved	The status of the app object: • **Not approved**: The app object is not approved because it was added to a published app. • **Approved**: The app object is approved because it belonged to the app when the app was published.
Published	The status of the app object: • **Not published**: The app object is not published to a stream. • **Published**: The app object is published to a stream. There are two alternatives: The app object itself has been published from Qlik Sense, or the app that the app object belongs to, has been published from Qlik Sense or from the Qlik Management Console.
Last modified	The date and time when the app object was last modified.
App	The name of the app that the app object belongs to.
Stream	The name of the stream that the app object belongs to.
Tags	The tags that are connected to the app object.
ID	The ID of the app object.
Created	The date and time when the app object was created.
Modified by	By whom the app object was modified.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌐▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌐▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*

Property	Description
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↩ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.
Edit	Edit the selected app objects. When you do not have update rights for the selected items, **Edit** is replaced by **View**.
View	View the selected app objects. When you do not have update rights for the selected items, **Edit** is replaced by **View**.
Delete	Delete the selected app objects. If you do not have delete rights for the selected items, **Delete** is disabled.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.

App object: associated items

The tables in this document show the fields available for the **Contents** and **Security rules** property groups.

By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

User access

User access is available from **Associated items** when you edit a resource.

The preview shows a grid of the target resources and the source users who have access to the selected items.

Depending on rights, you can either edit or view a user, a resource, or an associated rule.

Streams

A stream enables users to read and/or publish apps, sheets, and stories. Users who have publish access to a stream create the content for that specific stream. The stream access pattern on a Qlik Sense site is determined by the security rules for each stream. By default, Qlik Sense includes two streams: **Everyone** and **Monitoring apps**.

An app can be published to only one stream. However, if you duplicate the app to create a copy, you can publish the copy to another stream. Apps can be moved between streams.

In the hub, streams with no apps—either empty streams or streams that do not show apps due to the existing security rules for a user—will not appear. After you publish an app, move it from another stream, or delete it, the list of streams will update dynamically and the stream will appear in the hub or be hidden depending on whether it contains at least one app. Changes outside of the hub, for example in QMC, will not trigger an update to the stream list in the hub.

> *All authenticated users have read and publish rights to the **Everyone** stream and all anonymous users read-only rights. Three of the predefined admin roles (RootAdmin, ContentAdmin, and SecurityAdmin), have read and publish rights to the Monitoring apps stream.*

> *It is not recommended to create rules that allow users to edit published apps in streams.*

The **Streams** overview lists all the available streams. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

> *You can adjust the column width by dragging the header border.*

Name	The name of the stream.
Owner	The stream owner. By default, the creator of the stream.
Tags	The tags that are connected to the stream.
Last started sync	The date and time of the last started sync to a cloud environment.
Last successfully finished sync	The date and time of the last successfully finished sync to a cloud environment.
Sync status	The current status of the sync to Qlik Sense.
ID	The ID of the stream.
Created	The date and time when the stream was created.
Last modified	The date and time when the stream was last modified.

Modified by	By whom the stream was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
☐⧩	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ☐⧩ is displayed.

To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.

You can combine filtering with searching.

Searching and filtering in the QMC (page 25) |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.

> ⓘ *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.* |
| ☷ | Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns. |
| 🔍 | Search – both basic and more advanced searches.

Searching and filtering in the QMC (page 25) |
↻	Refresh the page.
Edit	Edit the selected streams.
Delete	Delete the selected streams.
➕ **Create new**	Create a new stream.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

> 💡 *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

Stream: associated items

The tables in this document show the fields available for the **Contents** and **Security rules** property groups.

By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

> 💡 *You can adjust the column width by dragging the header border.*

Apps

Apps is available from **Associated items** when you edit streams. The overview contains a list of the apps that are associated with the selected streams.

Associated items properties

Property	Description
Name	The name of the app.
Owner	The owner of the app.
Published	The date when the app was published.
Description	The description of the app.
File size (MB)	The size of the app.
Last reload	Date and time when the app was last reloaded.
ID	The ID of the app.
Created	Date and time when the app was created.
Last modified	Date and time when the app was last modified.
Modified by	By whom the app was modified.
Custom properties	Custom properties, if any, are listed here.

If you make a selection in the overview and click **Edit** in the action bar, the app edit page is displayed.

User access

User access is available from **Associated items** when you edit a resource.

The preview shows a grid of the target resources and the source users who have access to the selected items.

Depending on rights, you can either edit or view a user, a resource, or an associated rule.

Security rules

Security rules is available from **Associated items** when you edit streams. The overview contains a list of the security rules that are associated with the selected streams.

The **Security rules** property group contains the user condition properties.

User condition properties

Property	Description
Name	The name of the security rule.
Description	The description of what the rule does.
Resource filter	The ID for the rule.
Actions	The permitted actions for the rule.
Disabled	Status values: **Yes** or **No**.
Context	The security rule context (**QMC**, **Hub**, or **Both**).
Type	The security rule type (**Default**, **Read only**, or **Custom**).
Conditions	The security rule conditions.
ID	The ID of the security rule.
Created	Date and time when the security rule was created.
Last modified	Date and time when the security rule was last modified.
Modified by	By whom the security rule was modified.

If you make a selection in the overview and click **Edit** in the action bar, the edit security rule page is displayed.

Tasks

Tasks are used to perform a wide variety of operations and can be chained together in just any pattern. The tasks are handled by the Qlik Sense Scheduler Service (QSS). There are four types of tasks:

- Reload
- User synchronization
- External program
- Distribution

The **Tasks** overview lists all the available tasks. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

> *You can adjust the column width by dragging the header border.*

Task properties

Field/Button	Description
Name	The name of the task. Click 🔗 to display the task chaining summary (only applicable for reload tasks with a task chain trigger applied).
Associated resource	The name of the app or the user directory connector that the task is used on.

Type	Type of task:
	• Reload (for app)
	• User synchronization (for user directory connector)
	• External program (triggers a third-party program)
	• Distribution task (triggers app distribution to Qlik Cloud)
Enabled	Status values: **Yes** or **No**.

Status	The status of the task:
	••• Never started: Task has never been started.
	↻ Triggered: A request has been sent to the scheduler to run the task.
	↻ Started: Task has started.
	⧗ Queued: Task is queued and will be started when preceding tasks have been processed. Queuing is controlled by the value of **Max concurrent reloads**, see *Editing schedulers (page 420)*.
	↻ Abort initiated: Manager scheduler has received the abort request but has not started processing it.
	↻ Aborting: Manager scheduler has started processing the abort request.
	⊠ Aborted: Task has been aborted.
	✔ Success: Task execution was successful.
	✕ Failed: Task has been sent to worker scheduler for execution but failed to complete. For example, a reload can fail because of missing Read rights to the data connections or an error in the reload script.
	••• Skipped: Start of the task has been requested, but the task execution has for some reason not started. For example, the task might not be enabled.
	↻ Retrying: Start of the task failed and a new attempt has started.
	✕ Error: Task has not been successfully sent to worker scheduler for execution and returned an error. For example, an error can occur when there is no available worker scheduler to execute the task, or the application is already being updated by another task.
	••• Reset: State that the manager scheduler sets to tasks during startup, if their current status is non-terminal, that is, if they have states like Triggered, Started, or Queued, where execution has not yet ended.
	Click ⓘ to open a summary of the latest reload or user synchronization tasks.
	Task status information (page 65)
Last execution	The date and time of the last execution of the task. If never executed, no information is displayed.

Next execution	The trigger type that starts the next execution of the task: • **On task event trigger**: The task execution is initiated by the completion of another task. • **On multiple triggers**: The task has more than one trigger applied. • The date and time for the next execution of the task is displayed if the task has a scheduled trigger applied. • If the field is empty, no trigger is created for the task.
Tags	The tags that are connected to the task.
ID	The ID of the task.
Created	The date and time when the task was created.
Last modified	The date and time when the task was last modified.
Modified by	By whom the task was modified.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌐▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌐▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. ⓘ *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↩ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
⟳	Refresh the page.
Edit	Edit the selected task.

Delete	Delete the selected tasks.
Start	Start the selected tasks.
Stop	Stop the selected tasks.
⊕ **Reload task**	Create a new reload task.
⊕ **External program task**	Create a new external program task.
⊕**Distribution task**	Create a new distribution task.
More actions > Enable	Enable the selected tasks.
More actions > Disable	Disable the selected tasks.
More actions > Duplicate	Duplicate the selected reload task. External program tasks, distribution tasks, or user sync tasks cannot be duplicated.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

> *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

Task: associated items

The following associated items are available for reload tasks, external program tasks, and distribution tasks.

User access

User access is available from **Associated items** when you edit a resource.

The preview shows a grid of the target resources and the source users who have access to the selected items.

Depending on rights, you can either edit or view a user, a resource, or an associated rule.

User synchronization task: associated items

The following associated items are available for user sync tasks.

User access

User access is available from **Associated items** when you edit a resource.

The preview shows a grid of the target resources and the source users who have access to the selected items.

Depending on rights, you can either edit or view a user, a resource, or an associated rule.

Triggers

Triggers is available from **Associated items** when you edit tasks. The overview contains a list of the triggers that are associated with the selected tasks.

Triggers

Property	Description
Name	The trigger name.
Valid from	Displays year, date, and time according to the **Start** values that was entered when creating the trigger.
Valid until	Displays year, date, and time according to the **End** values that was entered when creating the trigger.
Schedule	Displays the repeat pattern according to the **Schedule** value that was chosen when creating the trigger.
Enabled	Status values: **Yes** or **No**.
ID	The ID of the trigger.
Created	The date and time when the trigger was created.
Last modified	The date and time when the trigger was last modified.
Modified by	By whom the trigger was modified.

You can manage the triggers from the overview by making a selection and clicking a button in the action bar.

If you click **Edit**, the trigger edit page is displayed.

Task status information

On the tasks overview page, in the **Status** column, each task has an information icon (🛈) that you can click to get a summary of the latest task execution. The summary contains the following information.

Task execution summary

Field	Description
Task status	The status presented in the task status window and the status column may sometimes differ. Click ↻ in the task status window to refresh the status for that specific task, or click ↻ to the far right on the tasks overview page to update the status for all tasks. For a description of the different task statuses, see *Tasks (page 60)*.
Host name	The server node that initiated the latest run of the task.

Date and timestamp	The date and time when the task execution steps were performed. The steps are presented with the latest step first.
	In the Task tables execution columns the times take the timezone difference into account. So this can show different from the popup.
Task steps performed	Description of the task execution step performed.

Reload tasks also have a **Download script log** button for easy access to the script log. When the button is dimmed, the sync between the central node and the node with the script log has not been completed.

Users

Users are imported from user directories. Once imported, you can manage user access:

- Use the security rules editor to create rules, based on user IDs and names, to provide access to Qlik Sense.
- Assign QMC administrative roles. The roles need to be defined in the security rules page.

> *You can edit users that are associated with a stream or data connection. Select the stream or data connection from the **Streams** overview or **Data Connections** overview, and click **User access** under **Associated items**. Select the user and click **Edit user**.*

The **Users** overview lists all the available users. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

> *You can adjust the column width by dragging the header border.*

Users

Field/Button	Description
Name	The name of the user. Click 🛈 to view user information in a separate window.
User directory	The directory that the user is associated with.
User ID	The user ID associated with the user.
Admin roles	The QMC administration roles associated with the user.
Inactive	Status values: **Yes** or **No**.
Blocked	Status values: **Yes** or **No**.
Delete prohibited	Status values: **Yes** or **No**.
Removed externally	Status values: **Yes** or **No**. When **Yes**, it is normally because the user has been removed from the user directory.

Tags	The tags that are connected to the user.
ID	The ID of the user.
Created	The date and time when the user was created.
Last modified	The date and time when the user was last modified.
Modified by	By whom the user was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌄▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌄▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↩ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
⟳	Refresh the page.
Edit	Edit the selected users.
Delete	Delete the selected users.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

> *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

User: associated items

The following associated items are available for users.

> *You can adjust the column width by dragging the header border.*

User access

User access is available from **Associated items** when you edit a resource.

The preview shows a grid of the target resources and the source users who have access to the selected items.

Depending on rights, you can either edit or view a user, a resource, or an associated rule.

Owned items

Owned items is available from **Associated items** when you edit users. The overview contains a list of the resources owned by the selected users.

Resources

Property	Description
Name	The name of the resource.
Owner	The user ID of the user who owns the resource.
Type	The type of resource, for example, app or stream.

If you make a selection in the overview and click **Edit** in the action bar, the edit page for the owned item is displayed. You can only edit two or more owned items simultaneously if they have the same edit page.

System notifications

The **System notifications** overview lists all the available system notifications. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

> *System notifications and System notification policies features are available only on Qlik Sense Enterprise on Windows installations licensed with a signed key. For more information on licenses, see: Qlik Sense licenses documentation.*

System notifications

Field/Button	Description

Title	Title of the notification.
Message	Text of the notification.
Application link	Link to the Qlik Sense app.
User groups	List of user groups that receive the system notification.
Users	List of users that receive the system notification.
Last triggered	The date and time of when the notification distribution was last triggered. If never triggered, no information is displayed.
ID	The ID of the system notification.
Created	The date and time when the notification was created.
Last modified	The date and time when the notification was last modified.
Modified by	By whom the notification was modified.
Custom properties	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⊟▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⊟▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. ⓘ *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
⚲	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*

↻	Refresh the page.
Edit	Edit the selected notifications.
Delete	Delete the selected notifications.
Trigger	Trigger the notification distributions.
⊕ **Create new**	Create a new system notification.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

See also:

System notifications policies

The **System notifications policies** overview lists all the available system notifications policies. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

> *System notifications and System notification policies features are available only on Qlik Sense Enterprise on Windows installations licensed with a signed key. For more information on licenses, see: Qlik Sense licenses documentation.*

System notification policies

Field/Button	Description
Name	Name of the policy.
Description	Description of the system notification policy.
Resource filter	Type of resource that the rule applies to. An asterisk (*) indicates that the rule applies to all resources.
Actions	Select **Notify** to distribute the notification. If **Notify** is unselected, no information is displayed.
Disabled	Status values: **Yes** or **No**.
Type	**Default** or **Custom**.
Tags	Tags connected to the notification.

Custom properties	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⊟▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⊟▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.
Edit	Edit the selected notification policy.
Delete	Delete the selected notification policy.
⊕ **Create new**	Create a new system notification policy.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

See also:

Creating a system notification policy (page 369)

Editing a system notification policy (page 371)

Deleting a system notification policy (page 372)

Audit

On the QMC audit page, you can query for resources and users, and audit the security rules, load balancing rules, or license rules that have been defined in the Qlik Sense system.
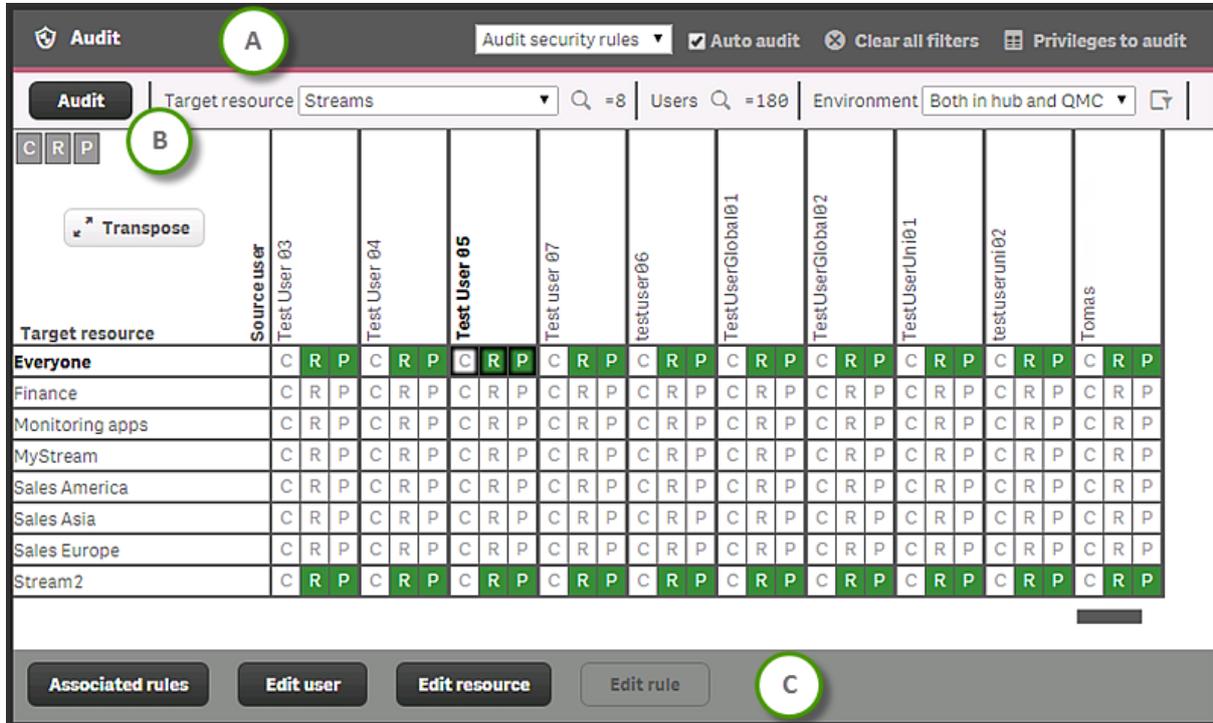
*Audit page with a query on **Streams**, with the Heading bar (A) and Audit bar (B) above, and the Action bar (C) below.*

Audit page heading bar options

- **Audit security rules** drop-down list: Select the rules to audit: security rules, load balancing rules, or license rules.

- **Auto audit**: When selected, all changes that are applied on the edit pages for resources, users, or rules will automatically refresh the audit table. Also, when editing, opening a security rule automatically generates a preview, if the resource type can be extracted.

- **Clear all filters**: Clear resource selection and user search query. You have to click **Audit** to update the grid.

- **Privileges to audit**: For security rules audits, you can select several different privileges to audit. What privileges that are available for a particular audit depends on the selected resource. Click ↩ to reset to the default privileges.

Audit privilege actions

Action	Description
C: **Create**	Create resource
R: **Read**	Read resource

Action	Description
U: **Update**	Update resource
D: **Delete**	Delete resource
E: **Export**	Export an app
A: **Export data**	Export app data
T: **Duplicate**	Duplicate an app
M: **Access offline**	Access apps offline
P: **Publish**	Publish a resource to a stream
O: **Change owner**	Change the owner of a resource
B: **Load balancing**	Control to which nodes that apps are load balanced
L: **Allow access**	Login access to a resource
V: **Approve**	Approve promotion of app sheets

Audit page Audit bar options

- **Audit**: Click **Audit** when you have selected target resource, users, and environment.
- **Target resource**: Select the resource to audit. Resources include the following:
  - Analytic connections
  - Apps
  - Content libraries
  - Data connections
  - App objects
  - Streams
  - Reload tasks
  - User synchronization tasks
  - Users
  - Security rules
  - Extensions
  - User directory connectors
  - Nodes
  - Login access (only for license rule audit)

  License rules audit is always on login access.

- **Users**: Click Q and use search to reduce the set of users. Auditing a large number of users and resources requires a lot of server processing and may take some time.
  See *Searching and filtering in the QMC (page 25)* for more information.

- **Environment**: Select the context for the audit.
  : Simulate user environment.

Simulate the user environment by setting the operating system, browser, and IP address. The available settings depend on the system setup and which browser headers that are available.

Example:

```
OS=Windows;
IP=10.88.3.35;
Browser= Firefox;
```

Audit page Action bar options

- **Associated rules**: Click to show the security rules that give access to the user/target combination.
- **Edit user**: Click to edit the selected user.
- **Edit resource**: Click to edit the selected resource.
- **Edit rule**: Click to edit the selected rule. (Only available when an associated rule has been selected.)
- **Show more**: Displayed when the audit generates more than 1000 results, and either users, resource, or both are unfiltered. When both **Target resource** and **Users** are filtered, all results are displayed.

> *If you do not have editing rights, the **Edit user** and **Edit resource** buttons are replaced by **View user** and **View resource** buttons.*

Auditing

> *You can only view users, resources, and rules that you have read access rights to.*

When you click **Audit**, the resulting audit table is displayed. You can pivot the table by clicking **Transpose**.

All green, yellow, red, or blue cells have rules attached to them:

- Green: The rule is valid and in use.
- Yellow: The rule is valid but disabled.
- Red: The rule is invalid.
- Blue: The rule is previewed.
- Dimmed values: The audit result is not fully retrieved, for performance reasons. Click **Show more** to get more results.

Select a cell and click **Associated rules** to view the details of the rules. You have also buttons for editing the user or resource.

Editing security rules, load balancing rules, or license rules

After performing an audit, you can click a cell and then choose to display the associated rules (which can be selected for editing), or edit the user, resource, or rule. When you edit, an editing pane is displayed to the left of the of the audit page. The editing pane displays all the properties for the item being edited.

Security rules

The Qlik Sense system includes an attribute-based security rules engine that uses rules as expressions to evaluate what type of access users should be granted for a resource.

The **Security rules** overview lists all the available security rules. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

> *You can adjust the column width by dragging the header border.*

<div align="center">Security rules overview</div>

Field/Button	Description
Name	The name of the rule. Names for generated rules have the following syntax: [resource type]_[access type]_[resource name]
Description	The description of the rule.
Resource filter	The type of resource that the rule applies to. An asterisk (*****) indicates that the rule applies to all resources. For generated rules, the Resource column includes the ID of the rule.
Disabled	Status values: **Yes** or **No**.
Context	Shows if the rule is for **QMC**, **Hub**, or **Both**.
Type	**Read only**, **Default**, or **Custom**.
Tags	The tags that are connected to the rule.
Conditions	Shows the conditions for the security rule.
ID	The security rule ID.
Created	The date and time when the security rule was created.
Last modified	The date and time when the security rule was last modified.
Modified by	By whom the security rule was modified.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌄▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌄▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*

Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.
Edit	Edit the selected security rule.
Delete	Delete the selected security rules.
⊕ **Create new**	Create a new security rule.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

If a resource is deleted, all load balancing rules and security rules associated with that resource are deleted automatically.

Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.

Actions (Basic view)

Select the actions that the user is allowed to perform on the resource. You must specify at least one action.

Access rule descriptions

Action	Description
Create	Create resource.
Read	Read resource.
Update	Update resource.
Delete	Delete resource.

Action	Description
Export	Export an app from Qlik Sense Enterprise into a qvf file.
Duplicate	Duplicate an app.
Publish	Publish a resource to a stream.
Approve	Approve an object belonging to an app.
Change owner	Change the owner of a resource.
Change role	Change user role.
Export data	Export data from an object. This includes the following actions: • "Export as image" for visualizations. • "Export as PDF" for visualizations. • "Export data" for visualizations. • "Export sheet" in the menu. • "Export story" in storytelling. *You cannot grant access to only a subset of these actions.* *You can enable export of data for anonymous users by creating a copy of the security rule ExportAppData and modifying the copy to only have* `resource.HasPrivilege("read")` *in* **Conditions**. *See Security rules included in Qlik Sense (page 535).*
Access offline	Access apps offline.

Conditions (Advanced view)

Define the resource and/or user conditions that the rule should apply to.

Syntax

```
resource.resourcetype = <resourcetypevalue> [OPERATOR resource.<property> =
<propertyvalue> [OPERATOR resource.<property> = <propertyvalue> ...]]
```

A simple condition would only consist of the first part: `resource.resourcetype = <resourcetypevalue>`. The succeeding operators, properties, and property values in the example above are optional.

If you select a resource and a resource condition from the drop-down list in the **Basic** view, the **Conditions** field in the **Advanced** view is automatically filled in with corresponding code for the selected resource type.

Conditions are defined using property-value pairs. You are not required to specify resource or user conditions. In fact, you can leave the **Conditions** field empty.

The order that you define conditions does not matter. This means that you can define the resources first and then the user and/or resource conditions or the other way round. However, it is recommended that you are consistent in the order in which you define resources and conditions as this simplifies troubleshooting.

When using multiple conditions, you can group two conditions by clicking **Group**. After the conditions have been grouped, you have the option **Ungroup**. Additional subgrouping options are **Split** and **Join**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that AND is superior to OR.

To enable synchronization between the **Basic** and **Advanced** sections (so called backtracking), extra parentheses are added to conditions created using the **Basic** section. Similarly, a user definition with an empty condition is automatically included in the **Conditions** text field if you add a resource using the **Basic** section. However, if you create your rule using the **Advanced** section only, and do not need backtracking, you do not need to follow these conventions.

Arguments

<div align="center">Argument descriptions</div>

Argument	Description
resource	Implies that the conditions will be applied to a resource.
resourcetype	Implies that the conditions will be applied to a resource of the type defined by the **resourcetypevalue**. You can also use predefined functions for conditions to return property values.
resourcetypevalue	Value used in the condition to find matches or non-matches, depending on what operator that is used (=, !=, or like). You must provide at least one resource type value.
property	The property name for the resource condition. See *Properties (page 78)* for available names.
propertyvalue	The value of the selected property name.
user	Implies that the conditions will be applied to a user.

Properties

The following property groups are available.

General

General properties descriptions and examples

Property	Description	Example
resource.@<customproperty>	Custom property associated with the resource. In the examples, @Department is the custom property name.	`resource.@Department = Finance. resource.@Department = user.userDirectory`
resource.name	Name of the resource.	`resource.name like "*US*"`. A string containing "US" will match the condition.
resource.id	ID of the resource.	`resource.id=5dd0dc16-96fd-4bd0-9a84-62721f0db427` The resource in this case is an app.

Resource user and owner of an object

Resource user and owner of an object properties

Property	Description	Example
user.email owner.email	Email of the user. Email of the owner.	`user.email="user@domain.com"` `owner.email="owner@domain.com"`
user.environment.browser	Session based attribute for browser. Use the "like" operator instead of the "=" operator, because the browser data is sent in a format that includes version and other details, for example: "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0". You can use the "=" operator instead, but then you need to specify the whole value.	`user.environment.browser like "*Firefox*"`
user.environment.context	Session based attribute for context. (The QMC has a separate setting for context.)	`user.environment.context="Management Access"`

Property	Description	Example
user.environment.device	Session based attribute for device.	`user.environment.device="iPhone"`
user.environment.ip	Session based attribute for IP address.	*Security rules example: Access to stream by IP address (page 607)*
user.environment.os	Session based attribute for operating system.	`user.environment.os like "Windows*"`
user.environment.secureRequest	Session based attribute for secureRequest. Value true - if SSL is used - otherwise false.	`user.environment.secureRequest="true"`
user.environment.[SAML attribute]	Session based attribute that is supplied at the time of authentication, such as user.environment.group.	`user.environment.xxx="<attribute name>"`
user.environment.[ticket attribute]	Session based attribute that is supplied at the time of authentication, such as user.environment.group.	`user.environment.xxx="<attribute name>"`
user.environment.[session attribute]	Session based attribute that is supplied at the time of authentication, such as user.environment.group.	`user.environment.xxx="<attribute name>"`
user.group owner.group	Group that the user belongs to. Group that the owner belongs to.	`user.group=resource.app.stream.@AdminGroup` `owner.group=@Developers`
user.userdirectory owner.userdirectory	User directory that the user belongs to. User directory that the owner belongs to.	`user.userdirectory="Employees"` `owner.userdirectory="Employees"`
user.userId owner.userId	ID of the user. ID of the owner.	`user.userId="<userID>"` `owner.userId="<ownerID>"`
user.roles owner.roles	Roles of the user. Roles of the owner.	`user.roles="AuditAdmin"` `owner.roles="SystemAdmin"`

> To use the user.environment conditions, you must enable **Extended security environment** in the virtual proxy.
>
> See: Virtual proxies (page 158)

Resource app

Resource app properties

Property	Description	Example
stream.name	Name of the stream that the app is published to.	`stream.name="Finance"`

Resource app.object

Resource app.object properties

Property	Description	Example
app.stream.name	Name of the stream that the app object is published to.	`app.stream.name="Test"`
app.name	Name of the app that the object is part of.	`app.name="Q3_Report"`
approved	Indicator of whether the object was part of the original app when the app was published. Values: true or false.	`resource.approved="true"`
description	Object description.	`resource.description="old"`
objectType	Possible values: • app_appscript • bookmark • dimension • embeddedsnapshot • genericvariableentry • hiddenbookmark • loadmodel • masterobject • measure • odagapplink • sheet • snapshot • story	`resource.objectType="sheet"`
published	Indicator of whether the object is published. Values: true or false.	`resource.published="false"`

Resource related to apps such as app.content and reloadtask

Resource related to apps such as app.content and reloadtask properties

Property	Description	Example
app.stream.name	Name of the stream that the app is published to.	`app.stream.name="Test"`
app.name	Name of the app.	`app.name="Q3_Report"`

Resource DataConnection

Resource DataConnection properties

Property	Description	Example
Type	Type of data connection. Possible values: • OLEDB • ODBC • Folder • Internet • Custom (for all custom connectors)	`resource.type!="folder"`

Resource SystemRule

Resource SystemRule properties

Property	Description	Example
Category	System rule category. Possible values: • Security • License • Sync	`resource.category="license"`
ResourceFilter	Resource filter of the rule.	`resource.resourcefilter matches "DataConnection_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}"`
RuleContext	Context for the rule. Possible values: • BothQlikSenseAndQMC • QlikSenseOnly • QMCOnly	`resource.rulecontext="BothQlikSenseAndQMC"`

Property	Description	Example
Type	Type of rule. Possible values: • Default • Read only • Custom	`resource.type!="custom"`

Resource ContentLibrary

Resource ContentLibrary properties

Property	Description	Example
Type	Possible values: • media	`resource.type="media"`

Resource ServerNodeConfiguration

Resource ServerNodeConfiguration properties

Property	Description	Example
IsCentral	Central node indicator, values: true or false.	`resource.iscentral="true"`
nodePurpose	Node purpose: development or production.	`resource.nodepurpose="production"`

Resource UserDirectory

Resource UserDirectory properties

Property	Description	Example
userDirectoryName	Name of the user directory.	`resource.userDirectoryname="Employees"`

Resource UserSyncTask

Resource UserSyncTask properties

Property	Description	Example
userDirectory.name	Name of the user directory connector.	`resource.userDirectory.name="Employees"`
userDirectory.userDirectoryName	Name of the user directory.	`userDirectory.userdirectoryname="Employees"`

Resource Widget

Resource Widget properties

Property	Description	Example
library.name	Name of the library that the widget belongs to.	`resource.library.name="Dev"`

> *Environment data received from external calls, for example, type of OS or browser, is not secured by the Qlik Sense system.*

Examples and results

Examples and results of **Resource filters**

Example	Result
Resource filter: App* **Conditions:**`resource.resourcetype="App" and (resource.name like "*")`	The rule will apply to all apps. > *The same rule can be defined by simply setting the Resource field to App* and leaving the Conditions field empty.*
Resource filter: App* or App.Object* or Stream* **Conditions:**`resource.resourcetype="App" or resource.resourcetype="Stream" or (resource.resourcetype="App.Object" and resource.objectType="sheet") and resource.name like "My*"`	The rule will apply to all apps, streams and sheets that have names beginning with "My".
`resource.resourcetype="ServerNodeConfiguration" and (resource.@Department="Finance")`	The rule will apply to all nodes with the custom property Department set to Finance.
`resource.resourcetype="ServerNodeConfiguration" and !(resource.@Department="Finance")`	The rule will apply to all nodes except the nodes with custom property Department set to Finance.
With **Resource filter** `= resource.resourcetype="App.Object" and (((resource.objectType="sheet" or resource.objectType="story")) and ((user.name="Myname")))`	The rule will apply to all apps, sheets, stories and the user with the name MyName.
With **Resource filter**=`Stream_*` `user.@Department="Finance" and !user.IsAnonymous ()`	The rule will apply to all streams and users with the custom property Department set to Finance given that the user is not logged in as anonymous.
With **Resource filter**=* and Conditions field empty	This rule will apply to all resources and all users.

Example	Result
user.name="MyUserName"	The rule will apply to the user with the user name MyUserName. 💡 *Try as much as possible not to create rules that apply to individuals. Use group memberships, user roles or custom properties to apply rules to groups of users.*
user.group="DL-MyDepartment"	The rule will apply to all members of the distribution group MyDepartment.
user.@Department="Sales"	The rule will apply to all users with the custom property @Department set to Sales.
user.roles="Developer"	The access rights defined in the Resource, Conditions and Actions field will be applied to the user role Developer. This role will now be available from the Roles drop-down list in the User edit page.
resource.resourcetype="App" and resource.name="My*" and user.role="QlikSenseAdmin"	The user.role can also be used together with an operator to specify that the rule applies if the user has the specified user role.
user.environment.os="Windows"	The rule will be applied to all external environments with operating system = Windows.

Resource filter (Advanced view)

A mandatory definition of the types of resources that the security rule applies to.

Syntax

```
resourcetype1[*][_*][, resourcetype2[*][_*], ...]
```

If you select a resource from the **Create rule from template list** in the **Identification** section, the **Resource filter** field in the **Basic** section is automatically filled in with the selected resource. The optional underscore and asterisk ('_*') are added by default. Selections made in the rule wizard drop-down lists in the **Basic** section are automatically added to the **Conditions** box in the **Advanced** section.

Arguments

Arguments

Argument	Description
resourcetype1	Required. You must enter at least one resource type name.
*	Optional wildcard. If included the rule will apply to all resource types beginning with the specified text. For example, **App*** will apply the rule to all resource types beginning with **"App"**, that is to say, all resources of type **App** and **App.Object**. If omitted the security rule will apply to resource types with the exact name specified in the Resource field. You must supply the GUID or template for GUIDs for the rule to work. Cannot be used in conjunction with '**_***' option.
_*	Optional wildcard. If included the rule will apply to all resources of the type specified. For example, **App_*** will apply the rule to all apps. Similarly, **App.Object_*** will apply the rule to all app objects. If omitted the security rule will apply to resource types with the exact name specified in the Resource field. You must supply the GUID or template for GUIDs for the rule to work. Cannot be used in conjunction with the '*****' option.

Properties

Security rule properties

Property	Security rule will be applied to
App	Apps
App.Object	Objects The Objects' objectTypes, for example: sheet, story, bookmark, measure or dimension.
ContentLibrary	Content libraries
DataConnection	Data connections
Extension	Extensions
ReloadTask	Reload tasks
ServerNodeConfiguration	The configuration of Qlik Sense nodes
Stream	Streams
SystemRule	Security rules
User	Users
UserDirectory	User directory connectors
UserSyncTask	User synchronization tasks

Examples and results

Examples and results

Example	Result
`App*`	The rule will apply to apps and app objects.
`App_*`	The rule will apply to apps only.

`App*, Streams*, App.Object*`
`resource.resourcetype="App.Object" and`
`(((resource.objectType="sheet")))`
	The rule will apply to apps, streams and sheets.
	
	You can leave out App.Object … in this example as App* will apply the rule to both apps and sheets.*

`Stream_88ee46c6-5e9a-41a7-a66a-` `f5d8995454ec`	The rule will apply to the stream with the specified GUID.
`Stream_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}`	The rule will apply to all existing streams.
Select **App** from the **Resource** drop-down list.	The following texts appear in the Advanced view: **Resource*** `App*` **Conditions*** `resource.resourcetype="App" and ( )` *If you don't enter a resource or a user condition inside the brackets, the security rule will by default apply to all apps and all users.*

Custom properties

You create a custom property to be able to use your own values in the security rules. You define one or more values for the custom property, and use these in the security rule for a resource.

The QMC checks for custom property changes every 20 seconds.
The **Custom properties** overview lists all the available custom properties. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

You can adjust the column width by dragging the header border.

Custom properties

Property name	Description

Name	Name of the custom property, defined from the QMC.
Description	Description of the rule. Optional.
Resource types	Resource types that the custom property is available for.
ID	Customer property ID.
Created	Date and time when the custom property was created.
Last modified	Date and time when the custom property was last modified.
Modified by	By whom the custom property was modified.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌧	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌧ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
Edit	Edit the selected custom property.
Delete	Delete the selected custom properties.
⊕ **Create new**	Create a new custom property.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.

License management

There are two license models: the serial and control number and the signed license key. These models define the terms of your license and the access types that you can allocate to users. With a signed license key, you need internet access (direct or through a proxy) to access the cloud-based license backend, for user assignments, analytic time consumption, and product activations.

There are two major license types: one based on access types, and one based on tokens.

- Access types licenses are the Professional and Analyzer Users licenses (user-based) and Analyzer Capacity licenses (capacity-based). With a Professional and Analyzer Users license you can allocate professional access and analyzer access. With an Analyzer Capacity license you can allocate analyzer capacity access, where consumption is time based (analyzer time).
- With a Qlik Sense Token license you use tokens to allocate access passes to users. You can allocate user access and login access.

An access type allows users to access the hub and apps within a Qlik Sense Enterprise on Windows site.

> *If you want to set up Qlik Sense Enterprise SaaS, please contact your Qlik representative or Qlik Support to obtain a valid license for the setup.*

- The **License usage summary** page displays the distribution of the different access types.
- The **Professional access allocations** page displays an overview and you can allocate, deallocate, or reinstate professional access for users.
- The **Professional access rules** page displays an overview and you can edit, delete, or create new professional access rules. The professional access rules are used to automatically allocate professional access.
- The **Analyzer access allocations** page displays an overview and you can allocate, deallocate, or reinstate analyzer access for users.
- The **Analyzer access rules** page displays an overview and you can edit, delete, or create new analyzer access rules. The analyzer access rules are used to automatically allocate analyzer access.
- The **Analyzer capacity rules** page displays an overview and you can edit, delete, or create new analyzer capacity rules. The analyzer capacity rules are used to automatically allocate analyzer capacity access.
- The **User access allocations** page displays an overview and you can allocate, deallocate, or reinstate user access for users.
- The **User access rules** page displays an overview and you can edit, delete, or create new user access rules. The user access rules are used to automatically allocate user access.
- The **Login access rules** page displays an overview and you can edit, delete, or create new login access rules.
- The **Site license** page is where you activate, or apply changes to, the LEF.

Professional access allocations

Professional access is allocated to an identified user to allow the user to access streams and apps within a Qlik Sense site. The professional access is intended for users who need access to all features in a Qlik Sense installation. A user with professional access can create, edit, and publish sheets or apps, and make full use of the available features, including administration of a Qlik Sense site.

For Qlik Sense installations licensed with a serial and control number, if you remove professional access allocation from a user, the access type is put in quarantine, if it has been used within the last seven days. If it has not been used within the last seven days, the professional access is released immediately. You can reinstate quarantined professional access, to the same user, within seven days.

The maximum number of parallel user connections for a single user of this type of access pass is five (5).If you use a license with a signed license key, accessing the QMC also counts and adds to the maximum number of parallel sessions, which is five. To avoid unnecessary session consumption, the root admin should not be allocated any type of access.

When a user with the maximum number of parallel user connections ends a connection (for example, by logging out) five minutes must pass before the user can use the access pass to add another connection (for example, by logging in).

Read more under **Status**.

The **Professional access allocations** overview lists all users with professional access. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

> 💡 *You can adjust the column width by dragging the header border.*

Profession access allocations properties

Field	Details
Name	Name of the user with an allocated (or quarantined) professional access.
	Deleted user is displayed if the user is deleted but is still in quarantine. When the quarantine period is over, the deleted user is removed from the overview.
User directory	User directory that the user is imported from.

Field	Details
Status	Status of the professional access: **Allocated** means that professional access is allocated to the identified user and the user can access the hub and apps. **Quarantined** (only in licenses with serial number) means the following: • The user cannot access streams and apps on the hub. • Professional access was previously allocated to the user and thereafter deallocated. • During the quarantine period, professional access can be reinstated to the original user. **Excluded** is displayed when you use a license with a signed license key and the number of allocated assignments is larger than defined by the license. In this case, the most recently assigned users are excluded until the number of allocations matches the number defined by the license. If more access allocations are made available, or if the admin removes access for others, access is re-allocated to excluded users. Exclusion can occur, for example, when the number of assignments in the license is reduced.
Last used	Date and time when the user accessed the hub. If you use a license with a signed license key, accessing the QMC also counts and adds to the maximum number of parallel sessions, which is five. To avoid unnecessary session consumption, the root admin should not be allocated any type of access.
ID	User access ID.
Created	Date and time when the professional access was created.
Last modified	Date and time when the professional access was last modified.
Modified by	By whom the professional access was modified.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⊾▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⊾▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*

Field	Details
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↩ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.
Deallocate	Deallocate professional access from the selected users.
Reinstate	Reinstate professional access to the selected users, when quarantined.
⊕**Allocate**	Allocate professional access to an identified user.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.

Professional access rules

A professional access rule defines which users who will automatically be assigned professional access when logging in.

The **Professional access rules** overview lists all professional access rules. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

You can adjust the column width by dragging the header border.

Professional access rules fields

Field	Description
Name	Name of the professional access rule.

Field	Description
Description	Description of the professional access rule.
Resource filter	Type of resource that the professional access rule applies to.
Disabled	Status values: **Yes** or **No**.
Type	Professional access rule type.
Conditions	A definition of the resource and/or users that needs to be met for the rule to apply.
Context	Specifies in which context the professional access rule applies: **Hub**, **QMC**, or **Both**.
ID	Professional access rule ID.
Created	Date and time when the professional access rule was created.
Last modified	Date and time when the professional access rule was last modified.
Modified by	By whom the professional access rule was modified.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⧨	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⧨ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. > ⓘ *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
⟳	Refresh the page.
Edit	Edit the selected professional access rule.

Field	Description
Delete	Delete the selected professional access rules.
⊕**Create new**	Create a new professional access rule.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

> *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

Analyzer access allocations

Analyzer access is allocated to an identified user to allow the user to access streams and apps in the hub. The analyzer access is intended for users who consume sheets and apps created by others. A user with analyzer access cannot create, edit, or publish sheets or apps, but can create and publish stories, bookmarks and snapshots based on data in apps. The user can also create bookmarks, print objects, stories, and sheets, and export data from an object to Excel.

For Qlik Sense installations licensed with a serial and control number, if you remove analyzer access allocation from a user, the access type is put in quarantine, if it has been used within the last seven days. If it has not been used within the last seven days, the analyzer access is released immediately. You can reinstate quarantined analyzer access, to the same user, within seven days.

The maximum number of parallel user connections for a single user of this type of access pass is five (5).When a user with the maximum number of parallel user connections ends a connection (for example, by logging out) five minutes must pass before the user can use the access pass to add another connection (for example, by logging in).

Read more about excluded under **Status**.

The **Analyzer access allocations** overview lists all users with analyzer access. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

> *You can adjust the column width by dragging the header border.*

Analyzer access allocation properties

Property	Description
Name	Name of the user with an allocated (or quarantined) analyzer access.
	Deleted user is displayed if the user is deleted but is still in quarantine. When the quarantine period is over, the deleted user is removed from the overview.

Property	Description
User directory	User directory that the user is imported from.
Status	Status of the analyzer access: **Allocated** means that analyzer access is allocated to the identified user and the user can access the hub and apps. **Quarantined** means the following: • The user cannot access streams and apps on the hub. • Analyzer access was previously allocated to the user and thereafter deallocated. • During the quarantine period, analyzer access can be reinstated to the original user. **Excluded** is displayed when you use a license with a signed license key and the number of allocated assignments is larger than defined by the license. In this case, the most recently assigned users are excluded until the number of allocations matches the number defined by the license. If more access allocations are made available, or if the admin removes access for others, access is re-allocated to excluded users. Exclusion can occur, for example, when the number of assignments in the license is reduced.
Last used	Date and time when the user accessed the hub.
ID	User access ID.
Created	Date and time when the analyzer access was created.
Last modified	Date and time when the analyzer access was last modified.
Modified by	By whom the analyzer access was modified.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⯆	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⯆ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*

Property	Description
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.
▦	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.
Deallocate	Deallocate analyzer access from the selected users.
Reinstate	Reinstate analyzer access to the selected users, when quarantined.
⊕ **Allocate**	Allocate analyzer access to an identified user.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.

Analyzer access rules

An analyzer access rule defines which users who will automatically be assigned analyzer access when logging in.

The **Analyzer access rules** overview lists all analyzer access rules. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

You can adjust the column width by dragging the header border.

Analyzer access rule properties

Property	Description
Name	Name of the analyzer access rule.

Property	Description
Description	Description of the analyzer access rule.
Resource filter	Type of resource that the analyzer access rule applies to.
Disabled	Status values: **Yes** or **No**.
Type	Analyzer access rule type.
Conditions	A definition of the resource and/or users that needs to be met for the rule to apply.
Context	Specifies in which context the user access rule applies: **Hub**, **QMC**, or **Both**.
ID	Analyzer access rule ID.
Created	Date and time when the analyzer access rule was created.
Last modified	Date and time when the analyzer access rule was last modified.
Modified by	By whom the analyzer access rule was modified.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
🔽	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, 🔽 is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
🔲	Column selector: Select which columns to display in the overview. Click ↩ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.
Edit	Edit the selected analyzer access rule.

Property	Description
Delete	Delete the selected analyzer access rules.
➕**Create new**	Create a new analyzer access rule.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

> *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

Analyzer capacity license

Analyzer capacity is a consumption-based license type, which is like analyzer access regarding available features. Users can access streams and apps in the hub and consume sheets and apps created by others. Analyzer capacity access allows users to create stories, bookmarks, and snapshots based on data in apps. Creating, editing, or publishing sheets or apps is not possible.

With an analyzer capacity license, you subscribe to analyzer time, a defined number of minutes per month (calendar date). These minutes are shared between users and can be consumed by anyone who is part of the user group, including anonymous users. Consumption is measured in units of six minutes. For each new six-minute period, a unit is consumed.

Analyzer capacity consumption

Analyzer capacity consumption is initiated when there is activity between the user and the Qlik Sense app. Idle time, when an app is visible but not used, will not consume additional time.

The following interactions are examples of activity between the user and Qlik Sense:

- When you open an app.
- When you make a selection in the app. For example, using Insight Advisor Chat or data profiling in the Data Catalog.
- When you navigate to a new sheet.
- When you reload the app or a scheduled reload takes place.

One unit of consumption is six minutes. When six minutes have passed, if there is any user activity with the app, a new six minute unit is consumed. If there is no activity within six minutes then you will be considered idle and no units will be consumed.

Unit consumption continues for as long as you are active. If you are active for 26 minutes, five units (30 minutes) are consumed. Analyzer capacity may be consumed when background services run. However, when a scheduled reload occurs in an app to which a user is connected, an additional unit is consumed - if there is not already an ongoing unit consumption.

The following diagrams show how consumption of Analyzer capacity is measured and when units are consumed.

Diagram of capacity consumption using one unit.
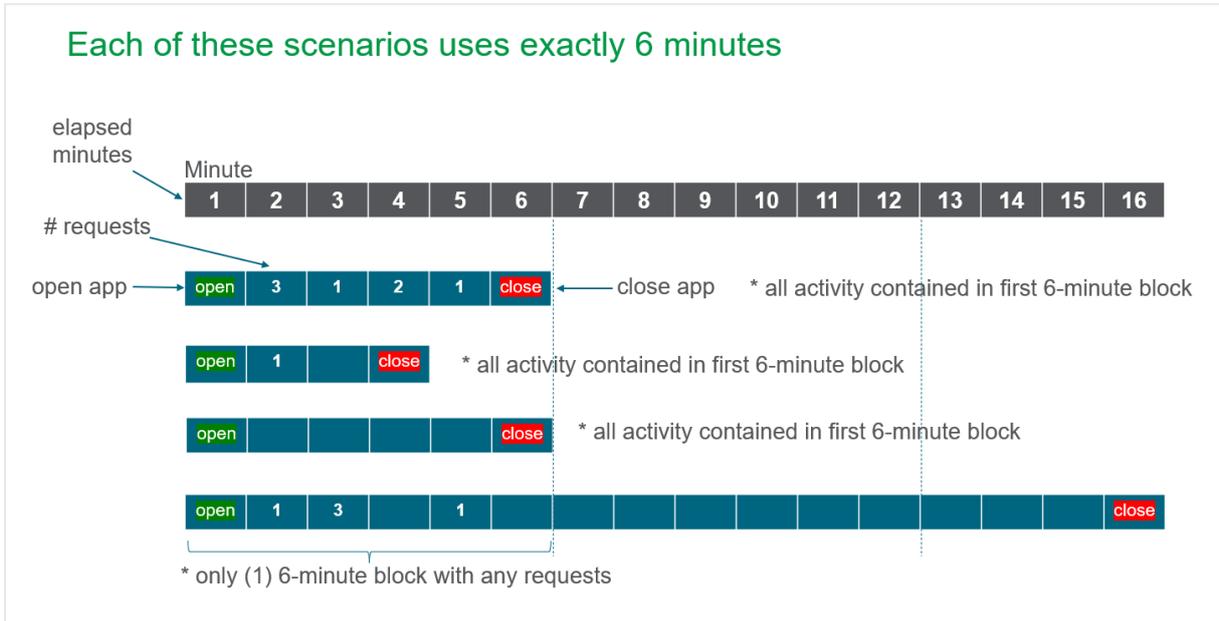
Diagram of capacity consumption using multiple units.
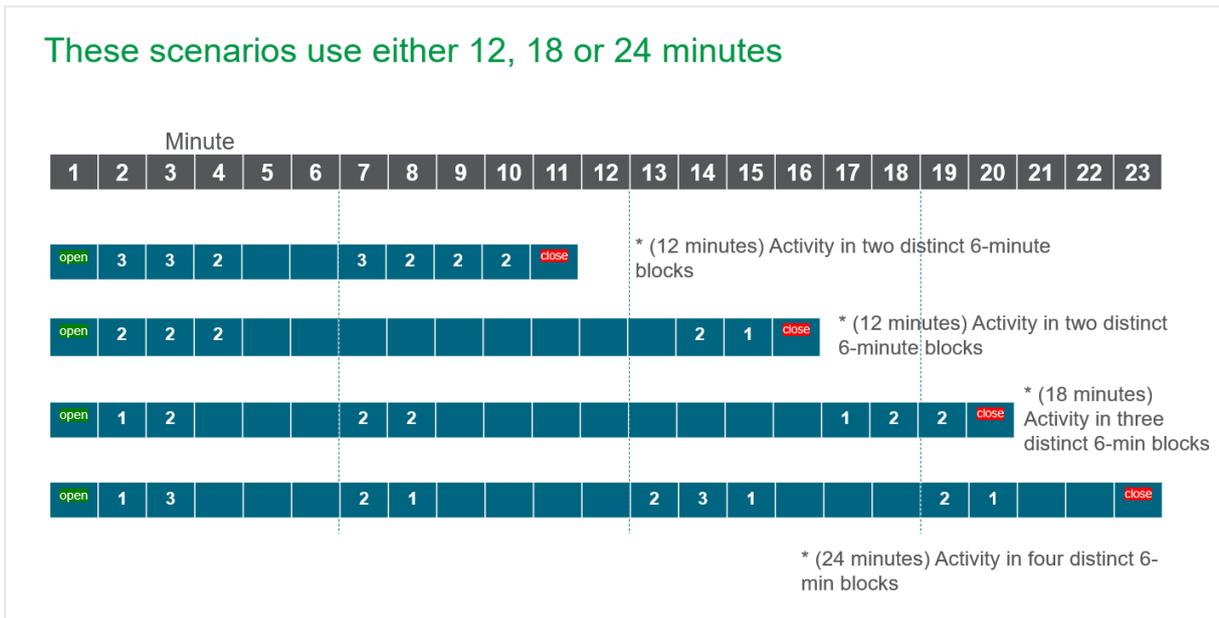
There is a key difference in how Qlik Sense Enterprise Client-Managed and Qlik Sense Enterprise SaaS calculate Analyzer capacity usage. Qlik Sense Enterprise Client-Managed uses the number of devices as part of the assessment for Analyzer capacity usage. Qlik Sense Enterprise SaaS uses the number of open apps as part of the assessment for Analyzer capacity usage. The following tables show some examples of how this is calculated:

Units consumed by device

Examples - apps and devices	Qlik Sense Enterprise Client-Managed
1 Qlik Sense application - 1 device	1 unit
2 Qlik Sense applications - 1 device	1 unit
3 Qlik Sense applications - 2 devices	2 units
5 Qlik Sense applications - 2 devices	2 units

> *A device is defined as a separate device such as a laptop or mobile device. This could also include a second browser.*

Units consumed by time

Example - apps and time	Qlik Sense Enterprise Client-Managed
1 Qlik Sense application - 6 minutes of activity	1 unit
1 Qlik Sense applications - 14 minutes of activity	3 units
2 Qlik Sense applications - 6 minutes of activity	1 unit
2 Qlik Sense applications - 14 minutes of activity	3 units

Analyzer capacity overage

When all of your Analyzer capacity has been consumed for the month, users who use Analyzer capacity to access Qlik Sense are denied access. Analyzer capacity consumption resets at the start of every month.

Analyzer capacity overage allows customers to consume more than their monthly entitlement to avoid having users locked out due to unexpectedly high usage. Analyzer capacity overage can be enabled by adding it to your subscription. The default is to match overage packs with the number of Analyzer capacity packs but this can be adjusted as needed.

Monitoring Analyzer capacity consumption

With a Qlik Sense Enterprise Client-Managed system, you can monitor Analyzer capacity consumption using the following:

- The **License Management Usage Summary** tab in the Qlik Management Console
- The **Usage Snapshot** tab in the **License Monitor** app
- The **Unified License History** tab in the **License Monitor** app. Use this tab to see individual user consumption.

Summary Analyzer capacity access

- The same features available as with Analyzer access.
- Assigned to a group of users, including anonymous users.
- Monthly subscription to a defined amount of minutes.
- Consumption in 6 minute blocks.
- Overage can be added to subscription.

Access details for users with analyzer or professional access

Analyzer access is allocated to users who consume sheets and apps created by others. Professional access is allocated to users who need access to all features in a Qlik Sense installation. The following tables detail what a user with analyzer or professional access can do in different areas in the hub based on access type.

App

Action	Hub - Work		Hub - Published	Everyone stream (or other stream with the same availability)	
	Analyzer	Professional	Professional	Analyzer	Professional
Create app	✗	✓	✗	✗	✗
Duplicate app	✗	✓	✓	✗	✓
List app	✓	✓	✓	✓	✓
Open apps and analyze	✓	✓	✓	✓	✓
Open app without data	✓	✓	✓	✓	✓
Delete app	✗	✓	✗	✗	✗
Manage app properties	✗	✓	✓	✗	✓
Export (download) app	✗	✓	✗	✗	✗
Import (upload) app	✗	✓	✗	✗	✗
Publish app	✗	✓	✗	✗	✗
Republish app (replace existing app)	✗	✓	✗	✗	✗
Add app to Favorites	✓	✓	✓	✓	✓
Remove app from Favorites	✓	✓	✓	✓	✓
Open app details	✓	✓	✓	✓	✓
Move app	✗	✗	✓	✗	✓

> *You can only open your own unpublished apps without data. You can only open apps in qvf format without data, not documents in qvw format.*

Sheet and visualizations

Action	Hub - Work		Hub - Published	Everyone stream (or other stream with the same availability)	
	Analyzer	Professional	Professional	Analyzer	Professional
Open public sheets	✗	✓	✓	✓	✓
Create sheet	✗	✓	✓	✗	✓
Copy sheet	✗	✓	✓	✗	✓
Delete sheet	✗	✓	✗	✗	✗
Duplicate sheet	✗	✓	✓	✗	✓
Edit sheet	✗	✓	✗	✗	✗
List sheets	✗	✓	✓	✓	✓
Unapprove sheet	✗	✗	✓	✗	✓
Use smart search	✗	✓	✓	✓	✓
Make selections	✗	✓	✓	✓	✓
Step backwards / forwards in selections	✗	✓	✓	✓	✓
Clear all selections from a specified field.	✗	✓	✓	✓	✓
Clear all selections in all states in the app. Optionally, overwrite locked selections.	✗	✓	✓	✓	✓
Clear selections from all fields except the	✗	✓	✓	✓	✓

one specified.
Optionally,
overwrite locked
selections.

Lock and unlock all selections in the app	✖	✔	✔	✔	✔
Lock a specified field	✖	✔	✔	✔	✔
Unlock a specified field	✖	✔	✔	✔	✔
Select possible / alternative / excluded values	✖	✔	✔	✔	✔

Visualization – More menu

	Hub - Work		Hub - Published	Everyone stream (or other stream with the same availability)	
Action	**Analyzer**	**Professional**	**Professional**	**Analyzer**	**Professional**
View full screen	✖	✔	✔	✔	✔
Open exploration menu and make edits	✖	✔	✔	✔	✔
Monitor in hub	✖	✔	✖	✖	✖
Add to master items	✖	✔	✖	✖	✔
Share (embed)	✖	✔	✔	✔	✔
Take snapshot	✖	✔	✔	✔	✔
Open snapshot library	✖	✔	✔	✔	✔
Download as Image / PDF / Data	✖	✔	✔	✔	✔

Visualization – Edit mode

	Hub - Work	Hub - Published	Everyone stream (or other stream with the same availability)

Action	Analyzer	Professional	Professional	Analyzer	Professional
Add to master items	✗	✓	✗	✗	✗
Cut	✗	✓	✗	✗	✗
Copy	✗	✓	✗	✗	✗
Delete	✗	✓	✗	✗	✗

Insight advisor

Action	Hub - Work		Hub - Published	Everyone stream (or other stream with the same availability)	
	Analyzer	Professional	Professional	Analyzer	Professional
Use Insight Advisor	✗	✓	✓	✓	✓

Storytelling

Action	Hub - Work		Hub - Published	Everyone stream (or other stream with the same availability)	
	Analyzer	Professional	Professional	Analyzer	Professional
Create story	✗	✓	✓	✓	✓
Publish story	✗	✓	✓	✓	✓
Duplicate story	✗	✓	✓	✓	✓
Delete story	✗	✓	✓	✓	✓
Export story to PowerPoint / PDF	✗	✓	✗	✓	✗
Download story as PowerPoint / PDF	✗	✗	✓	✗	✓

Bookmarks

Action	Hub - Work		Hub - Published	Everyone stream (or other stream with the same availability)	
	Analyzer	Professional	Professional	Analyzer	Professional

Create bookmarks	✗	✓	✓	✓	✓
Delete bookmarks	✗	✓	✓	✓	✓
Open public bookmarks	✗	✓	✓	✓	✓
See public bookmark details	✗	✓	✓	✓	✓
Copy public bookmarks	✗	✓	✓	✓	✗
Apply bookmark: Apply a selection that is defined in a bookmark.	✗	✓	✓	✓	✓

> *You can open the QMC with analyzer access, but you have no access to any sections.*

Analyzer capacity rules

An analyzer capacity rule defines which users are automatically assigned analyzer capacity access when logging in.

The **Analyzer capacity rules** overview lists all analyzer capacity rules. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

> *You can adjust the column width by dragging the header border.*

Analyzer capacity rule fields

Property	Description
Name	Name of the analyzer capacity rule.
Description	Description of the analyzer capacity rule.
Resource filter	Type of resource that the analyzer capacity rule applies to. *Defining resource filters (page 567)*
Disabled	Status values: **Yes** or **No**.
Type	Analyzer capacity rule type.
Conditions	A definition of the resource and/or users that needs to be met for the rule to apply.
Context	Specifies in which context the user access rule applies: **Hub**, **QMC**, or **Both**.

Property	Description
ID	Analyzer capacity rule ID.
Created	Date and time when the analyzer capacity rule was created.
Last modified	Date and time when the analyzer capacity rule was last modified.
Modified by	By whom the analyzer capacity rule was modified.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌕	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌕ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.
Edit	Edit the selected analyzer capacity rule.
Delete	Delete the selected analyzer capacity rules.
⊕ **Create new**	Create a new analyzer capacity rule.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

User access allocations

You allocate user access to an identified user to allow the user to access the streams and the apps within a Qlik Sense site. There is a direct relationship between the access type (user access) and the user. If you deallocate user access from a user, the access type is put in quarantine if it has been used within the last seven days. If it has not been used within the last seven days, the user access is removed and the tokens are released immediately. You can reinstate quarantined user access, to the same user, within seven days. Then the user is given access again without using more tokens.

The **User access allocations** overview lists all users with user access. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

> *You can adjust the column width by dragging the header border.*

<div align="center">User access allocation properties</div>

Name	The name of the user with an allocated (or quarantined) user access.
	Deleted user is displayed if the user is deleted but is still in quarantine. When the quarantine period is over, the deleted user is removed from the overview.
User directory	The user directory that the user is imported from.
Status	The status of the user access:
	Allocated means that user access is allocated to the identified user and the user can access the hub and apps.
	Quarantined means the following:
	• The user cannot access streams and apps on the hub.
	• User access was previously allocated to the user and thereafter deallocated.
	• The token is not available for new allocation until the end of the quarantine period (seven days).
	• During the quarantine period, user access can be reinstated to the original user.
Last used	The date and time when the user accessed the hub.
ID	The user access ID.
Created	The date and time when the user access was created.
Last modified	The date and time when the user access was last modified.
Modified by	By whom the user access was modified.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.

⌐▽	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌐▽ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
⊞	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
⟳	Refresh the page.
Deallocate	Deallocate user access from the selected users.
Reinstate	Reinstate user access to the selected users, when quarantined.
⊕**Allocate**	Allocate user access to an identified user.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.

User access rules

A user access rule defines which users that will automatically be assigned user access when logging in.

The **User access rules** overview lists all user access rules. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

You can adjust the column width by dragging the header border.

User access rule properties

Property	Description
Name	The name of the user access rule.
Description	The description of the user access rule.
Resource filter	The type of resource that the user access rule applies to.
Disabled	Status values: **Yes** or **No**.
Type	The user access rule type.
Conditions	A definition of the resource and/or users that needs to be met for the rule to apply.
Context	Specifies in which context the user access rule applies: **Hub**, **QMC**, or **Both**.
ID	The user access rule ID.
Created	The date and time when the user access rule was created.
Last modified	The date and time when the user access rule was last modified.
Modified by	By whom the user access rule was modified.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌸	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌸ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↩ to reset to the default columns.

$\mathbb{Q}$	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
$\circlearrowright$	Refresh the page.
Edit	Edit the selected user access rule.
Delete	Delete the selected user access rules.
$\oplus$**Create new**	Create a new user access rule.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

> *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

User access rules: associated item

User access is available from **Associated items** when you edit a resource.

The preview shows a grid of the target resources and the source users who have access to the selected items.

Depending on rights, you can either edit or view a user, a resource, or an associated rule.

Login access rules

One token equals a predefined amount of login access passes. The login access allows a user to access streams and apps for a predefined amount of time. This means that a single user may use several login access passes within a day. You create security rules specifying which users the login access is available for.

When you delete a login access (group), tokens are released immediately if the login access contains enough unused login access passes. The number of tokens that are released is dependent on the number of used login access passes. Used login access passes are not released until 28 days after last use. For example: If you allocated tokens giving 1000 login access passes to a group, they cannot use more than 1000 login access passes over 28 days. Also, if 100 login access passes are consumed on day 1, the 100 are available again on day 29. If no access passes are in use then all tokens assigned to the login access instance will be released when it is deleted.

> *App reloads will extend the session and consume access passes also when the app is not actively used. If a browser page is open with an app, app reloads will result in additional access pass consumption.*

The **Login access rules** overview lists all login access rules. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector ($\boxplus$) to add fields.

Login access group properties

Property	Descriptions
Name	The name of the login access group.
Allocated tokens	The number of tokens that are allocated to the login access group, providing a number of access passes.
Used login access passes	The number of access passes that have been used, when users from the group have logged in to the hub.
Remaining login access passes	The number of access passes that are available for users in the group, for logins to the hub.
ID	The ID of the login access group.
Created	The date and time when the login access group was created.
Last modified	The date and time when the login access group was last modified.
Modified by	By whom the login access group was modified.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⬚▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⬚▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. ⓘ *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↩ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.

Property	Descriptions
Edit	Edit the selected login access group.
Delete	Delete the selected login access groups.
⊕**Create new**	Create a new login access group.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

Login access rules: associated items

The **Login access rules** overview lists all associated items for the login access rules. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

> *You can adjust the column width by dragging the header border.*

User access

User access is available from **Associated items** when you edit a resource.

The preview shows a grid of the target resources and the source users who have access to the selected items.

Depending on rights, you can either edit or view a user, a resource, or an associated rule.

License rules

The property group **License rules** contains the properties for the login access rule.

License rule properties

Property name	Description
Name	The name of the license rule.
Description	A description of the rule purpose.
Resource filter	The resource filter for the rule.
Actions	The allowed actions for the license rule.
Disabled	Status values: **Yes** or **No**.
Context	The context for the license rule (**QMC**, **Hub**, or **Both**).
Type	The license rule type.
Conditions	The license rule conditions.
ID	The ID of the license rule.
Created	Date and time when the license rule was created.

Property name	Description
Last modified	Date and time when the license rule was last modified.
Modified by	By whom the license rule was modified.

If you make a selection in the overview and click **Edit** in the action bar, the login access rule edit page is displayed.

Site license

Before you can begin working with the Qlik Management Console (QMC), you need to enter your license information. If the license information has expired, you need to update it.

You have two options when entering your license, you either use a serial number and a control number, or a signed license key. The analyzer capacity license requires a signed license key.

With a signed license key, you need internet access (direct or through a proxy) to access the cloud-based license backend, for user assignments, analytic time consumption, and product activations.

> *With a signed license key, license information can be viewed in the QMC after the license key is entered and saved using **Apply**.*

The License Enabler File (LEF) determines the number of available tokens for a Qlik Sense site. The access types determine the access pattern within a Qlik Sense site. Allocating access types to users reduces the number of available tokens.

The property group **Site license** contains properties related to the license for the Qlik Sense system. All fields are mandatory and must not be empty.

Site licence properties

Property name	Description
Owner name	The user name of the Qlik Sense product owner.
Owner organization	The name of the organization that the Qlik Sense product owner is a member of.
Serial number	The serial number assigned to the Qlik Sense software.
Control number	The control number assigned to the Qlik Sense software.
LEF access	The License Enabler File (LEF) assigned to the Qlik Sense software.

Extensions

Extensions can be several different things: A widget library, a custom theme, or a visualization extension, used to visualize data, for example, in an interactive map where you can select different regions.

The **Extensions** overview lists all the available extensions. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

💡	*You can adjust the column width by dragging the header border.*

Extension fields

Field	Description
Name	The extension name, defined from the QMC.
Owner	The extension owner, by default the user who uploaded the extension.
Tags	The tags that are connected to the extension.
ID	The ID of the extension.
Created	The date and time when the extension was created.
Last modified	The date and time when the extension was last modified.
Modified by	By whom the extension was modified.
\<Custom properties>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌧▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌧▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. ⓘ *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
⟳	Refresh the page.

Field	Description
Edit	Edit the selected extensions.
Delete	Delete the selected extensions.
⊕**Import**	Import a new extension. ⚠ *If you import an extension that already exists in QMC, when prompted, replace the existing file with the new one by clicking **Replace**, or click ✕ to cancel.*
Export	Export an extension. ⓘ *When you export an app, extensions are not included in the export. This may result in some visualizations not being rendered when moving apps between different instances of Qlik Sense. The extensions can be obtained from the shared folder given during the installation, for example: \\<domain>\QlikShare\StaticContent\Extensions.*
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

💡 *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

Extension: associated items

The tables in this document show the fields available for the **Contents** and **Security rules** property groups.

By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

💡 *You can adjust the column width by dragging the header border.*

User access

User access is available from **Associated items** when you edit a resource.

The preview shows a grid of the target resources and the source users who have access to the selected items.

Depending on rights, you can either edit or view a user, a resource, or an associated rule.

Security rules

Security rules is available from **Associated items** when you edit extensions. The overview contains a list of the security rules that are associated with the selected extensions.

The **Security rules** property group contains the user condition properties.

User condition properties

Property	Description
Name	The name of the security rule.
Description	The description of what the rule does.
Resource filter	The ID for the rule.
Actions	The permitted actions for the rule.
Disabled	Status values: **Yes** or **No**.
Context	The security rule context (**QMC**, **Hub**, or **Both**).
Type	The security rule type (**Default**, **Read only**, or **Custom**).
Conditions	The security rule conditions.
ID	The ID of the security rule.
Created	Date and time when the security rule was created.
Last modified	Date and time when the security rule was last modified.
Modified by	By whom the security rule was modified.

If you make a selection in the overview and click **Edit** in the action bar, the edit security rule page is displayed.

Tags

You create tags and apply them to resources to be able to search and manage the environment efficiently from the resource overview pages in the QMC.

The **Tags** overview lists all the available tags. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

> *You can adjust the column width by dragging the header border.*

Tags properties

Field/Button	Description
Name	The name of the QMC tag.
Occurrences	The number of resources that the tag is connected to.
ID	The ID of the tag.
Created	The date and time when the tag was created.
Last modified	The date and time when the tag was last modified.
Modified by	By whom the tag was modified.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.

⌐▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌐▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
⊞	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.
Edit	Edit the selected tags.
Delete	Delete the selected tags.
⊕ **Create new**	Create a new tag.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.

On-demand apps

On-demand apps are generated in the Qlik Sense hub from navigation links that connect selection apps to template apps. Selection and template apps can also be published to streams from the QMC or from the Qlik Sense hub. Generated on-demand apps can also be published from the QMC or the Qlik Sense hub.

You can adjust the column width by dragging the header border.

On-demand app service properties

Selection and template apps can be created without the On-demand app service being enabled, but the service must be enabled to create navigation links and generate on-demand apps. The following properties of the On-demand app service can be managed:

Property descriptions

Property	Description
Enable on-demand app service	Enables and disables the On-demand app service. The service is disabled by default.
	When the service is switched from enabled to disabled, any pending requests to generate on-demand apps are allowed to finish. But once the service has been disabled, no new requests to generate apps will be accepted.
Enable dynamic views	With dynamic views you can refresh charts from within your analytic tool environment. The on-demand app service must be turned on to enable dynamic views.
	Turn on dynamic views to allow app sheets to contain charts that are loaded from data sources on-demand.
	If you have apps whose sheets contain charts based on dynamic views and the **Dynamic views** setting is disabled for the tenant, the apps will continue to function with the following limitations:
	• All dynamic charts appear dimmed (and without data) to indicate that the dynamic view functionality has been disabled.
	• The sheet editor does not expose the dynamic view assets.
	All charts and features not related to dynamic views will continue to function normally.
Logging level	Specifies the level of detail written to the service log file.
Number of apps that can be generated at one time	Specifies the number of apps the service can generate at one time. The default is 1 and the maximum is 10.
	This setting affects the response time for an app generation, but the amount of data loaded must also be considered when setting the number of apps that can be generated at one time. When the data load sizes are moderate, a higher number of apps generated at one time will improve response time for each app. But when load sizes are large, the response can be slower than if the setting were lower and apps had to wait in queue to be generated.
	In a multi-node environment, the setting for the number of apps that can be generated at one time applies to all instances of the On-demand app services running in that environment. If multiple services use the same Qlik associative engine, the load on that Qlik associative engine could be the cumulative number of apps to generate at one time from the multiple instances of the service.

Property	Description
Number of days before purging historical data	Specifies the number of days certain historical data about on-demand apps is kept before the data is removed. Values can be 0-365. A setting of 0 means the data is never deleted. The default value is 90 days. The On-demand app service keeps data about navigation links and about requests to generate and reload on-demand apps. When an on-demand app navigation link is deleted, it is retained in a decommissioned state. When the number of days specified before purging is reached, data about the navigation link is removed. The On-demand app service also retains information about requests to generate and reload on-demand apps. When on-demand apps are deleted, the information about their reload requests is retained for the number of days specified before purging.
Allow anonymous user to generate apps	Allows anonymous users to generate on-demand apps from navigation points on published selection apps. This setting applies only on Qlik Sense systems that have set anonymous authentication. *Anonymous authentication (page 457)* An anonymous user can generate apps only from navigation links that are published automatically. If the generated app is not published automatically, the anonymous user would not have access to it.
The proxy user that will be used for generating apps on behalf of the anonymous users	Select a user to serve as a proxy user for anonymous users. Choose any registered user who can create on-demand app requests. The proxy user must also have read permission on the on-demand selection apps that are accessible to anonymous users. Do not select an administrative user (*INTERNAL\sa-xxx*) as the proxy or any user who has root admin privileges. ⚠ *When creating streams that will contain on-demand selection apps that can be used by anonymous users, you must set the security rule to permit read access to the on-demand app proxy user. Failure to include read access to the proxy user will cause all of the links in the app navigation bar to show as "Invalid".* Although a single user serves as the proxy for all anonymous users, each anonymous user is identified and distinguished by the On-Demand App Service. This allows each anonymous user access to the his generated apps but prevents other anonymous users from accessing those apps. Each anonymous user can access only apps she has generated.

Property	Description
Number of minutes to keep apps generated by anonymous users	Specifies the amount of time an app generated by an anonymous is kept before it is deleted. The default setting is 60 minutes.
	The time is measured from the last data load.
	There is also a retention time setting on navigation links. For an app generated by an anonymous user, the shorter of the two retention time settings is used.
	For example, when a navigation link with a retention time setting of 24 hours is used by an anonymous user and the setting for the **Number of minutes to keep apps generated by anonymous users** is set to 60 minutes, the app would be deleted 60 minutes after its last data load. If however the navigation link setting for retention time is 30 minutes, then the app generated by the anonymous user would be deleted 30 minutes after the last data load.
	⚠ *If **Number of minutes to keep apps generated by anonymous users** is set to zero (0), then the apps are kept for the longest time possible, which is 365 days.*

User directory connectors

The user directory connector (UDC) connects to a configured directory service to retrieve users. The UDCs supplied with the Qlik Sense installation are Generic and Advanced LDAP, Active Directory, ApacheDS, ODBC, Access (via ODBC), Excel (via ODBC), SQL (via ODBC), and Teradata (via ODBC).

> ⓘ *No UDC is required for a local user to log on to Qlik Sense. However, for the local user to be able to access apps, you need to allocate access. With a user-based license, you can use professional or analyzer access rules. With a token-based license, you can use user or login access rules to allocate access. Alternatively, a local user can first log on to be recognized as a user, and then be allocated tokens.*

> ⓘ *Qlik Sense supports only Microsoft directory servers to be added as User Directory Connectors of type Active directory, Generic LDAP and Advanced LDAP.*

> ⓘ *User attribute names and values must comply with the syntax definition of the LDAP standard when used in security rules. This means that the following constraints apply:*
> *• Attribute name: Can only contain a-z, A-Z, 0-9, and "-". Must start with a-z or A-Z.*
> *• Attribute value: Any UTF-8 string.*

> *If you use a PostgreSQL database, and have table names with capital letters, or special characters, such as ".", you must enclose the table names with quotation marks. Without quotation marks, validation of the table names will result in an error. Examples of table names: "table.Name", public."Table" (or "Table"), testschema."Table".*

> *If you sync users and a user attribute has the same name as a column in the user table, that column will be unavailable in the column selector and table rendering may be erratic.*

The **User directory connectors** overview lists all the available user directory connectors. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

User directory connectors

Field/Button	Description
Name	The name of the user directory connector configuration, entered from the QMC.
User directory	The user directory name depends on the user directory configuration: • Entered manually for ODBC and LDAP. • Generated from the connector's properties for Active Directory. > *The value of the **User directory** must be unique; otherwise the connector cannot be configured. The **User directory** value is used when creating a security rule to a user directory.*
Type	Generic LDAP, Advanced LDAP, Microsoft Active Directory, ApacheDS, ODBC, Access (via ODBC), Excel (via ODBC), or SQL (via ODBC).
Configured	Status values: **Yes** or **No**. To be configured, the user directory name must be unique and not blank.
Operational	Status values: **Yes** or **No**. Operational means that the configuration of the connector properties enables communication with the user directory. > *Different connectors require different properties. Check the UserManagement_Repository log at this location:* > *%ProgramData%\Qlik\Sense\Log\Repository\Trace.*

Status	The status of the user directory connector: • **Idle**: When no synchronization is performed. • **External fetch**: The first phase of the synchronization, when fetching the data from the directory service. • **Database store**: The second phase of the synchronization, when storing the data in the QRS. *If the status is displayed as **Idle** and **Last started** is more recent than **Last finished** the synchronization has failed.*
Last started sync	The date and time when synchronization of user data last started. The synchronization is either triggered by a task or started manually from the user directory connectors overview. *Last started sync and **Last successfully finished sync** are updated when a user synchronization is triggered, which happens, for example, when a user who belongs to the UDC or the same domain accesses the hub, the dev-hub, or the QMC.*
Last successfully finished sync	The date and time when synchronization of user data last finished successfully. *Last started sync and **Last successfully finished sync** are updated when a user synchronization is triggered, which happens, for example, when a user who belongs to the UDC or the same domain accesses the hub, the dev-hub, or the QMC.*
Tags	The names of the connected tags.

Sync user data for existing users	Status values: **Yes** or **No**. Yes is displayed when this option is selected. • When selected, only the existing users are synchronized. An existing user is a user who has logged in to Qlik Sense and/or been previously synchronized from the configured directory service. • When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service. You can create a filter to **Active Directory**, **ApacheDS**, **Generic LDAP**, or **Advanced LDAP**, if you only want to synchronize a selection of users. *We recommend that you keep this option selected if you have a user directory with a large number of users and user attributes.* *The user attributes are only synced when a user logs in to the hub. Even if you delete the user in the QMC, the active session is still valid for the user that has been deleted. If the hub is only refreshed, the user is added to the database, but without any attributes.*
ID	The ID of the user directory connector.
Created	The date and time when the user directory was created.
Last modified	The date and time when the user directory connector was last modified.
Modified by	The user ID of the user who modified the user directory connector.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⧩	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⧩ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*

⊞	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page. ⓘ *If you have added a new user directory connector type you need to press F5 to refresh the list of available user directory connectors.*
Edit	Edit the selected user directory connector.
Delete	Delete the selected user directory connector.
Sync	Synchronize the user data via the selected user directory connectors.
⊕**Create new**	Create a new user directory connector.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

💡 *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

User directory connectors Generic LDAP properties

The following property groups are available for user directory connectors of the type Generic LDAP.

Identification

All fields are mandatory and must not be empty.

Identification properties

Property	Description
Name	The name of the UDC configuration, defined from the QMC.
Type	The UDC type.

User sync settings

User sync properties

Property	Description	Default value
Sync user data for existing users	• When selected, only the existing users are synchronized. An existing user is a user who has logged in to Qlik Sense and/or been previously synchronized from the configured directory service. • When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service. You can create a filter to **Active Directory**, **ApacheDS**, **Generic LDAP**, or **Advanced LDAP**, if you only want to synchronize a selection of users. *The user attributes are only synced when a user logs in to the hub. Even if you delete the user in the QMC, the active session is still valid for the user that has been deleted. If the hub is only refreshed, the user is added to the database, but without any attributes.*	Selected

Connection

Connection properties

Property	Description	Default value
User directory name	Must be unique, otherwise the connector will not be configured. The name of the UDC instance (to be compared to the domain name of an Active Directory). Together with the user's account name, this name makes a user unique. *Not entered manually for Active Directory.*	-
Path	The URI used to connect to the directory server. To support SSL, specify the protocol as LDAPS instead. *Custom ports are not supported.*	ldap://company.domain.com
User name	The optional user ID used to connect to the directory server. If this is empty, the user running the Qlik Sense repository is used to log on to the directory server.	-
Password	The optional password for the user.	-

> *When a user creates an Active Directory connector, the connector will only work if the user running the Qlik Sense services is allowed to access the directory server. If the user running the Qlik Sense services is not allowed to access the directory server, a user name and a password that allows access to the directory server must be provided.*

Advanced

The **Advanced** property group contains the advanced LDAP connector properties in the Qlik Sense system.

Advanced properties

Property	Description	Default value
Additional LDAP filter	Used as the LDAP query to retrieve the users in the directory.	-
Synchronization timeout (seconds)	The timeout for reading data from the data source.	240
Page size of search	Determines the number of posts retrieved when reading data from the data source. When the specified number of posts have been found, search is stopped and the results are returned. When search is restarted, it continues where it left off. > *If the user synchronization is unsuccessful, try setting the value to '0' (zero), which is equal to not doing a paged search.*	2000 (For ApacheDS: 1000)
Use optimized query	This property allows Qlik Sense to optimize the query for directories containing many groups in proportion to the number of users retrieved. > *To be able to use the optimization, the directory must be set up so that the groups refer to the users. If the directory is not set up correctly, the optimized query will not find all groups connected to the users.* This property is only visible for Generic LDAP and Active directory search, (Active Directory always uses optimization).	Not selected

Property	Description	Default value
Authentication type	Optional. Authentication type to connect to LDAP. The values can be comma separated. Values: *Secure, Encryption, SecureSocketsLayer, ReadonlyServer, FastBind, Signing, Sealing, Delegation, ServerBind*. > *To support "LDAP Channel Binding and LDAP Signing in Active Directory and Generic LDAP UDCs", use the following Authentication type values: Secure,Signing.*	*FastBind* or *Anonymous*, based on the credentials settings.

Directory entry attributes

> *The directory entry attributes are case-sensitive.*

Directory entry attribute properties

Property	Description	Default value
Type	The attribute name that identifies the type of directory entry (only users and groups are used by the LDAP UDC).	objectClass
User identification	The attribute value of the directory entry that identifies a user.	inetOrgPerson
Group identification	The attribute value of the directory entry that identifies a group.	group
Account name	The unique user name (within the UDC) that the user uses to log in.	sAMAccountName
Email	The attribute name that holds the emails of a directory entry (user).	mail
Display name	The full name of either a user or a group directory entry.	name
Group membership	The attribute indicates direct groups that a directory entry is a member of. Indirect group membership is resolved during the user synchronization. This setting, or the one below, **Members of directory entry**, is allowed to be empty, which means that the group membership is resolved using only one of the two settings.	memberOf
Members of directory entry	The attribute name that holds a reference to the direct members of this directory entry. See also the **Group membership** setting, above.	member

Property	Description	Default value
Custom attributes (only Advanced LDAP)	Extra LDAP object attributes to be retrieved. The custom attributes can be used in security rules and license assignment rules. Separate multiple custom attributes with commas. For an example of using custom attributes, see Qlik Sense Enterprise on Windows: How to sync custom attributes from Active Directory with Advanced LDAP.	-

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

User directory connectors Advanced LDAP properties

The following property groups are available for user directory connectors of the type Advanced LDAP.

Identification

All fields are mandatory and must not be empty.

Identification properties

Property	Description
Name	The name of the UDC configuration, defined from the QMC.
Type	The UDC type.

User sync settings

User sync properties

Property	Description	Default value
Sync user data for existing users	• When selected, only the existing users are synchronized. An existing user is a user who has logged in to Qlik Sense and/or been previously synchronized from the configured directory service. • When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service. You can create a filter to **Active Directory**, **ApacheDS**, **Generic LDAP**, or **Advanced LDAP**, if you only want to synchronize a selection of users. *The user attributes are only synced when a user logs in to the hub. Even if you delete the user in the QMC, the active session is still valid for the user that has been deleted. If the hub is only refreshed, the user is added to the database, but without any attributes.*	Selected

Connection

LDAP connection properties

Property	Description	Default value
User directory name	Must be unique, otherwise the connector will not be configured. The name of the UDC instance (to be compared to the domain name of an Active Directory). Together with the user's account name, this name makes a user unique. *Not entered manually for Active Directory.*	

Property	Description	Default value
Host	Hostname with port separated by ":" If hostname is the IP address, add the following value in the **Flags** field: *no_fqdn*. Use port 3268/(If LDAPs: 3269) for Global catalog search. Check the corresponding ports open to LDAP server from the Qlik Sense installed server for the access.	company.com:port
User name	The optional user ID used to connect to the directory server. Format: *Domain name\User name* *If user name and password are empty, the user will be considered as an Anonymous user.*	
Password	The optional password for the user. *If user name and password are empty, the user will be considered as an Anonymous user.*	
Timeout (seconds)	Connection timeout in seconds.	500
Base DN	Base DN in LDAP to select.	cn=builtin,dc=company,dc=com

When a user creates an Active Directory connector, the connector will only work if the user running the Qlik Sense services is allowed to access the directory server. If the user running the Qlik Sense services is not allowed to access the directory server, a user name and a password that allows access to the directory server must be provided.

Advanced

The **Advanced** property group contains the advanced LDAP connector properties in the Qlik Sense system.

LDAP advanced properties

Property	Description	Default value
Page size	Determines the number of posts retrieved when reading data from the data source. When the specified number of posts have been found, search is stopped and the results are returned. When search is restarted, it continues where it left off. *If the user synchronization is unsuccessful, try setting the value to '0' (zero), which is equal to not doing a paged search.*	2000 (For ApacheDS: 1000)
Use optimized query	This property allows Qlik Sense to optimize the query for directories containing many groups in proportion to the number of users retrieved. *To be able to use the optimization, the directory must be set up so that the groups refer to the users. If the directory is not set up correctly, the optimized query will not find all groups connected to the users.* This property is only visible for Generic LDAP, Advanced LDAP, and Active directory search (Active Directory always uses optimization).	Not selected
Timeout (seconds)	The timeout for reading data from the data source.	400
Authentication type	Authentication type to connect to LDAP. Options: *Anonymous*, *Basic*, *Negotiate*, *NTLM*, *Digest*, *Sicily*, *DPA*, *MSN*, *External*, *Kerberos*.	-

Property	Description	Default value
Flags	Flags to mention LDAP connection session settings. Multiple values can be specified, comma separated. *Tcpkeepalive*: Enables TCP keep-alive. *Autoreconnect*: Enables Autoreconnect. *Rootdsecache*: Enables the internal RootDSE cache. *Sealing*: Enables Kerberos encryption. *Secure socket layer or ssl*: Enables secure socket layer on the connection. *Signing*: Enables Kerberos encryption. *Connectionless*: Specifies whether the connection is UDP. *No_fqdn*: Use this flag if host in the **Host** field is given as an IP address. *noclientcert*: Skip the default callback function used to specify client certificates when establishing an SSL connection. *NoCertVerify*: Skip server certificate verification when an SSL connection is established. ⓘ *Don't use NoCertVerify and Certdebug together.* *Certdebug*: Get specific server certificate validation errors, if any, for debugging. *AllProps*: Fetch all attributes of the LDAP object.	-

Property	Description	Default value
Locator flags	Locator flag for DC locator. Multiple values can be specified, comma separated. *None* *ForceRediscovery* *DirectoryServiceRequired* *DirectoryServicePreferred* *GCRequired* *PdcRequired* *IPRequired* *KdcRequired* *TimeServerRequired* *WriteableRequired* *GoodTimeServerPreferred* *AvoidSelf* *OnlyLdapNeeded* *IsFlatName* *IsDnsName* *ReturnDnsName* *ReturnFlatName*	-
Search LDAP filter	Optional LDAP filter query.	-
Protocol version	LDAP protocol version to use.	3
Simple authentication and security layer (SASL) method	SASL Binding method: *gssapi* *external* *gss-spnego* *digest-md5*	-
Certificate path	Path of the client certificates to send for authentication.	-

Directory entry attributes

ℹ	*The directory entry attributes are case-sensitive.*

LDAP directory entry attribute properties

Property	Description	Default value
Type	The attribute name that identifies the type of directory entry (only users and groups are used by the LDAP UDC).	objectClass
User identifier	The attribute value of the directory entry that identifies a user.	inetOrgPerson
Group identifier	The attribute value of the directory entry that identifies a group.	group
Account name	The unique user name (within the UDC) that the user uses to log in.	sAMAccountName
Email	The attribute name that holds the emails of a directory entry (user).	mail
Display name	The full name of either a user or a group directory entry.	name
Group membership	The attribute indicates direct groups that a directory entry is a member of. Indirect group membership is resolved during the user synchronization. This setting, or the one below, **Members of directory entry**, is allowed to be empty, which means that the group membership is resolved using only one of the two settings.	memberOf
Members of directory entry	The attribute name that holds a reference to the direct members of this directory entry. See also the **Group membership** setting, above.	member
Custom attributes	Extra LDAP object attributes to be retrieved. The custom attributes can be used in security rules and license assignment rules. Separate multiple custom attributes with commas. For an example of using custom attributes, see ↪ [Qlik Sense Enterprise on Windows: How to sync custom attributes from Active Directory with Advanced LDAP](#).	

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

User directory connectors Active Directory properties

The following property groups are available for user directory connectors of the type Active Directory.

Identification

All fields are mandatory and must not be empty.

Identification properties

Property	Description
Name	The name of the UDC configuration, defined from the QMC.
Type	The UDC type.

User sync settings

User sync properties

Property	Description	Default value
Sync user data for existing users	• When selected, only the existing users are synchronized. An existing user is a user who has logged in to Qlik Sense and/or been previously synchronized from the configured directory service. • When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service. You can create a filter to **Active Directory**, **ApacheDS**, **Generic LDAP**, or **Advanced LDAP**, if you only want to synchronize a selection of users. *The user attributes are only synced when a user logs in to the hub. Even if you delete the user in the QMC, the active session is still valid for the user that has been deleted. If the hub is only refreshed, the user is added to the database, but without any attributes.*	Selected

Connection

The **Connection** property group contains the Active Directory connection properties in the Qlik Sense system.

Connection properties

Property	Description	Default value
Path	The URI used to connect to the AD domain.	ldap://company.domain.com
User name	The optional user ID used to connect to the AD server. If this is empty, the user running the Qlik Sense repository is used to log on to the AD server.	-
Password	The optional password for the user above.	-

> *If you have users in several subdomains in your Active Directory, you need to create one user directory connector for each subdomain.*

Advanced

The **Advanced** property group contains the advanced Active Directory properties.

Advanced properties

Property	Description	Default value
Additional LDAP Filter	Used as the LDAP query to retrieve the users in the AD.	Blank
Synchronization timeout (seconds)	The timeout for reading data from the data source.	240
Page size of search	Determines the number of posts retrieved when reading data from the data source. When the specified number of posts have been found, search is stopped and the results are returned. When search is restarted, it continues where it left off. *If the user synchronization is unsuccessful, try setting the value to '0' (zero), which is equal to not doing a paged search.*	2000

Tags

<div align="center">Tags properties</div>

Property	Description
Tags	*If no tags are available, this property group is empty.*
	Connected tags are displayed under the text box.

User directory connectors ApacheDS properties

The following property groups are available for user directory connectors of the type ApacheDS.

Identification

All fields are mandatory and must not be empty.

<div align="center">Identification properties</div>

Property	Description
Name	The name of the UDC configuration, defined from the QMC.
Type	The UDC type.

User sync settings

<div align="center">User sync properties</div>

Property	Description	Default value
Sync user data for existing users	• When selected, only the existing users are synchronized. An existing user is a user who has logged in to Qlik Sense and/or been previously synchronized from the configured directory service. • When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service. You can create a filter to **Active Directory**, **ApacheDS**, **Generic LDAP**, or **Advanced LDAP**, if you only want to synchronize a selection of users. *The user attributes are only synced when a user logs in to the hub. Even if you delete the user in the QMC, the active session is still valid for the user that has been deleted. If the hub is only refreshed, the user is added to the database, but without any attributes.*	Selected

Connection

Connection properties

Property	Description	Default value
User directory name	Must be unique, otherwise the connector will not be configured. The name of the UDC instance (to be compared to the domain name of an Active Directory). Together with the user's account name, this name makes a user unique. *Not entered manually for Active Directory.*	-
Path	The URI used to connect to the directory server. To support SSL, specify the protocol as LDAPS instead. *Custom ports are not supported.*	ldap://company.domain.com
User name	The optional user ID used to connect to the directory server. If this is empty, the user running the Qlik Sense repository is used to log on to the directory server.	-
Password	The optional password for the user.	-

When a user creates an Active Directory connector, the connector will only work if the user running the Qlik Sense services is allowed to access the directory server. If the user running the Qlik Sense services is not allowed to access the directory server, a user name and a password that allows access to the directory server must be provided.

Advanced

The **Advanced** property group contains the advanced LDAP connector properties in the Qlik Sense system.

Advanced properties

Property	Description	Default value
Additional LDAP filter	Used as the LDAP query to retrieve the users in the directory.	-
Synchronization timeout (seconds)	The timeout for reading data from the data source.	240

Property	Description	Default value
Page size of search	Determines the number of posts retrieved when reading data from the data source. When the specified number of posts have been found, search is stopped and the results are returned. When search is restarted, it continues where it left off. 💡 *If the user synchronization is unsuccessful, try setting the value to '0' (zero), which is equal to not doing a paged search.*	2000 (For ApacheDS: 1000)
Use optimized query	This property allows Qlik Sense to optimize the query for directories containing many groups in proportion to the number of users retrieved. ⚠ *To be able to use the optimization, the directory must be set up so that the groups refer to the users. If the directory is not set up correctly, the optimized query will not find all groups connected to the users.* This property is only visible for Generic LDAP and Active directory search, (Active Directory always uses optimization).	Not selected
Authentication type	Optional. Authentication type to connect to LDAP. The values can be comma separated. Values: *Secure*, *Encryption*, *SecureSocketsLayer*, *ReadonlyServer*, *FastBind*, *Signing*, *Sealing*, *Delegation*, *ServerBind*. ℹ *To support "LDAP Channel Binding and LDAP Signing in Active Directory and Generic LDAP UDCs", use the following Authentication type values: Secure,Signing.*	*FastBind* or *Anonymous*, based on the credentials settings.

Directory entry attributes

The **Directory entry attributes** property group contains the directory entry attributes for the LDAP connector.

ℹ *The directory entry attributes are case-sensitive.*

Directory entry attribute properties

Property	Description	Default value
Type	The attribute name that identifies the type of directory entry (only users and groups are used by the ApacheDS UDC).	objectClass
User identification	The attribute value of the directory entry that identifies a user.	inetOrgPerson
Group identification	The attribute value of the directory entry that identifies a group.	groupOfNames
Account name	The unique user name (within the UDC) that the user uses to log in.	uid
Email	The attribute name that holds the emails of a directory entry (user).	mail
Display name	The full name of either a user or a group directory entry.	cn
Group membership	The attribute name that indicates direct groups that a directory entry is a member of. Indirect group membership is resolved during the user synchronization. This setting or the one below, **Members of directory entry**, is allowed to be empty, which means that the group membership is resolved using only one of the two settings.	-
Members of directory entry	The attribute name that holds a reference to the direct members of this directory entry. See also the **Group membership** setting, above.	member

Tags

Tags properties

Property	Description
Tags	💡 *If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

User directory connectors ODBC properties

Four ODBC options exist when creating a new user directory connector (UDC). They all have the same properties and fields, but for **Access (via ODBC)**, **Excel (via ODBC)**, **SQL (via ODBC)**, and **Teradata (via ODBC)**, some of the fields contain default values for support. You will most likely have to change those values.

> ℹ️ *If you use a PostgreSQL database, and have table names with capital letters, or special characters, such as ".", you must enclose the table names with quotation marks. Without quotation marks, validation of the table names will result in an error. Examples of table names: "table.Name", public."Table" (or "Table"), testschema."Table".*

> ℹ️ *If you sync users and a user attribute has the same name as a column in the user table, that column will be unavailable in the column selector and table rendering may be erratic.*

The following property groups are available for ODBC UDC.

Identification

All fields are mandatory and must not be empty.

Identification properties

Property	Description
Name	The name of the UDC configuration, defined from the QMC.
Type	The UDC type.

User sync settings

User sync properties

Property	Description	Default value
Sync user data for existing users	• When selected, only the existing users are synchronized. An existing user is a user who has logged in to Qlik Sense and/or been previously synchronized from the configured directory service. • When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service. You can create a filter to **Active Directory**, **ApacheDS**, **Generic LDAP**, or **Advanced LDAP**, if you only want to synchronize a selection of users. > ℹ️ *The user attributes are only synced when a user logs in to the hub. Even if you delete the user in the QMC, the active session is still valid for the user that has been deleted. If the hub is only refreshed, the user is added to the database, but without any attributes.*	Selected

Connection

> ℹ️ *When loading .txt files using Microsoft Access Text Driver (*.txt, *.csv), you must use the connector type **Access (via ODBC)** instead of **ODBC**.*

Connection properties

Property	Description	Default value
User directory name	The name of the user directory. Must be unique, otherwise the connector will not be configured. The name must not contain spaces.	-
Users table name	The name of the table containing the users. Include the file extension in the table name, for example: *Table.csv*. *When setting up an Oracle ODBC user directory connector, the* **Users table name** *and* **Attributes table name** *must be prefaced by the owner of those tables. For example: OWNER.USERS instead of only USERS.*	-
Attributes table name	The name of the table containing the user attributes. Include the file extension in the table name, for example: *Table.csv*. *When setting up an Oracle ODBC user directory connector, the* **Users table name** *and* **Attributes table name** *must be prefaced by the owner of those tables. For example: OWNER.USERS instead of only USERS.*	-

Visible connection string	The visible part of the connection string that is used to connect to the data source. Specify one of the following:
	
	• A full connection string, for example: *Driver={SQL Server Native Client 11.0};Server=localhost;Database=Users;Trusted_Connection=yes;*
	  1. *Driver* must point to a driver currently on the machine. In the **ODBC Data Source Administrator**, check which driver to specify. Search for "data source" to find the application.
	  2. *Server* must point to the server that you want to connect to.
	  3. *Database* must point to the database where the tables are.
	  4. *Trusted_Connection=yes* may be required, depending on the setup. In this example it is required.
	
	• A pointer to an established System DSN, for example, *dsn=MyDSN;*
	
	The two connection strings are concatenated into a single connection string when making the connection to the database.
		-

Property	Description	Default value
Encrypted connection string	The encrypted part of the connection string that is used to connect to the data source. Typically, this string contains user name and password. **Example:** Assume that you have a connection string as follows: *Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;Uid=Admin;Pwd=verySecretAdminPassword;* You do not want to store that connection string in the database as it is, because the secret password would then be visible to others. To protect the password, do the following: Save the first part: *Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;* in the **Visible connection string** field, and the second part: *Uid=Admin;Pwd=verySecretAdminPassword;* in the **Encrypted connection string** field. The second part is then stored encrypted in the database and is not shown when you open the UDC again for editing. *The two connection strings are concatenated into a single connection string when making the connection to the database.*	-
Synchronization timeout (seconds)	The timeout for reading data from the data source.	240

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

User directory connector: associated items

The following table presents the available fields for the associated items. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

> *You can adjust the column width by dragging the header border.*

User access

User access is available from **Associated items** when you edit a resource.

The preview shows a grid of the target resources and the source users who have access to the selected items.

Depending on rights, you can either edit or view a user, a resource, or an associated rule.

Tasks

Tasks is available from **Associated items** when you edit a used directory connector. The overview contains a list of tasks associated with the selected used directory connector.

Task properties

Property	Description
Name	The name of the task.
Type	The type of task (user synchronization or reload).
UDC name	The user directory connector that the task is associated with.
Enabled	Status values: **Yes** or **No**.
Status	The status of the task.
Tags	The tags associated with the task.
ID	The ID of the task.
Created	Date and time when the task was created.
Last modified	Date and time when the task was last modified.
Modified by	By whom the task was modified.
Custom properties	Custom properties, if any, are listed here.

Monitoring apps

The governance apps present data from the Qlik Sense log files.

The following apps are included in the default installation:

- License Monitor
- Operations Monitor

Select **Monitoring apps** on the **QMC start** page, or from the **Start**▼ drop-down menu, to open the hub for the stream **Monitoring apps** with the apps License Monitor and Operations Monitor.

The default path to the Qlik Sense log folder is *%ProgramData%\Qlik\Sense\Log\<Service>*.

> ⚠ *Do not delete the **Monitoring apps** stream. If the stream is deleted, it is irrevocably gone. (RootAdmins, ContentAdmins, and SecurityAdmins can delete the stream.)*

Service cluster

A service cluster is a collection of nodes. Gathering the nodes into a cluster enables central configuration.

On a multi-node site, the service cluster stores configurations, such as persistence type, database connection, and static content folder, for all nodes. All nodes are linked to the service cluster so that the settings can be unified.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Service cluster** on the QMC start page or from the **Start**▼ drop-down menu to display the service cluster page.

Identification

Identification properties

Property	Description
Name	Service cluster name.

Cluster settings

Cluster settings properties

Property	Description
Root folder	The root folder path will, by default, be used for the root subfolders, unless a different path is explicitly stated. If the root folder has the path *//myhost/share*, the default root subfolder path will be *//myhost/share/<root subfolder>*.
App folder	Root subfolder to which all nodes connect to retrieve apps.
Static content root folder	Root subfolder that contains static content, such as images.
Archived logs root folder	Root subfolder, one for each host.
Failover timeout (minutes)	Amount of time that the central node can be offline before a failover occurs. Default value: 10 minutes. This value is editable.

Data encryption

Database encryption properties

Property	Description
QVF encryption	Encrypts the Qlik Sense apps (QVF) with the encryption key provided in the *Encryption key* input field. App content (data and bookmarks) is being encrypted when saved. Apps that were created before QVF encryption was enabled will be encrypted the next time they are saved with updates to data or bookmarks.
QVD encryption	Encrypts new Qlik Sense data files (QVD) that are created with the STORE command in the data load script. The QVDs are encrypted with the encryption key provided in *Encryption key* input field. Data files are being encrypted when stored. Data files that were created before QVD encryption was enabled will be encrypted the next time the data is stored.
Encryption key	The encryption key to be used to encrypt Qlik Sense apps and Qlik Sense data files. This is the *Thumbprint* field of the encryption certificate.

Impersonation

Impersonation properties

Property	Description
Reload tasks	By selecting **Reload tasks**, you activate impersonation. Impersonation enables you to run reload tasks with the permissions of the app owner. Within a task chain, apps can have different owners, and then permissions to sources are dependent on each individual owner's access rights. When **Reloads tasks** is unselected, reload tasks run on behalf of the internal system account, *sa_scheduler*, that has elevated privileges and, technically, can use any data source.

Help us improve

Help us improve properties

Property	Description
Data collection	To improve our products and services, Qlik collects system and usage data. The data is anonymized, it does not contain any personal data. Data collection is a check box in the installation procedure, and is by default selected, that is, Qlik is entitled to collect data. Both during installation and afterward, you can select not to send data to Qlik by clearing the selection **Data collection**. To change the data collection setting in the QMC, you must have the required privilege.

Nodes

A node is a server that is using the configured Qlik Sense services. There is always a central node in a deployment and nodes can be added for different service configurations. There is always a repository on every node.

A Qlik Sense site is a collection of one or more server machines (that is, nodes) connected to a common logical repository or central node.

> *In a Shared Persistence multi-node installation, you can make one or more nodes failover candidates. In the case of a central node failure, a failover candidate will assume the role of central node.*

The **Nodes** overview lists all the available nodes. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

> *You can adjust the column width by dragging the header border.*

Node properties

Property	Description
Name	The name of the node.
Host name	The name of the host.
Central node	Status values: **Yes** or **No**. Displays **Yes** if the node is the central node.
Status	Displays the status of the services. One of the following statuses is displayed: • **(x) of (y) services are running** The number of services (x) that are running compared to the number of enabled services (y) on the node. • **(x) of (y) services are stopped** The number of services (x) that are stopped compared to the number of enabled services (y) on the node. • **(z) has stopped** The name of the service (z) that has stopped (if only one service has stopped). > *Click ⓘ in the **Status** column for more detailed information on the status of the node.*
Tags	The tags that are connected to the node.
Node purpose	Which environment the node is intended for: **Production**, **Development**, or **Both**.

Property	Description
Engine	Status values: **Yes** or **No**. **Yes**: The Qlik Sense Engine Service (QES) is active.
Proxy	Status values: **Yes** or **No**. **Yes**: The Qlik Sense Proxy Service (QPS) is active.
Printing	Status values: **Yes** or **No**. **Yes**: The Qlik Sense Printing Service (QPR) is active.
Scheduler	Status values: **Yes** or **No**. **Yes**: The Qlik Sense Scheduler Service (QSS) is active.
ID	The ID of the node.
Created	The date and time when the node was created.
Last modified	The date and time when the node was last modified.
Modified by	By whom the node was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌄▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌄▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. ⓘ *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↩ to reset to the default columns.

Property	Description
🔍	Search – both basic and more advanced searches. _Searching and filtering in the QMC (page 25)_
↻	Refresh the page.
Edit	Edit the selected nodes.
Delete	Delete the selected nodes.
Redistribute	Redistribute the selected nodes.
⊕**Create new**	Create a new node.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

> 💡 _Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items._

Node: associated items

The following associated items are available for nodes.

User access

User access is available from **Associated items** when you edit a resource.

The preview shows a grid of the target resources and the source users who have access to the selected items.

Depending on rights, you can either edit or view a user, a resource, or an associated rule.

Engines

The Qlik Sense Engine Service (QES) is the application service that handles all application calculations and logic.

The **Engines** overview lists all the available engines. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

> 💡 _You can adjust the column width by dragging the header border._

Engine **Node** properties

Property	Description
Node	The name of the engine node.

Property	Description

Status	One of the following statuses is displayed:
	
	• **Running**
	   The service is running as per normal.
	• **Stopped**
	   The service has stopped.
	• **Disabled**
	   The service has been disabled.
	
	Click 🛈 *in the* **Status** *column for more detailed information on the status.*
	
	Checking the status of Qlik Sense services (page 373).

Tags	The tags that are connected to the engine.
App autosave interval (seconds)	The number of seconds between autosaving of the apps. Autosave is always performed when a session ends. Everything except data is saved. To persist data, perform a reload in Data load editor.
App cache time (seconds)	The number of seconds that a Qlik Sense app is allowed to remain in memory, after the last session that used the app has ended.
Working folder	A scheduled reload will search for files in this directory when relative paths are used to define file location. *This setting is used to support legacy features in QlikView scripts for relative paths to files during reload. You cannot use this setting to change the directory where the apps are stored.*
Max number of undos	The maximum number of undos when editing app content, such as sheets, objects, bookmarks, and stories: min = 0, max = 999.
Performance log interval (minutes)	The number of minutes in-between performance logging entries.
Audit activity log level	Levels: **Off** or **Basic** (a limited set of entries)
Service log level	Each level from **Error** to **Info** includes more information than the previous level.
System log level	All the standard engine messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.

Property	Description
Performance log level	All the performance messages are saved to this logger (by default updated default every five minutes). The log contains, for example, the number of active users, the number of open sessions, and the CPU load.Each level from **Fatal** to **Debug** includes more information than the previous level.
QIX performance log level	All the QIX protocol performance messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Audit log level	More detailed, user-based messages are saved to this logger, for example, when the user makes a selection in an app. Each level from **Fatal** to **Debug** includes more information than the previous level.
Session log level	All the session messages are saved to this logger when a client session is terminated, for example, user information, machine ID, IP address and port number.Each level from **Fatal** to **Debug** includes more information than the previous level.
Traffic log level	All the traffic messages are saved to this logger, for example, all JSON-messages to and from the engine.Each level from **Fatal** to **Debug** includes more information than the previous level.
Analytic connections log level	All the analytic connections messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Allow data lineage	Status values: **Yes** or **No**. The data lineage is the origin of the data that is loaded into Qlik Sense).
Min memory usage (%)	The minimum memory capacity used by Qlik Sense.
Max memory usage (%)	The maximum memory capacity used by Qlik Sense.
CPU throttle (%)	The amount of CPU capacity used by Qlik Sense. Range: 0 - 100%
Standard mode	Status values: **Yes**: standard mode. **No**: legacy mode. For security reasons, Qlik Sense in standard mode does not support absolute or relative paths in the data load script or functions and variables that expose the file system. ⚠️ *Disabling standard mode can create a security risk by exposing the file system.*
HTTP callback port	The callback port used by the Qlik Sense Repository Service for sending HTTP events to engine.

Property	Description
Hypercube memory limit (bytes)	Limit for how much memory a hypercube evaluation can allocate during a request. If multiple hypercubes are calculated during the request, the limit is applied to each hypercube calculation separately . Note that the limit is not enforced on every allocation. If the setting has the value 0, the engine applies a global heuristic to limit the amount of simultaneously executing requests that allocate a lot of memory to calculations. A negative value disables the limit. For performance reasons, memory usage and limits are checked periodically rather than on every allocation, therefore it is possible to briefly exceed the limit in some cases.
Reload memory limit (bytes)	Limit for how much memory a reload request can allocate. A negative value or 0 disables the limit. For performance reasons, memory usage and limits are checked periodically rather than on every allocation, therefore it is possible to briefly exceed the limit in some cases.
Export memory limit (bytes)	Limit for how much memory the export part of an export data request can allocate. Allocations made due to calculations are not counted against this limit. A negative value or 0 disables the limit. For performance reasons, memory usage and limits are checked periodically rather than on every allocation, therefore it is possible to briefly exceed the limit in some cases.
Hypercube time limit (seconds)	Limits the single core CPU time equivalent that a hypercube calculation can use. The single core CPU time equivalent is a heuristic that approximates the CPU time spent, divided by the number of cores used during the calculation. This is not a hard limit and it is dependent on the complexity of processed calculation. A negative value or 0 disables the limit. For performance reasons, the CPU time is not tracked exactly.
Export time limit (seconds)	Limits the CPU time that the export part of an export data request can use. A negative value or 0 disables the limit.
Reload time limit (seconds)	Limits the CPU time that a reload request can use. A negative value or 0 disables the limit.

Property	Description
Create search index during reload	Status values: **Yes** or **No**. When selected, all apps on the server are indexed during reload so that performance during the first search session is improved.
ID	The ID of the engine.
Created	The date and time when the engine was created.
Last modified	The date and time when the engine was last modified.
Modified by	By whom the engine was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⯆▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⯆▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. ⓘ *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
⟳	Refresh the page.
Edit	Edit the selected engines.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

> *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

Printing

The Qlik Sense Printing Service (QPR) manages export in Qlik Sense.

The **Printing** overview lists all the available printing nodes. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

> *You can adjust the column width by dragging the header border.*

Available fields and buttons

Field	Details
Node	The name of the printing node.
Status	One of the following statuses is displayed: • **Running** The service is running as per normal. • **Stopped** The service has stopped. • **Disabled** The service has been disabled. > *Click ⓘ in the **Status** column for more detailed information on the status.* *Checking the status of Qlik Sense services (page 373).*
Tags	The tags that are connected to the printing service.
Audit activity log level	Each level from **Fatal** to **Debug** includes more information than the previous level.
Service log level	Each level from **Error** to **Info** includes more information than the previous level.
ID	The ID of the printing service.
Created	The date and time when the printing service was created.
Last modified	The date and time when the printing service was last modified.
Modified by	By whom the printing service was modified.

> *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

Proxies

The Qlik Sense Proxy Service (QPS) manages the Qlik Sense authentication, session handling, and load balancing.

The **Proxies** overview lists all the available proxies. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

> *You can adjust the column width by dragging the header border.*

<div align="center">Node properties</div>

Property	Details
Node	The name of the proxy node.

Status	One of the following statuses is displayed:
	
	• **Running**
	  The service is running as per normal.
	• **Stopped**
	  The service has stopped.
	• **Disabled**
	  The service has been disabled.
	
	> *Click 🛈 in the **Status** column for more detailed information on the status.*
	
	Checking the status of Qlik Sense services (page 373).

Tags	The tags that are connected to the proxy.
Service listen port HTTPS (default)	The secure listen port for the proxy, which by default manages all Qlik Sense communication. > *Make sure that port 443 is available for the Qlik Sense Proxy Service (QPS) to use because the port is sometimes used by other software, for example, web servers.*
Allow HTTP	Status values: **Yes** or **No**. **Yes**: Unencrypted communication is allowed. This means that both https (secure communication) and (http) unencrypted communication is allowed.

Property	Details
Service listen port HTTP	The unencrypted listen port, used when HTTP connection is allowed.
Authentication listen port	The listen port for the internal authentication module. ⓘ *When editing this port as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.*
Kerberos authentication	Status values: **Yes** or **No**. **Yes**: Kerberos authentication is enabled.
REST API listen port	The listen port for the proxy API. ⓘ *When editing this port as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.*
SSL browser certificate thumbprint	The thumbprint of the Secure Sockets Layer (SSL) certificate that handles the encryption of traffic from the browser to the proxy. When editing a proxy certificate and the Qlik Sense services run with an account without administrator privileges, you need to configure the private key permissions for the certificate.
Keep-alive timeout (seconds)	The maximum timeout period for a single HTTP/HTTPS request before closing the connection. Protection against denial-of-service attacks. This means that if an ongoing request exceeds this period, Qlik Sense proxy will close the connection. Increase this value if your users work over slow connections and experience closed connections.
Max header size (bytes)	The maximum total header size.
Max header lines	The maximum number of lines in the header.
Audit activity log level	Levels: **Off** or **Basic** (a limited set of entries)
Audit security log level	Levels: **Off** or **Basic** (a limited set of entries)
Service log level	Each level from **Error** to **Info** includes more information than the previous level.
Audit log level	More detailed, user-based messages are saved to this logger, for example, proxy calls. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log level	All the performance messages are saved to this logger. For example, performance counters and number of connections, streams, sessions, tickets, web sockets and load balancing information. Each level from **Fatal** to **Debug** includes more information than the previous level.

Property	Details
Security log level	All the certificates messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
System log level	All the standard proxy messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log interval (minutes)	The interval of performance logging.
ID	The ID of the proxy.
Created	The date and time when the proxy was created.
Last modified	The date and time when the proxy was last modified.
Modified by	By whom the proxy was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⬒	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⬒ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. > ℹ️ *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
⊞	Column selector: Select which columns to display in the overview. Click ↩ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*

Property	Details
⟳	Refresh the page.
Edit	Edit the selected proxy.
Show more items	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

> 💡 *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

Proxy: associated items

The following associated items are available for proxies.

Virtual proxies

The **Virtual proxies** property group contains the virtual proxy properties in the Qlik Sense system.

Virtual proxies properties

Property	Description
Description	The description of the virtual proxy.
Prefix	The path name in the proxy's URI that defines each additional path. Example: *https://[node/[prefix]/*
Session cookie header name	The name of the HTTP header used for the session cookie. This value is mandatory and must not be blank. ⓘ *From the February 2019 release, a suffix (-HTTP) is added to the session cookie header name when a user accesses the system over http.* 💡 *It can be useful to include the values of the Prefix property above as a suffix in the cookie name.*
Is default virtual proxy	Status values: **Yes** or **No**.
Custom properties	Custom properties, if any, are listed here.

Virtual proxies

One or more virtual proxies run on each Qlik Sense Proxy Service (QPS), making it possible to support several sets of site authentication, session handling, and load balancing strategies on a single proxy node.

The **Virtual proxies** overview lists all the available virtual proxies. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

> You can adjust the column width by dragging the header border.

Virtual proxies

Field/Button	Description
Description	The description of the virtual proxy.
Prefix	The path name in the proxy's URI that defines each additional path. You can only use lowercase letters in the prefix.
Session cookie header name	The name of the HTTP header used for the session cookie. > From the February 2019 release, a suffix (-HTTP) is added to the session cookie header name when a user accesses the system over http.
Is default virtual proxy	Status values: **Yes** or **No**.
Authentication method	**Ticket**: a ticket is used for authentication. **Header authentication static user directory**: allows static header authentication, where the user directory is set in the QMC. **Header authentication dynamic user directory**: allows dynamic header authentication, where the user directory is fetched from the header. - SAML: SAML2 is used for authentication. - JWT: JSON Web Token is used for authentication. - OIDC: OpenID Connect is used for authentication.
Linked to proxy service	Status values: **Yes** or **No**.
Tags	The tags that are connected to the virtual proxy.

Header authentication header name	The header name. The name cannot contain any of the following strings: • X-Qlik-Security • X-Qlik-User • X-Qlik-ProxySession • X-Qlik-ProxyId • X-Qlik-Trace • X-Qlik-App • X-Qlik-Capabilities For example, *Qlik-User*, *Y-Qlik-Userheader*, or *Userheader* are valid values, while *X-Qlik-Userheader* would result in an invalid request.
Header authentication static user directory	The name of the user directory where additional information can be fetched for header authenticated users.
Header authentication dynamic user directory	The pattern used for identification of the user directory where additional information can be fetched for header authenticated users.
Anonymous access mode	Three possible values: • **No anonymous user**: Users must supply user identity and credentials. • **Allow anonymous user**: Users enter as anonymous but can switch and log in with a user account. • **Always anonymous user**: Users are always anonymous.
Windows authentication pattern	The chosen authentication pattern for logging in. If the User-Agent header contains the Windows authentication pattern string, Windows authentication is used. If there is no matching string, form authentication is used.
Session cookie domain	By default the session cookie is valid only for the machine that the proxy is installed on. This (optional) property allows you to increase its validity to a larger domain. Example: `company.com`
Has secure attribute (https)	Option for session cookie that has the Secure attribute and uses https.
SameSite attribute (https)	SameSite attribute values for https: **No attribute**, **None**, **Lax**, **Strict** For more information, see *SameSite cookie attribute (page 167)*

Has secure attribute (http)	Option for session cookie that has the Secure attribute and uses http.
SameSite attribute (http)	SameSite attribute values for http: **No attribute**, **None**, **Lax**, **Strict** For more information, see *SameSite cookie attribute (page 167)*

Additional response headers	Headers added to all HTTP responses back to the client. Example:
	
	`Header1: value1`
	
	`Header2: value2`

Session inactivity timeout (minutes)	The maximum period of time with inactivity before timeout. After this, the session is invalid and the user is logged out from the system.
Extended security environment	Status values: **Yes** or **No**. **Yes**: The following information about the client environment is sent in the security header: OS, device, browser, and IP. **No**: The user can run the same engine session simultaneously on multiple devices.
SAML Metadata IdP	The metadata from the IdP, used to configure the service provider. Must exist for SAML authentication to work.
SAML entity ID	ID to identify the service provider. The ID must be unique.
SAML attribute for user ID	The SAML attribute name for the attribute describing the user ID.
SAML attribute for user directory	The SAML attribute name for the attribute describing the user directory.
SAML signing algorithm	The hash algorithm used for signing SAML requests. In order to use SHA-256, a third-party certificate is required, where the associated private key has the provider "Microsoft Enhanced RSA and AES Cryptographic Provider".
JWT attribute for user ID	The JWT attribute name for the attribute describing the user ID.
JWT attribute for user directory	The JWT attribute name for the attribute describing the user directory. If the name value is enclosed in brackets, that value is used as a constant attribute value: [example] gives the constant attribute value 'example'.
Intended audience (aud attribute)	The intended audience is the recipient of the token. The audience value is a string, typically the base address of the resource being accessed, such as https://qlik.com.

SAML single logout	Enable service provider initiated flow for SAML single logout. When enabled, make sure the IdP metadata file includes a logout URI. You also need to regenerate the metadata file and update the IdP configuration.
Disable optional OIDC attributes	Only to be used when syncing users through a user directory connector. When selected, the attributes **name**, **groups**, **email**, and **picture** coming from user directory connector sync are protected from being overwritten by the attributes from the OIDC.
OpenID Connect metadata URI	The URL to the endpoint that provides configuration information for the OAuth clients to interface with the identity provider using the OpenID Connect protocol.
Client ID	ID of the configured client at the identity provider for user authentication.
Realm	Name to associate with the identity provider, used for naming consistency in multi-cloud.
sub	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values. If the subject attribute value format is *domainname\username*, **realm** is optional. If not, **realm** is mandatory.
name	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values.
groups	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values.
email	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values.
client_id	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values.
picture	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values.
scope	Used in the OAuth 2.0 specification to specify the access privileges when issuing an access token. For example, use this option to add a groups scope in case the identity provider requires that to support a user groups feature.
ID	The ID of the virtual proxy.
Created	The date and time when the virtual proxy was created.
Last modified	The date and time when the virtual proxy was last modified.
Modified by	By whom the virtual proxy was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.

⌕▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌕▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
⚲	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.
Edit	Edit the selected virtual proxies.
Delete	Delete the selected virtual proxies.
Download SP metadata	Download user configuration data from the identity provider. The information is available as IdP metadata that users can download and provide the service provider (Qlik Sense) with. The metadata is uploaded from the QMC and stored in the database (VirtualProxyConfig table) as a text field (samlMetadataIdP).
⊕ **Create new**	Create a new virtual proxy.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.

Virtual proxy: associated items

The following associated items are available for virtual proxies.

Proxies

The Qlik Sense Proxy Service (QPS) manages the Qlik Sense authentication, session handling, and load balancing.

Proxy properties

Property	Description
Node	The proxy name.
Status	One of the following statuses is displayed: • **Running** The service is running as per normal. • **Stopped** The service has stopped. • **Disabled** The service has been disabled. Click 🛈 *in the* **Status** *column for more detailed information on the status.* *Checking the status of Qlik Sense services (page 373).*
Service listen port HTTPS (default)	The secure listen port for the proxy, which by default manages all Qlik Sense communication. *Make sure that port 443 is available for the Qlik Sense Proxy Service (QPS) to use because the port is sometimes used by other software, for example, web servers.*
Allow HTTP	Status values: **Yes** or **No**. **Yes**: Unencrypted communication is allowed. This means that both https (secure communication) and (http) unencrypted communication is allowed. *From the February 2019 release, a suffix (-HTTP) is added to the session cookie header name when a user accesses the system over http.*
Service listen port HTTP	The unencrypted listen port, used when HTTP connection is allowed.

Property	Description
Authentication listen port	The listen port for the internal authentication module. ⓘ *When editing this port as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.*
Kerberos authentication	Status values: **Yes** or **No**. **Yes**: Kerberos authentication is enabled.
REST API listen port	The listen port for the proxy API. ⓘ *When editing this port as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.*
SSL browser certificate thumbprint	The thumbprint of the Secure Sockets Layer (SSL) certificate that handles the encryption of traffic from the browser to the proxy. When editing a proxy certificate and the Qlik Sense services run with an account without administrator privileges, you need to configure the private key permissions for the certificate.
Keep-alive timeout (seconds)	The maximum timeout period for a single HTTP/HTTPS request before closing the connection. Protection against denial-of-service attacks. This means that if an ongoing request exceeds this period, Qlik Sense proxy will close the connection. Increase this value if your users work over slow connections and experience closed connections.
Max header size (bytes)	The maximum total header size.
Max header lines	The maximum number of lines in the header.
Audit activity log level	Levels: **Off** or **Basic** (a limited set of entries)
Audit security log level	Levels: **Off** or **Basic** (a limited set of entries)
Service log level	Each level from **Error** to **Info** includes more information than the previous level.
Audit log level	More detailed, user-based messages are saved to this logger, for example, proxy calls. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log level	All the performance messages are saved to this logger. For example, performance counters and number of connections, streams, sessions, tickets, web sockets and load balancing information. Each level from **Fatal** to **Debug** includes more information than the previous level.
Security log level	All the certificates messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.

Property	Description
System log level	All the standard proxy messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log interval (minutes)	The interval of performance logging.
ID	The ID of the proxy.
Created	The date and time when the proxy was created.
Last modified	The date and time when the proxy was last modified.
Modified by	By whom the proxy was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌐▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌐▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Edit	Edit the selected proxy.
Unlink	Unlink a proxy service from the selected proxy. ⓘ *A virtual proxy must be linked to a proxy service in order to work.*
➕ **Link**	Link a proxy service to the selected proxy.
Show more items	The overview shows a set number of items by default. To show more items, scroll to the end of the list and click **Show more items**. Sorting and filtering of items is always done on the full database list of items, not only the items that are displayed.

💡 *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

SameSite cookie attribute

The SameSite cookie attribute is used by browsers to identify how first-party and third-party cookies are to be handled. The purpose of the SameSite attribute is to protect the privacy rights of web users and reduce the risk of cross-site request forgeries (CSRF/XSRF). CSRF is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts.

With the release Chrome 80 the SameSite cookies attribute was turned on by default. Other browsers, such as Microsoft Edge, Firefox, and Safari also support SameSite cookies, but the feature is not always turned on by default.

SameSite attribute values

SameSite has three values for different levels of security:

- Strict: Browsers only send cookies with requests originating from the same domain/site as the target domain. This will stop CSRF attacks.
- Lax: Does not restrict originating site, but enforces target domain to be the same as cookie domain. This will stop cross-site cookies.
- None: Clearly communicates that you intentionally want the cookie sent in a third-party context.

> *Site in this context is the domain suffix and the part of the domain just before it. For the web site https://help.qlik.com, qlik.com counts as the site.*

In Chrome 80 and later, cookies that have no declared SameSite value will default to SameSite=Lax. This means that cookies will automatically be sent only in a first party context unless they opt-out by explicitly setting the value None.

Only cookies with the `SameSite=None; Secure` setting will be available for external access, provided they are being accessed from secure connections.

[Qlik Sense: Missing SameSite attribute now blocks requests in Chrome 80 and future browsers SSL/TLS communication problems after you install KB 931125](#)

Schedulers

The Qlik Sense Scheduler Service (QSS) manages the scheduled tasks (reload of Qlik Sense apps or user synchronization) and task chaining. Depending on the type of Qlik Sense deployment, the QSS runs as manager, worker, or both on a node.

The **Schedulers** overview lists all the available schedulers. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

> *You can adjust the column width by dragging the header border.*

Node properties

Property	Description
Node	The name of the scheduler node.

Status	One of the following statuses is displayed:
	
	• **Running**
	  The service is running as per normal.
	• **Stopped**
	  The service has stopped.
	• **Disabled**
	  The service has been disabled.
	
	> 💡 *Click* ℹ️ *in the **Status** column for more detailed information on the status.*
	
	Checking the status of Qlik Sense services (page 373).

Tags	The tags that are connected to the scheduler.
Type	• **Manager**: sends the task to a worker QSS within the site. • **Worker**: receives the task from the manager QSS and executes the task. • **Manager and worker**: when the manager QSS also acts a worker QSS, on a single node site.
Max concurrent reloads	The maximum number of reloads that the scheduler can perform at the same time.
Engine timeout (minutes)	If the number for **Max concurrent reloads** is reached (a separate property), the request to start a new engine process is queued, waiting for the number of running reload processes to go below **Max concurrent reloads**. If this does not happen within the given time period, the request to start a new engine process is removed from the queue.
Audit activity log level	User-related actions are saved to this logger. Levels: **Off** or **Basic** (a limited set of entries)
Service log level	Each level from **Error** to **Info** includes more information than the previous level.
Application log level	All the application messages for the scheduler service are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Audit log level	Detailed, user-based messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log level	All the performance messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.

Property	Description
Security log level	Security-related messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
System log level	All the standard scheduler messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Task execution log level	All the task execution messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
ID	The ID of the scheduler.
Created	The date and time when the scheduler was created.
Last modified	The date and time when the scheduler was last modified.
Modified by	By whom the scheduler was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⊡▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⊡▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. ⓘ *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↩ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*

Property	Description
↻	Refresh the page.
Edit	Edit the selected scheduler.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

💡 *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

Repositories

The Qlik Sense Repository Service (QRS) manages persistence and synchronization of Qlik Sense apps, licensing, security, and service configuration data. The QRS attaches to a Qlik Sense Repository Database and is needed by all other Qlik Sense services to run and to serve Qlik Sense apps. In addition, the QRS stores the Qlik Sense app structures and the paths to the binary files (that is, the app data stored in the local file system).

The **Repositories** overview lists all the available repositories. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

💡 *You can adjust the column width by dragging the header border.*

Node properties

Property	Details
Node	The name of the repository node.

Status	One of the following statuses is displayed:
	
	• **Running**
	  The service is running as per normal.
	• **Stopped**
	  The service has stopped.
	• **Disabled**
	  The service has been disabled.
	
	💡 *Click ⓘ in the **Status** column for more detailed information on the status.*
	
	Checking the status of Qlik Sense services (page 373).

Property	Details
Audit activity log level	Levels: **Off** or **Basic** (a limited set of entries)
Audit security log level	Levels: **Off** or **Basic** (a limited set of entries)
Service log level	Each level from **Error** to **Info** includes more information than the previous level.
Application log level	All the application messages for the repository service are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Audit log level	Detailed, user-based messages are saved to this logger, for example, security rules information. Each level from **Fatal** to **Debug** includes more information than the previous level.
License log level	All the license messages are saved to this logger. For example, token usage and user access allocation. Levels: **Info** or **Debug**
Qlik Management Console (QMC) log level	All the QMC messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log level	All the performance messages for the repository service are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Security log level	All the certificates messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Synchronization log level	All the synchronization information in a multi-node environment are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
System log level	All the standard repository messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
User management log level	All the user sync messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Tags	The tags that are connected to the repository.
ID	The ID of the repository.
Created	The date and time when the repository was created.
Last modified	The date and time when the repository was last modified.
Modified by	By whom the repository was modified.
\<Custom properties\>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.

Property	Details
⧨	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⧨ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
⊞	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.
Edit	Edit the selected repository.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.

Load balancing rules

The **Load balancing rules** overview lists all the available load balancing rules. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (⊞) to add fields.

You can adjust the column width by dragging the header border.

Load balancing rule properties

Property	Description
Name	Name of the rule. Names for generated rules have the following syntax: [resource type]_[access type]_[resource name]
Description	Description of the rule.
Resource filter	Type of resource that the rule applies to. An asterisk (*****) indicates that the rule applies to all resources.
Actions	Action for the rule (load balancing).
Disabled	Status values: **Yes** or **No**.
Type	Type is **Default** for rules that are created when installing Qlik Sense. If you edit or create a new rule, the type is changed to **Custom**. A third type is **Read only**.
Tags	Tags that are connected to the load balancing rule.
Conditions	Conditions of the load balancing rule.
ID	ID of the load balancing rule.
Created	Date and time when the load balancing rule was created.
Last modified	Date and time when the load balancing rule was last modified.
Modified by	By whom the load balancing rule was modified.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌧	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌧ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.

Property	Description
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
↻	Refresh the page.
Edit	Edit the selected load balancing rule. When you do not have update rights for the selected items, **Edit** is replaced by **View**.
View	View the selected load balancing rule. When you do not have update rights for the selected items, **Edit** is replaced by **View**.
Delete	Delete the selected load balancing rules. If you do not have delete rights for the selected items, **Delete** is disabled.
⊕**Create new**	Create a new load balancing rule.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

> 💡 *Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down Ctrl while clicking the items, or drag over the items.*

Load balancing rules properties

The following property groups are available for load balancing rules.

Resource filter (Advanced view)

Security rule will be applied to a Qlik Sense **App**.

Syntax:

```
resource.resourcetype = "[property name]_*"
```

Examples:

```
resource.resourcetype = "App_*"
```

Conditions (Advanced view)

Define the resource and/or user conditions that the load balancing rule should apply to.

Syntax

```
[resource.resourcetype = "resourcetypevalue"] [OPERATOR]
[(((resource.property = propertyvalue) [OPERATOR (resource.property =
propertyvalue)))]
```

If you select a resource and a resource condition from the drop-down list in the **Basic** view, the **Conditions** field in the **Advanced** view is automatically filled in with corresponding code for the selected resource type.

Conditions are defined using property-value pairs. You are not required to specify resource or user conditions. In fact, you can leave the **Conditions** field empty.

> *If you define a rule without specifying at least one **Resource** or **Node access** condition, your rule will apply to all resources and / or nodes.*

The order that you define conditions does not matter. This means that you can define the resources first and then the user and/or resource conditions or the other way round. However, it is recommended that you are consistent in the order in which you define resources and conditions as this simplifies troubleshooting.

Arguments

Argument descriptions

Argument	Description
resource	Implies that the conditions will be applied to a resource.
resourcetype	Implies that the conditions will be applied to a resource of the type defined by the **resourcetypevalue**. You can also use pre-defined functions for conditions to return property values.
resourcetypevalue	You must provide at least one resource type value, for available values. *Resource filter (Advanced view) (page 174)*
property	The property name for the resource condition, for available names. *Properties (page 175)*
propertyvalue	The value of the selected property name.

Properties

Property descriptions

Property name	Description
name	The name of the resource
owner.environment.browser	The browser environment of the owner of the resource
owner.environment.device	The device environment of the owner of the resource
owner.environment.ip	The IP environment of the owner of the resource
owner.environment.os	The OS environment of the owner of the resource
owner.environment.requesttype	The request type environment of the owner of the resource
owner.group	The group memberships of the owner retrieved from the user directory.

Property name	Description
owner.name	The user name of the owner of the resource
owner.userdirectory	The user directory of the owner of the resource
owner.userid	The user id of the owner of the resource
streams.name	The name of the associated stream

Examples and results

Examples and results

Example	Result
`resource.resourcetype="App" and (resource.name like "*")`	The rule will apply to all apps. *The same rule can be defined by simply setting the **Resource** field to App* and leaving the **Conditions** field empty.*
`resource.resourcetype="App" and (resource.name like "My*")`	The rule will apply to all apps that have names beginning with "My".
`resource.resourcetype="App" and (resource.@Department="Test")`	The rule will apply to all apps with the custom property Department set to Test.
`resource.resourcetype="App" and ! (resource.@Department="Test")`	The rule will apply to all nodes except the nodes with custom property Department set to Test.
With **Resource filter**=* and Conditions field empty	This rule will apply to all resources and all users.

Actions (Basic view)

The load balancing rule action is always defined as **Load balancing**.

Cloud distribution

In the cloud distribution section, you work with setting up and monitoring the distribution of apps from Qlik Sense Enterprise on Windows to Qlik Sense Enterprise SaaS. With such a deployment, apps published to a stream in Qlik Sense Enterprise on Windows can automatically also be distributed to Qlik Sense Enterprise SaaS. To be able to distribute apps to cloud, you must have a license with multi-cloud.

The following sections are available if you have a license with multi-cloud:

- **App distribution status**: Monitor the distribution of apps.
- **Distribution policies**: Determine whether a published app can be distributed to deployments in Qlik Sense Enterprise SaaS. To be distributed, a published app must have a distribution policy connected to

it.

- **Deployment setup**: Configuring a deployment in Qlik Sense Enterprise on Windows.

App distribution status

The **App distribution status** overview lists status of app distributions from Qlik Sense Enterprise on Windows to Qlik Sense Enterprise SaaS. The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

> **App distribution status** *is a subsection of* **Cloud distribution** *and only available if you have a license with multi-cloud.*

App distribution status properties

Property	Description
ID	ID of the app distribution.
Last distribution	Date and time of the last distribution.
App name	Name of the distributed app.
App ID	ID of the distributed app.
Deployment name	Name of the deployment to which the app has been distributed.
Deployment ID	ID of the deployment to which the app has been distributed.
Node	Node from which the app is distributed.
Status	Distribution status, values: **In Progress**, **Queued**, **Success**, **Deleting**, or **Failure**.
Created	Date and time when the app distribution was first distributed to the deployment.

Distribution policies

To be able to distribute apps from Qlik Sense Enterprise on Windows to Qlik Sense Enterprise SaaS, you must define distribution policies. Distribution policies are used to determine whether a published app can be distributed to one or more of the deployments in Qlik Sense Enterprise SaaS. If a published app is not covered by a distribution policy it will not be distributed.

The **Distribution policies** overview lists all the available distribution policies.

> **Distribution policies** *is a subsection of* **Cloud distribution** *and only available if you have a license with multi-cloud.*

The following table presents the available fields and buttons. By default, only some of the fields are displayed. You can use the column selector (▦) to add fields.

You can adjust the column width by dragging the header border.

Policy field descriptions

Field	Description
Name	Name of the policy.
Description	Description of the rule.
Resource filter	Type of resource that the rule applies to. An asterisk (*****) indicates that the rule applies to all resources.
Actions	Action for the rule (Distribute).
Disabled	Status values: **Yes** or **No**.
Type	Type is **Default** for rules that are created when installing Qlik Sense. If you edit or create a new rule, the type is changed to **Custom**. A third type is **Read only**.
Tags	Tags that are connected to the distribution policy.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌃▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌃▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Actions	Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.*
▦	Column selector: Select which columns to display in the overview. Click ↰ to reset to the default columns.
🔍	Search – both basic and more advanced searches. *Searching and filtering in the QMC (page 25)*
⟳	Refresh the page.

Edit	Edit the selected distribution policy. When you do not have update rights for the selected items, **Edit** is replaced by **View**.
View	View the selected distribution policy. When you do not have update rights for the selected items, **Edit** is replaced by **View**.
Delete	Delete the selected distribution policy. If you do not have delete rights for the selected items, **Delete** is disabled.
➕ Create new	Create a new distribution policy.
Show more	The overview shows a set number of items, by default. To show more items, scroll to the end of the list and click **Show more**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

Deployment setup

With a multi-cloud setup, you can deploy to Qlik Sense Enterprise SaaS. Qlik Sense Enterprise SaaS supports deployment on an infrastructure managed by Qlik.

The setup differs depending on whether or not you use a local bearer token.

Setup with a local bearer token

A local bearer token simplifies the deployment setup. Instead of using the token endpoint, client ID, and client secret properties to retrieve a bearer token from the IdP, a bearer token is generated locally.

Before you start setting up your deployment, make sure you have the tenant URL, provided by Qlik in your welcome email.

To set up your deployment:

1. In the bottom left corner, click **Set up new**.
2. Enter a deployment name.
3. **API endpoint**: Enter the tenant URL, which is sent to you from Qlik.
4. Enter audience: `qlik.api`. Audience is needed by the app distribution service to get API tokens from cloud.
5. Ensure that **Use local bearer token** is selected and click **Apply**.
   The local bearer token is generated.
6. By default, the **Qlik Cloud format** check box is selected. The text box then displays the IdP definition.
7. Choose the format you want to use and click **Copy to clipboard** to save the text. You need this text when you configure your tenant.
8. For Qlik Sense Enterprise SaaS, you paste the IdP definition in the **Local bearer token** text box on the tenant configuration page.

Setup with IdP integration

Before you start setting up your deployment, make sure you have the following:

- Client ID and client secret (collected from your IdP provider)
- Token endpoint
- Tenant URL (provided by Qlik in your welcome email)

To set up your deployment:

1. In the bottom left corner, click **Set up new**.
2. Enter a deployment name. (You can use this name in distribution policies for the distribution of apps.)
3. **API endpoint**: Enter the tenant URL, which is sent to you from Qlik.
4. Enter audience: `qlik.api`. Audience is needed by the app distribution service to get API tokens from cloud.
5. Enter Client ID and Client secret.
6. Enter Token endpoint, also known as *Authentication URL*.
7. Click **Apply**.

Certificates

Qlik Sense uses certificates for authentication. A certificate provides trust between nodes within a Qlik Sense site. The certificates are used within a Qlik Sense site to authenticate communication between services that reside on multiple nodes.

If you want to add a third-party tool to your Qlik Sense installation, you need to export the certificates.

You can use the exported certificates to do the following:

- Use an external authentication module.
- Move the certificates manually to a node, instead of using the QMC functionality when creating a new node.

Log collector

With the log collector, you can collect and export log files from a period that you define. The logs facilitate troubleshooting for Qlik Support.

Collected files

The following files are available for collection.

Windows event log

The log collector reads Windows application event logs and only extracts Qlik Sense related events. With these logs, Qlik Support can analyze all Qlik Sense services starts and stops, warnings, and errors.

System information

The log collector uses standard Windows Management Instrumentation (WMI) for collecting information about the local server, current hotfixes, and service packs. The log collector also uses the command line for detecting proxy setups, which services are running, certificate names, and internet settings. This information is useful when troubleshooting connectivity and Windows related problems.

Scriptlog files from Qlik folders

The log collector scans the archived log files. Currently active logs files are scanned from each Qlik Sense server node using a Universal Naming Convention (UNC) path.

Collecting and exporting log files

Do the following:

1. Enter start and end date, manually, or by using the calendar: 🗓️⊙.

   > ℹ️ *Folders that don't contain any logs from the specified time period are not collected.*

2. Enter the support case number.

3. Select which additional logs you want to include:
   - Windows event log
   - System information
   - Scriptlog files from Qlik folders

4. **Ignore log-folder filter and export all**: When selected all logs are collected. When not selected only the following folders are collected:
   ```
   AboutService
   AppDistributionService
   BrokerService
   CapabilityService
   ConnectorRegistryProxy
   ConverterService
   DataProfiling
   DepGraphService
   DeploymentBasedWarningsService
   DownloadPrepService
   Engine
   HubService
   HybridDeploymentService
   HybridSetupConsoleBff
   Licenses
   OdagService
   Printing
   Proxy
   Repository
   ResourceDistributionService
   Scheduler
   WebExtensionService
   ```

   > ℹ️ *Normally, the default log set, without all the logs, is sufficient for troubleshooting by Qlik.*

5. Click **Collect and export logs**.

A zip file is generated that you can send to Qlik Support.

Log collector output

The following are all separate files:

- App list - *https://{senseApiSupport.Host}:4242/qrs/app/full*
- CallInfo - *https://{senseApiSupport.Host}:4242/qrs/license/accesstypeinfo*
- License agent - *https://{senseApiSupport.Host}:4242/qrs/license*
- Proxy service info - *https://{senseApiSupport.Host}:4242/qrs/ProxyService/full*
- Qlik Sense machine info - *https://{senseApiSupport.Host}:4242/qrs/servernodeconfiguration/full*
- Qlik Sense service info - *https://{senseApiSupport.Host}:4242/qrs/servicestatus/full*
- QRS about - *https://{senseApiSupport.Host}:4242/qrs/about*
- Service cluster - *https://{senseApiSupport.Host}:4242/qrs/ServiceCluster/{_serviceClusterId}*

The following files are contained in a configuration folder:

- All installed connectors and their configuration files
- postgresql.conf
- postgresql_pg_hba.conf
- Engine_Settings.ini
- Sense_Host.cfg
- Repository.exe.config
- Repository.Core.dll.config
- Repository.Domain.dll.config
- Repository.Synchronization.dll.config
- Repository.User.dll.config
- Printing.exe.config
- Qlik.Printing.CefSharp.exe.config
- Qlik.Sense.Printing.dll.config
- Scheduler.exe.config
- Proxy.exe.config

Additional logs:

- Current logs folder
- Archived logs - *https://{senseApiSupport.Host}:4242/qrs/ServiceCluster/{_serviceClusterId}*
- System Info - *C:\\Windows\\System32\\systeminfo.exe /S {hostName}*
- Windows logs
- Script logs

Service certificates

Certificates are used for secure communication between two entities, such as a proxy and a browser, or two internal services.

There are two types of certificates in Qlik Sense, server certificates and trust zone certificates:

- Server certificates are used to protect the communication between the Qlik Sense Proxy Service and the Qlik Sense Client running in your browser.

- Trust zone certificates are used to protect the communication between Qlik Sense internal services.

> *The rest of this description will focus on the trust zone certificates and will not cover the server certificates in any further detail.*

Qlik Sense trust zone certificates and keys used for TLS with mutual authentication

The Qlik Sense trust zone is based on Transport Layer Security (TLS) with mutual authentication between the internal services.

To establish TLS with mutual authentication every service needs three certificates and two private keys:

Root certificate

The root certificate is used for verifying the certificate sent by the service you want to talk to.

Windows certificate store location: *Local Computer > Trusted Root Certification Authority*.

Service certificate and service private key

The service certificate and service private key are used for server authentication when your service acts as a server, that is, when another service calls an API in your service.

Windows certificate store location: *Local Computer > Personal > Certificates*.

Client certificate and client private key

The client certificate and client private key are used for client authentication when your service acts as a client, that is, when your service calls an API in another service.

Windows certificate store location: *Local service user > Personal Certificates*.

For services implemented in node.js, copies of the certificates reside in the following folder: *%ProgramData%\Qlik\Sense\...\ExportedCertificates*. In the following example, the service acts as a server.
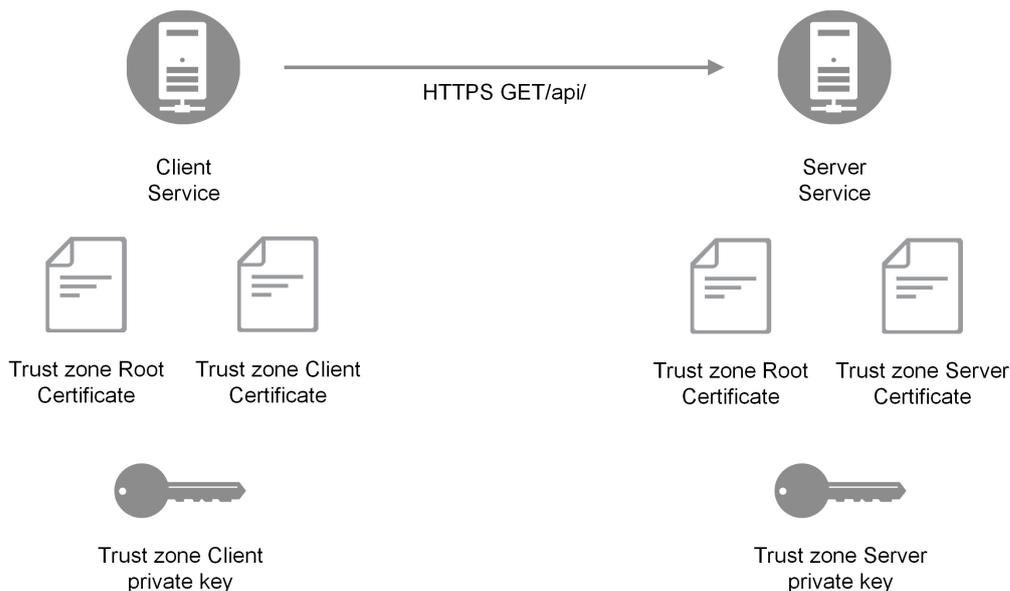
Example where the service acts as a server

The common name of the server certificates will carry the hostname of the server, and it is used by the client to validate that the domain name of the server matches the information in the certificate. In the following example, the client service negotiates TLS with the server *server.domain.com*.
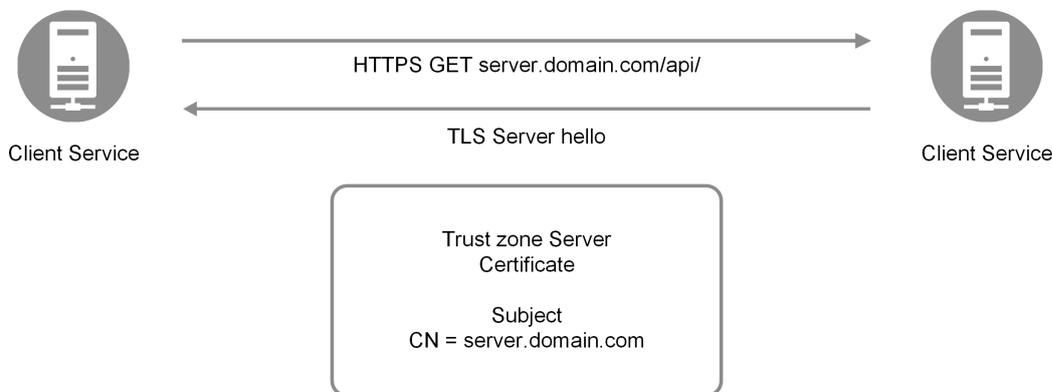
Example where the client service negotiates TLS with the server

The common name of the server certificate is entered by the administrator during the node registration process in the QMC.

QlikServiceCluster certificate

The QlikServiceCluster certificate is used for distributing apps from Qlik Sense Enterprise on Windows to multi-cloud deployments.

Windows certificate store location: *Local Computer > Personal > Certificates*.

Manual configuration

Manual configuration is required when upgrading multi-node sites that are using or will use app distribution.

If upgrading from June 2020 (or earlier) to September 2020 (or later), read more here: FAQ: QlikServiceCluster certificate for distributing apps from Qlik Sense Enterprise on Windows.

Manual configuration is not required in the following cases:

- New deployments of single-node or multi-node sites.
- Upgrade of single-node sites.
- Upgrade of multi-node sites that will not use app distribution.

Configuring the expiry date of Qlik Sense certificates

Qlik Sense offers the ability to configure the expiry date of its certificates. The default value is 5 years (60 months). The minimum value is 12 and the maximum value is 60 months. Any value below the minimum or above the maximum will be ignored and set to the border value—12 or 60 months respectively.

Qlik Sense trust zone key management

Where do all the keys and certificates come from? All node keys and certificates are created by the central node. The keys are randomly generated and the corresponding certificates are signed by the trust zone Root private key. The trust zone Root private key is a third private key used by Qlik Sense. But this key is only used to issue new certificates, it is not involved in establishing mutual TLS. When the central node has generated certificates and keys for a new node, it will encrypt them with a randomly generated password and send them to a REST endpoint in the new node.

An administrator will have to enter the password on the new node so that the keys and certificates can be decrypted and installed on the new node. The password is entered on a web page that is only served on localhost. In practice, all of this happens in the node registration work flow in the QMC.

The certificate and key distribution procedure is described in the following example.
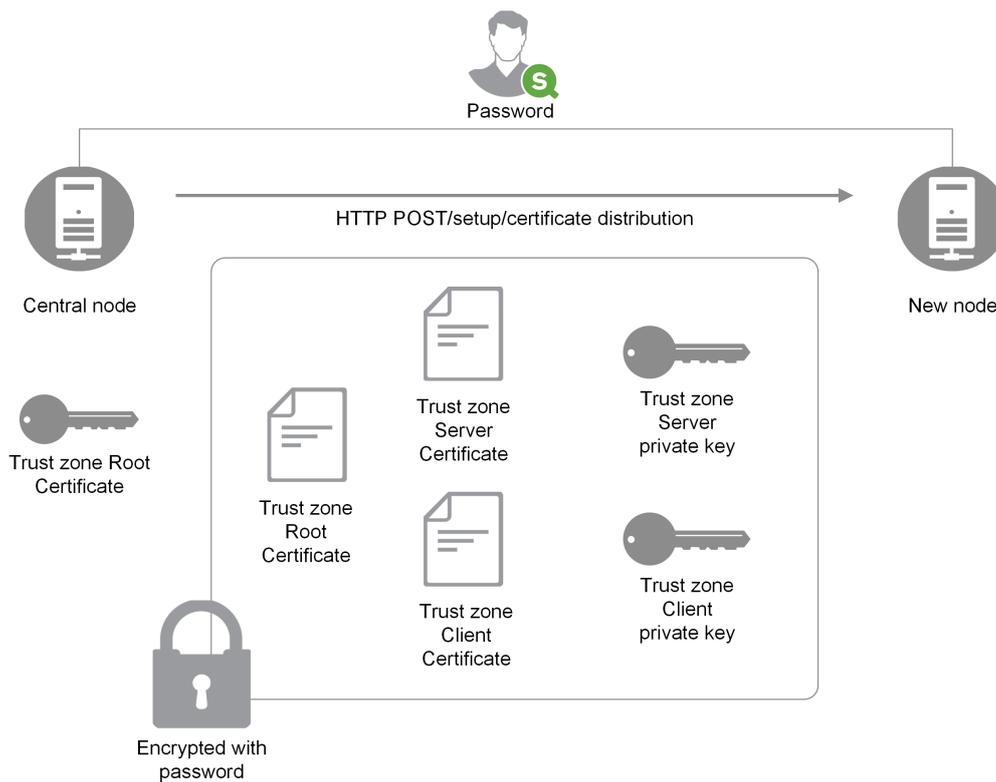
Certificate and key distribution procedure

You use a certificate extension to identify the certificates as Qlik certificates, and the value of this extension defines the role of the certificate as either "root", "service", or "client".

Database encryption

Some fields in the database are encrypted at the application layer by Qlik Sense. This is typically fields that contain credentials, such as passwords for connections. Database fields are encrypted with a symmetric key that must be available on all Qlik Sense nodes and you use the trust zone server certificate to carry the key.

The database encryption algorithm and key are stored in the trust zone server certificate as extensions. Every extension is identified by an object identifier (OID), which indicates the contents of the extension:

- 1.3.6.1.5.5.7.13.1: The symmetrical database key
- 1.3.6.1.5.5.7.13.2: The algorithm of the database key

Both these fields are encrypted with the public key of the trust zone server certificate. This means that it is only the service that can decrypt them since it is the only entity that has access to the trust zone server private key.

Encryption certificates

Encryption keys are best managed through certificates. The certificates must be stored in a certificate store for the user running the Engine service.

The encryption certificate functions as a shell around the encryption key. The key can be fetched even if the certificate has expired, and therefore there is no need to renew an expired encryption certificate.

Encryption keys

The encryption solution uses two types of keys:

- Data encryption keys
- Key encryption keys

Data encryption keys

Data encryption keys (DEK) are auto-generated keys for AES-256 encryption of the data. A new key is generated for each object that is encrypted.

Key encryption keys

Key encryption keys (KEK) are private and public key pair for secure, asymmetric encryption of the data encryption keys. The public key is used to encrypt the data and the private key is used to decrypt the data encrypted by the public key.

> *Only keys using the RSA algorithm are supported.*

The key used for key encryption is specified in the Qlik Management Console (QMC) *Data encryption* section of the *Service cluster* resource, see *Service cluster (page 145)*.

Encryption certificate requirements:

- The certificate key is stored in the Microsoft Cryptography Next Generation (CNG) Key Storage Provider.
- The certificate is stored in the Windows Certificate store under CurrentUser for the user running the Engine service.

Using data encryption

This is the common workflow for using the data encryption feature in Qlik Sense.

1. Create an encryption certificate: *Creating encryption certificates using Windows PowerShell (page 189)*.
2. Enable encryption and specify the key: *Enabling encryption and specifying the key (page 188)*.
3. For multi-node deployments, export the encryption certificate: *Exporting encryption certificates using Windows PowerShell (page 191)*.
4. For multi-node deployments, import the encryption certificate on all nodes: *Importing encryption certificates using Windows PowerShell (page 193)*.

> *Make sure to back up the certificate. You may not be able to open your encrypted app if the certificate is lost. It is your responsibility to safe keep the certificate backup for as long as it is needed.*

Encrypting QVD files shared with QlikView

If you have QVD files used in both QlikView and Qlik Sense Enterprise on Windows, make sure that the same thumbprint is defined for both products.

Enabling encryption and specifying the key

The Qlik associative engine is configured by defining the encryption key thumbprint in QMC. Copy the value of the *Thumbprint* field from the certificate and paste it into the *Encryption key* field in the QMC.

> *The certificate must be stored in a certificate store for the user running the Engine service.*

Do the following:

1. Open the Certificate Manager tool (certmgr.msc).
2. Locate the certificate.
3. Right click the certificate and select **Open**.
4. On the **Details** tab, select the **Thumbprint** field and copy the value.
5. In the QMC, go to **Service cluster** > **Data encryption**.
   Enable one or both of the data encryption options: **QVF encryption** and **QVD encryption**.
   Paste the Thumbprint value into the **Encryption key** field.
   Service cluster (page 145)

Qlik Sense Enterprise on Windows accepts Secure Hash Algorithm 1 (SHA-1) thumbprints in the 40-digit hexadecimal string form without spaces.

Example:

If your certificate thumbprint contain spaces, like `56 38 88 bb 6a ea 55 eb 0d 33 d9 d8 b9 09 e0 d2 ef 26 ff bd`, you enter it in the **Encryption key** field as follows:

`563888bb6aea55eb0d33d9d8b909e0d2ef26ffbd`

> *If your organization has a key rotation policy, you may need to update the thumbprint definition when the key is changed.*
> *Remember to keep the certificate containing the old key on the server until all QVFs and QVDs have been saved with the new key.*

Managing encryption certificates

There are many tools available for managing certificates but this documentation will focus on creating and distributing certificates using Windows PowerShell and Microsoft Management Console.

If other tools are used, the requirements are:

- a RSA key is used
- the key is stored in a CNG KeyStorageProvider

- the certificate is stored in a certificate store for the user running the Engine

Creating encryption certificates using Windows PowerShell

It is not necessary to use certificates issued by a certificate authority (CA), you can also issue and sign your own self-signed certificates. Encryption certificates that you create must be stored in a certificate store for the user running the Engine service.

To create the new encryption certificate, use the **New-SelfSignedCertificate** cmdlet to create a self-signed certificate.

Syntax: Windows Server 2016 and later
```
PS C:\Users\johndoe.ACME> New-SelfSignedCertificate -Subject <Certifcate name> -KeyAlgorithm
RSA -KeyLength <Key length, e.g.4096> -Provider "Microsoft Software Key Storage Provider" -
KeyExportPolicy ExportableEncrypted
-CertStoreLocation "cert:\CurrentUser\My"
```

Syntax: Windows Server 2012 R2
```
PS C:\Users\johndoe.ACME> New-SelfSignedCertificate -DnsName <Certifcate name> -
CertStoreLocation "cert:\CurrentUser\My"
```

New-SelfSignedCertificate cmdlet parameters Windows Server 2016 and later

The following parameters should at minimal be defined when creating the certificate using PowerShell for Windows Server 2016 and later.

> ℹ️ *For complete documentation, see the* ⤷   [Microsoft New-SelfSignedCertificate documentation](#).

-Subject

Specifies the string that appears in the subject of the new certificate. This cmdlet prefixes **CN=** to any value that does not contain an equal sign. For multiple subject relative distinguished names (also known as RDNs), separate each subject relative distinguished name with a comma (,). If the value of the relative distinguished name contains commas, separate each subject relative distinguished name with a semicolon (;).

```
-Subject <Certifcate name>
```

-KeyAlgorithm

Specifies the name of the algorithm that creates the asymmetric keys that are associated with the new certificate. Must be **RSA**.

```
-KeyAlgorithm RSA
```

-KeyLength

Specifies the length, in bits, of the key that is associated with the new certificate.

```
-KeyLength <Key length, e.g.4096>
```

-Provider

Specifies the name of the KSP or CSP that this cmdlet uses to create the certificate. Should be **Microsoft Software Key Storage Provider**.

```
-Provider "Microsoft Software Key Storage Provider"
```

-KeyExportPolicy

Specifies the policy that governs the export of the private key that is associated with the certificate. The acceptable values for this parameter are:

- Exportable
- ExportableEncrypted (default)
- NonExportable

```
-KeyExportPolicy ExportableEncrypted
```

-CertStoreLocation

Specifies the certificate store in which to store the new certificate. If the current path is *Cert:\CurrentUser* or *Cert:\CurrentUser\My*, the default store is **Cert:\CurrentUser\My**. Otherwise, you must specify **Cert:\CurrentUser\My** for this parameter.

```
-CertStoreLocation "cert:\CurrentUser\My"
```

New-SelfSignedCertificate cmdlet parameters Windows Server 2012 R2

The following parameters should at minimal be defined when creating the certificate using PowerShell for Windows Server 2012 R2.

> *For complete documentation, see the* ⤷   [Microsoft New-SelfSignedCertificate documentation](.).

-DnsName

Specifies one or more strings to put into the Subject Alternative Name extension of the certificate. The first DNS name is also saved as Subject Name and Issuer Name.

```
-DnsName <Certifcate name>
```

-CertStoreLocation

Specifies the certificate store in which to store the new certificate. If the current path is *Cert:\CurrentUser* or *Cert:\CurrentUser\My*, the default store is **Cert:\CurrentUser\My**. Otherwise, you must specify **Cert:\CurrentUser\My** for this parameter.

```
-CertStoreLocation "cert:\CurrentUser\My"
```

New-SelfSignedCertificate defaults Windows Server 2012 R2

The following defaults apply for the **New-SelfSignedCertificate** cmdlet in Windows Server 2012 R2:

- Key algorithm: RSA
- Key length: 2048
- Extended key usage (EKU): Client authentication and Server authentication
- Key usage: Digital signature, Key encipherment (a0)
- Validity: one year

Example: creating a data encryption certificate using PowerShell for Windows Server 2016 and later

In this example, the user called test is creating a self-signed exportable encrypted certificate with the subject `MyTestCert` and a key length of `4096` bits. The certificate is to be stored in `Cert:\CurrentUser\My`.

Type the following command in Microsoft PowerShell:

```
PS C:\Users\test> New-SelfSignedCertificate -Subject MyTestCert -KeyAlgorithm RSA -KeyLength
4096 -Provider "Microsoft Software Key Storage Provider" -KeyExportPolicy ExportableEncrypted
-CertStoreLocation "cert:\CurrentUser\My"
```

By default, the certificate expires after one year if the `NotAfter` parameter is not defined. In this example, the certificate expires after three years:

```
PS C:\Users\test> New-SelfSignedCertificate -Subject MyTestCert -KeyAlgorithm RSA -KeyLength
4096 -Provider "Microsoft Software Key Storage Provider" -KeyExportPolicy ExportableEncrypted
-CertStoreLocation "cert:\CurrentUser\My" -NotAfter (Get-Date).AddYears(3)
```

Result:

When the certificate has been created, the following is displayed in Microsoft PowerShell:

```
   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
563888BB6AEA55EB0D33D9D8B909E0D2EF26FFBD  CN=MyTestCert
```

Exporting encryption certificates using Windows PowerShell

To export a encryption certificate, use the **Export-PfxCertificate** cmdlet.

Syntax:
```
PS C:\Users\johndoe.ACME> Export-PfxCertificate -cert cert:\currentuser\My\<certificate
thumbprint> -FilePath <FileName>.pfx -Password <Password or variable>
```

Export-PfxCertificate cmdlet parameters

The following parameters should at minimal be defined when exporting the certificate.

> ℹ️ *For complete documentation, see the* ⤷ [Microsoft Export-PfxCertificate documentation](.)

-cert

Specifies the path to the certificate to be exported.

```
-cert cert:\currentuser\My\<certificate thumbprint>
```

-FilePath

Specifies the path for the PFX file to be exported.

```
-FilePath <FileName>.pfx
```

-Password

Specifies the password used to protect the exported PFX file. The password should be in the form of secure string. This parameter must be specified, or an error will be displayed.

```
-Password <Password or variable>
```

Example: exporting a data encryption certificate

In this example the user called test will export the encryption certificate previously created to a PFX file.

1. First, create a secure string of the plain text password string and store it in the `$mypwd` variable. For this he is using the **ConvertTo-SecureString** cmdlet.
   Type the following command in Microsoft PowerShell:
   ```
   PS C:\Users\test> $mypwd = ConvertTo-SecureString -String "MyPassword" -Force -
   AsPlainText
   ```
2. Then proceed with the actual exporting of the encryption certificate with thumbprint
   `563888bb6aea55eb0d33d9d8b909e0d2ef26ffbd` using the **Export-PfxCertificate**
   cmdlet. The password variable created in the previous step is called to protect the exported PFX file.
   Type the following command in Microsoft PowerShell:
   ```
   PS C:\Users\test> Export-PfxCertificate -cert
   cert:\currentuser\My\563888bb6aea55eb0d33d9d8b909e0d2ef26ffbd -Filepath MyTestCert.pfx -
   Password $mypwd
   ```

Result:

When the certificate has been exported, the following is displayed in Microsoft PowerShell:

```
    Directory: C:\Users\test


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        11/20/2019     11:21           4294 MyTestCert.pfx
```

Backing up encryption certificates using Microsoft Management Console

You should always have a back up of the certificate. If the certificate is lost from the server, or in case of a hard disk failure, you may not be able to open your encrypted app. It is your responsibility to keep safe the certificate backup for as long as it is needed.

You can use the same procedure as for exporting when backing up your certificate, see *Exporting encryption certificates using Windows PowerShell (page 191)*.

Another way of backing up your encryption certificates is to do it with Microsoft Management Console. The below example shows how to export or back up your SSL certificate with a private key using Microsoft Management Console.

Do the following:

1. On the Windows Server where the SSL certificate is installed, open the Microsoft Management Console: type `mmc` in the Windows search menu and open it.

2. In the Console window, click **File > Add/Remove Snap-in**.

3. In the Add or Remove Snap-ins window, select **Certificates** from the Available snap-ins pane on the left side and then click **Add >**.

4. In the dialog, select **My user account** and then click **Next**.

5. In the Add or Remove Snap-ins window, click **OK**.

6. In the Console window, in the Console Root pane on the left side, expand Certificates (Current user) and locate the certificate that you want to export or back up.

7. In the center pane, right-clock on the certificate that you want to export or back up, and then click **All Tasks > Export**.

8. In the Certificate Export Wizard, on the Welcome to the Certificate Export Wizard page, click **Next**.

9. On the Export Private Key page, select **Yes, export the private key**, and then click **Next**.

10. On the Export File Format page, select **Personal Information Exchange – PKCS #12 (.PFX)** and then check **Include all certificates in the certification path if possible**.

    > ⚠️   *Do not select **Delete the private key if the export is successful***.

    Click **Next**.

11. On the Security page, check the **Password** box, then create and confirm the password.

    > ℹ️   *This password will be required when you import or restore the certificate with private key.*

    Then check the **Group or user name** box. If applicable, select the Active Directory user or group account to which you want to assign access to the certificate with private key. Then click **Add**. Click **Next**.

12. On the File to Export page, click **Browse** to specify the save location and the file name of the back up file and then click **Save**.
    Back on the File to Export page, click **Next**.

13. On the Completing the Certificate Export Wizard page, verify that the settings are correct and then click **Finish**.

14. You should receive a message stating that the export was successful, and the SSL certificate with private key is now saved to the location that you selected .

Importing encryption certificates using Windows PowerShell

To import an encryption certificate, for example, on other machines, use the `Import-PfxCertificate` cmdlet.

> ℹ️   *Encryption certificates that you import must be stored in a certificate store for the user running the Engine service*

Syntax:
```
PS C:\Users\johndoe.ACME> Import-PfxCertificate -CertStoreLocation cert:\currentuser\My -
FilePath <FileName>.pfx [-Exportable] -Password $mypwd
```

Import-PfxCertificate cmdlet parameters

The following parameters should at minimal be defined when importing the certificate.

> ℹ️ *For complete documentation, see the* ↪ [Microsoft Import-PfxCertificate documentation](#).

-CertStoreLocation

Specifies the path of the store to which certificates will be imported. If this parameter is not specified, then the current path is used as the destination store.

```
-CertStoreLocation cert:\currentuser\My
```

-FilePath

Specifies the path for the PFX file.

```
-FilePath <FileName>.pfx
```

-Exportable

Optional.

Specifies whether the imported private key can be exported. If this parameter is not specified, then the private key cannot be exported.

```
-Exportable
```

-Password

Specifies the password for the imported PFX file in the form of a secure string.

```
-Password $mypwd
```

Example: importing a data encryption certificate

In this example, the user called test2 will import the encryption certificate with thumbprint `563888BB6AEA55EB0D33D9D8B909E0D2EF26FFBD` previously exported to a PFX file.

1. First, create a secure string of the plain text password string and store it in the `$mypwd` variable. For this, user test2 is using the **ConvertTo-SecureString** cmdlet.
   Type the following command in Microsoft PowerShell:
   ```
   PS C:\Users\test2>  $mypwd = ConvertTo-SecureString -String "MyPassword" -Force -AsPlainText
   ```

2. Then proceed with the actual importing of the PFX file using the **Import-PfxCertificate** cmdlet. The password variable created in the previous step is called to access the PFX file. Type the following commands in Microsoft PowerShell:
   ```
   PS C:\Users\test2>  Import-PfxCertificate -CertStoreLocation cert:\currentuser\My -FilePath MyTestCert.pfx -Exportable -Password $mypwd
   ```

Result:

When the certificate has been exported, the following is displayed in Microsoft PowerShell:

```
PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My
```

```
Thumbprint                                Subject
----------                                -------
563888BB6AEA55EB0D33D9D8B909E0D2EF26FFBD  CN=MyTestCert
```

Restoring encryption certificates using Microsoft Management Console

You can use the same procedure as for importing when restoring your certificate, see *Importing encryption certificates using Windows PowerShell (page 193)*.

If you backed up your certificate using Microsoft Management Console, as described in *Backing up encryption certificates using Microsoft Management Console (page 192)*, then follow the example below to restore your SSL certificate.

> *Encryption certificates that you restore must be stored in a certificate store for the user running the Engine service*

Do the following:

1. On the Windows Server where you want to install the SSL certificate, open the Microsoft Management Console: type `mmc` in the Windows search menu and open it.
2. In the Console window, click **File > Add/Remove Snap-in**.
3. In the Add or Remove Snap-ins window, select **Certificates** from the Available snap-ins pane on the left side and then click **Add >**.
4. In the dialog, select **My user account** and then click **Next**.
5. In the Add or Remove Snap-ins window, click **OK**.
6. In the Console window, in the Console Root pane on the left side, expand Certificates (Current user), right-click on the Personal folder, and then select **All Tasks > Import**.
7. In the Welcome to the Certificate Import Wizard window, click **Next**.
8. On the File to import page, Click **Browse** to locate and select the PFX file that you want to import, and then click **Next**.

   > *Make sure to select All files (*.*) in the file type drop-down of the File Explorer window, as it by default is set to search for X.509 Certificate (*.cert,*.crt) file types only.*

9. On the Private key protection page, type the password that was created when the SSL certificate was exported / backed up.
   Then check the **Mark this key as exportable** box. This means you can back up or export the SSL certificate when needed.
   Then also check the **Include all extended properties** box.
   Click **Next**.
10. On the Certificate Store page, select **Place all certificates in the following store** and then click **Browse**.
    In the Select Certificate Store window, select **Personal** and click **OK**.
    Back on the Certificate Store page, click **Next**.

11. Verify that all settings are correct on the Completing the Certificate Import Wizard page, and then click **Finish**.

12. You should receive a message stating that the import was successful, and the SSL certificate with private key is now saved to the Personal store (folder).

1.6   Managing QMC resources

The administration of a Qlik Sense environment includes managing and handling the following:

- Licenses
- Apps: publishing, duplicating, reloading, importing, deleting
- Streams
- Data connections and extensions
- Users: synchronizing, access types, ownership, admin roles, inactivating, deleting
- Tasks and triggers
- Nodes and services
- Custom properties and tags

> *For some useful tips regarding how to work with the QMC, see QMC performance – best practices (page 444).*

> *For troubleshooting QMC resources, see* Troubleshooting - Managing QMC resources*.*

Managing licenses

Licenses

There are two license models: the serial and control number and the signed license key. These models define the terms of your license and the access types that you can allocate to users. With a signed license key, you need internet access (direct or through a proxy) to access the cloud-based license backend, for user assignments, analytic time consumption, and product activations.

There are two major license types: one based on access types, and one based on tokens.

- Access types licenses are the Professional and Analyzer Users licenses (user-based) and Analyzer Capacity licenses (capacity-based). With a Professional and Analyzer Users license you can allocate professional access and analyzer access. With an Analyzer Capacity license you can allocate analyzer capacity access, where consumption is time based (analyzer time).
- With a Qlik Sense Token license you use tokens to allocate access passes to users. You can allocate user access and login access.

An access type allows users to access the hub and apps within a Qlik Sense Enterprise on Windows site.

> *If you want to set up Qlik Sense Enterprise SaaS, please contact your Qlik representative or Qlik Support to obtain a valid license for the setup.*

For detailed information on Qlik Sense licensing options, see Qlik's legal terms, product terms, and Licensing Service Reference Guide:

- [Qlik Legal Terms](#)
- [Qlik Product Terms](#)
- [Qlik Licensing Service Reference Guide](#)

Access types licenses

Access types licenses grant a predefined number of professional and analyzer access allocations. The distribution of the access types is determined by the license model.

> *The license check for access types licenses (professional and analyzer) occurs when you access the hub. If you access the hub without a license and subsequently are assigned professional or analyzer access, the license check has already occurred, and you will get a "no access pass" error, stopping you from interacting with apps. Log out and log in again for the license to be recognized.*

Professional access

Professional access is allocated to an identified user to allow the user to access streams and apps within a Qlik Sense site. The professional access is intended for users who need access to all features in a Qlik Sense installation. A user with professional access can create, edit, and publish sheets or apps, and make full use of the available features, including administration of a Qlik Sense site.

For Qlik Sense installations licensed with a serial and control number, if you remove professional access allocation from a user, the access type is put in quarantine, if it has been used within the last seven days. If it has not been used within the last seven days, the professional access is released immediately. You can reinstate quarantined professional access, to the same user, within seven days.

The maximum number of parallel user connections for a single user of this type of access pass is five (5).If you use a license with a signed license key, accessing the QMC also counts and adds to the maximum number of parallel sessions, which is five. To avoid unnecessary session consumption, the root admin should not be allocated any type of access.

When a user with the maximum number of parallel user connections ends a connection (for example, by logging out) five minutes must pass before the user can use the access pass to add another connection (for example, by logging in).

> *If you use a license with a signed license key, accessing the QMC also counts and adds to the maximum number of parallel sessions, which is five. To avoid unnecessary session consumption, the root admin should not be allocated any type of access.*

Analyzer access

Analyzer access is allocated to an identified user to allow the user to access streams and apps in the hub. The analyzer access is intended for users who consume sheets and apps created by others. A user with analyzer access cannot create, edit, or publish sheets or apps, but can create and publish stories, bookmarks and snapshots based on data in apps. The user can also create bookmarks, print objects, stories, and sheets, and export data from an object to Excel.

For Qlik Sense installations licensed with a serial and control number, if you remove analyzer access allocation from a user, the access type is put in quarantine, if it has been used within the last seven days. If it has not been used within the last seven days, the analyzer access is released immediately. You can reinstate quarantined analyzer access, to the same user, within seven days.

The maximum number of parallel user connections for a single user of this type of access pass is five (5).When a user with the maximum number of parallel user connections ends a connection (for example, by logging out) five minutes must pass before the user can use the access pass to add another connection (for example, by logging in).

Analyzer capacity access

Analyzer capacity is a consumption-based license type, which is like analyzer access regarding available features. Users can access streams and apps in the hub and consume sheets and apps created by others. Analyzer capacity access allows users to create stories, bookmarks, and snapshots based on data in apps. Creating, editing, or publishing sheets or apps is not possible.

With an analyzer capacity license, you subscribe to analyzer time, a defined number of minutes per month (calendar date). These minutes are shared between users and can be consumed by anyone who is part of the user group, including anonymous users. Consumption is measured in units of six minutes. For each new six-minute period, a unit is consumed.

For more information, see *Analyzer capacity license (page 98)*

Token-based licenses

When you allocate tokens, the number of available tokens is reduced. Each access type costs a certain number of tokens, and if the token balance is zero or insufficient, you cannot allocate more to the access types. You can free up tokens and choose to use the tokens differently. The number of tokens for the Qlik Sense site can be increased or decreased by activating a new license.

User access pass

You allocate user access to an identified user to allow the user to access the streams and the apps within a Qlik Sense site. There is a direct relationship between the access type (user access) and the user. If you deallocate user access from a user, the access type is put in quarantine if it has been used within the last seven days. If it has not been used within the last seven days, the user access is removed and the tokens are released immediately. You can reinstate quarantined user access, to the same user, within seven days. Then the user is given access again without using more tokens.

Summary user access pass:

- Assigned to an identified user.

- Daily access to analyze or create content.

- Unlimited access to streams, apps, and other resources.

- The maximum number of parallel sessions is five.

- 1 token = 1 user access pass.

> *You can have both a user access pass and the possibility to consume login access passes. If you have five active sessions, opening an additional session will consume from your login access passes.*

Login access pass

One token equals a predefined amount of login access passes. The login access allows a user to access streams and apps for a predefined amount of time. This means that a single user may use several login access passes within a day. You create security rules specifying which users the login access is available for.

When you delete a login access (group), tokens are released immediately if the login access contains enough unused login access passes. The number of tokens that are released is dependent on the number of used login access passes. Used login access passes are not released until 28 days after last use. For example: If you allocated tokens giving 1000 login access passes to a group, they cannot use more than 1000 login access passes over 28 days. Also, if 100 login access passes are consumed on day 1, the 100 are available again on day 29. If no access passes are in use then all tokens assigned to the login access instance will be released when it is deleted.

> *App reloads will extend the session and consume access passes also when the app is not actively used. If a browser page is open with an app, app reloads will result in additional access pass consumption.*

Summary login access pass:

- Intended for infrequent users.

- Usage of Qlik Sense can be customized and limited.

- Time limit of 60 consecutive minutes per pass.
  When a session is closed after 20 min, and analysis is resumed after 4 hours, a new login access pass is used.

- Passes are released every 28 days.

- 1 token = 10 login access passes.

Activating the license

The first time you start the QMC, the **Site license properties** page is displayed. All fields are empty and you must enter the license information. Entering the license information makes you the root administrator (RootAdmin) for the Qlik Sense site.

You can license Qlik Sense Enterprise using a serial and control number or a signed key. You must use a license with a signed key if you are licensing analyzer capacity access.

> After changing to a license with a signed key, you cannot return to using the old serial and control number license model. To learn more about the product licenses, see Qlik product licenses.

Do the following:

1. If licensing Qlik Sense using a control and serial number, fill out the mandatory fields.
   a. Enter the following:

      The property group **Site license** contains properties related to the license for the Qlik Sense system. All fields are mandatory and must not be empty.

      Site licence properties

Property name	Description
Owner name	The user name of the Qlik Sense product owner.
Owner organization	The name of the organization that the Qlik Sense product owner is a member of.
Serial number	The serial number assigned to the Qlik Sense software.
Control number	The control number assigned to the Qlik Sense software.
LEF access	The License Enabler File (LEF) assigned to the Qlik Sense software.

   b. Expand **LEF access** and click **Get LEF and preview the license** to download a LEF file from the Qlik Sense LEF server. Alternatively, copy the LEF information from a LEF file and paste it in the text field.
      LEF was successfully retrieved is displayed.

      > **Failed to get LEF from server** is displayed if the serial number or control number is incorrect.

2. If licensing Qlik Sense using a signed key, enter the signed key in the dedicated field.
3. Click **Apply** in the action bar to apply and save your changes.
   Successfully licensed is displayed.

   > With a signed license key, license information can be viewed in the QMC after the license key is entered and saved using **Apply**.

4. Click **Close**.

You have now activated the license. Next you need to allocate professional access or user access to yourself.

> *You give users access to Qlik Sense by managing the access types: professional or analyzer access (user-based license) or user access or login access (token-based license), according to which consumption model you prefer for accessing Qlik Sense.*

> *With a signed license key, click **Refresh license definition** to synchronize the license definition in QMC with new updates to the license.*

Activating the license offline

To activate the product license, you must connect to the Qlik License Backend Server over the internet. In some cases, you may not have immediate access to the internet and require offline license activation. Depending on your license, offline licensing or temporary product activation is possible.

If you have a product serial and control number, you can request your License Enabler File (LEF) from Qlik Support, which you can then paste into the **Site license properties** page. For detailed instructions on how to obtain your LEF from Qlik Support, see [How to request a control number and LEF](#).

If you have a signed license key, you can only license your product over the internet. However, you can request a Signed License Definition from Qlik Support, which allows you to operate the product for a limited time before licensing your product online. For detailed instructions, see [Activate Qlik Products without Internet access - April 2020 and onwards](#).

Getting to know the license usage summary page

Depending on what type of license you have, the **License usage summary** page looks different.

User-based license

The **License usage summary** overview shows the access availability, and the distribution of the two access types: professional access and analyzer access. You cannot adjust the total number of users of professional and analyzer access from this page, that is determined by the license for the Qlik Sense site.

Analyzer capacity is a variant of analyzer access where you subscribe to analyzer time and consume units in six-minute blocks. When using that license, the overview will display total time and used time. For more information about analyzer capacity, see *Analyzer capacity license (page 98)*.
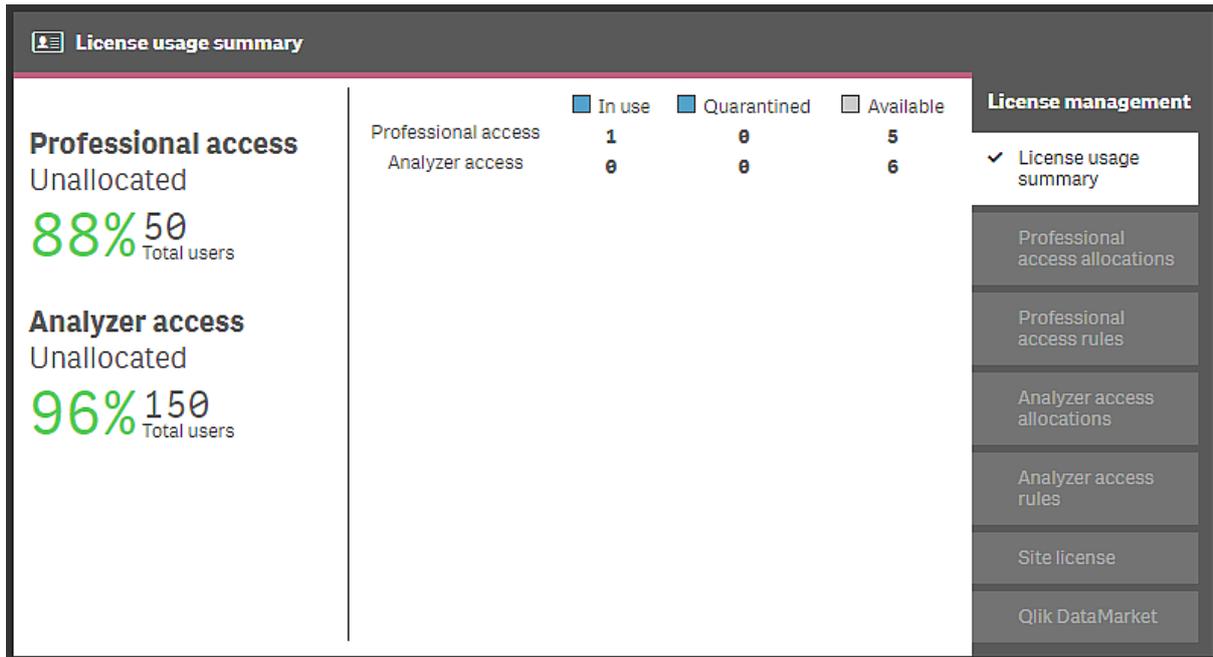
The section to the left shows the percentage of unallocated professional and analyzer accesses and the total number of access users.

The section to the right shows the access distribution:

- **Professional access**: the number of professional access allocations to identified users.
- **Analyzer access**: the number of analyzer access allocations to identified users.

Status

- **In use**: the number of access allocations that are currently in use.
- **Quarantined** (only for licenses with serial and control number): the number of access allocations that will be released when the quarantine period is over.
- **Available**: the number of access allocations that are currently not in use.

Token-based license

The **License usage summary** overview shows the token availability and how the tokens are distributed between the different access types. You cannot adjust the token usage from this page. The number of tokens is determined by the license for the Qlik Sense site.
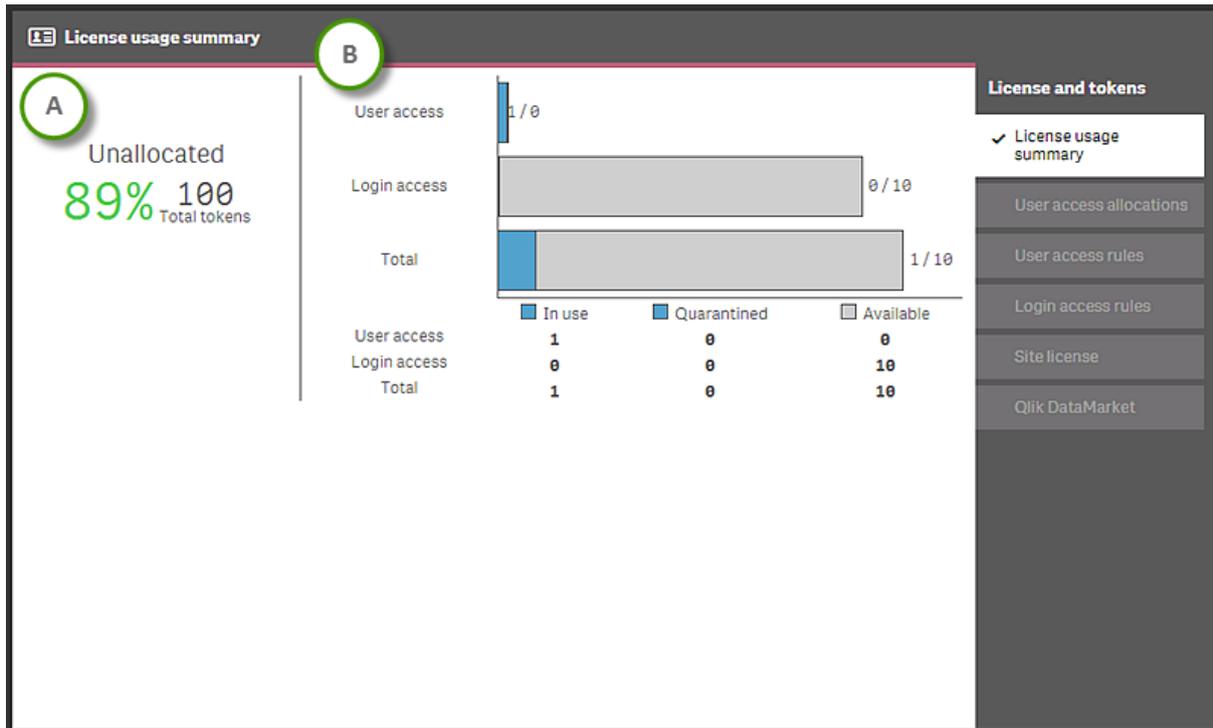
Section (A) shows the proportion of unallocated tokens (in percent) and the total number of tokens.

Section (B) shows the access distribution:

- **User access**: the number of tokens that are allocated to identified users.
- **Login access**: the number of tokens that are allocated to login access groups.
- **Total**: the sum of the above.

Status

- **In use**: the number of allocated tokens that are currently in use.
- **Quarantined**: the number of tokens that will be released when the quarantine period is over.
- **Available**: the number of allocated tokens that are currently not in use.

> *One token is used when a user with allocated user access makes the first login to the hub. One token is used when the first login access pass in a batch of login access passes is used. For example, if you have allocated 3 tokens to login access, providing for 30 login access passes and 11 login access passes are in use, **In use** displays 2 (tokens). Tokens allocated to user access in quarantine are in use until the quarantine period (seven days) is over. A used login access pass is released 28 days after last use.*

Changing the license

The license properties can be changed after they have been set for the first time.

Changing a LEF license

Updating the LEF does the following:

- User-based license: Changes the number of professional and analyzer access allocations for the Qlik Sense site.
- Token-based license: Changes the number of tokens for the Qlik Sense site. You use the tokens on access types to give the users access to the hub.

> *In addition to the site license accepting licenses with serial and control number, there is also the license with a signed key. You must use a license with a signed key if you are licensing analyzer capacity access. Please note that after changing to a license with a signed key, you cannot return to using the old serial and control number license model.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select **Site license** in the panel to the right.
4. Edit the fields.

   The property group **Site license** contains properties related to the license for the Qlik Sense system. All fields are mandatory and must not be empty.

   Site licence properties

Property name	Description
Owner name	The user name of the Qlik Sense product owner.
Owner organization	The name of the organization that the Qlik Sense product owner is a member of.
Serial number	The serial number assigned to the Qlik Sense software.
Control number	The control number assigned to the Qlik Sense software.
LEF access	The License Enabler File (LEF) assigned to the Qlik Sense software.

   Expand **LEF access** and click **Get LEF and preview the license** to download a LEF file from the Qlik Sense LEF server. Alternatively, copy the LEF information from a LEF file and paste it in the text field.

   LEF was successfully retrieved is displayed.

   > *Failed to get LEF from server is displayed if the serial number or control number is incorrect.*

5. Click **Apply** in the action bar to apply and save your changes.
   Changes have been applied is displayed.

   > *Failed to apply changes is displayed if any value is incorrect.*

Updating a signed key license

Updating a signed key license changes the number of professional and analyzer access allocations, and number of minutes for the analyzer capacity license.

1. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
2. Select **Site license** in the panel to the right.
3. Insert a new signed key in the dedicated field.
4. Click **Apply** in the action bar to apply and save your changes.
   Changes have been applied is displayed.

> ⓘ   *Failed to apply changes is displayed if any value is incorrect.*

Refreshing the license definition

With a signed license key, refresh the license definition to manually update the license properties in QMC when there has been a change to the license. Only the RootAdmin and DeploymentAdmin roles can refresh the license definition. You cannot refresh the license definition while editing the signed license key in QMC or if the signed license key has expired.

Do the following:

1. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
2. Select **Site license** in the panel to the right.
3. Click **Refresh license definition** in the action bar to synchronize any changes to the license with the license definition in QMC.
   The **License definition updated** field shows the timestamp when was the license definition was last updated. The timestamp might take up to 10 minutes to reflect a change. This is because the Qlik Sense Repository Service only polls the License Backend Server (LBS) for the latest license definition every 10 minutes. For example, if you manually refresh the license definition at 9 PM, and the next QRS poll is at 9:09 PM, the timestamp will be updated only at 9:09 PM.

Managing apps

You can create and publish apps to streams from the Qlik Sense hub, if you have the appropriate access rights. Apps can also be published from the QMC. To publish an app that is created in a Qlik Sense Desktop installation, you must first import it from the QMC. The security rules applied to the app, stream, or user, determine who can access the content and what the user is allowed to do. The app is locked when published. Content can be added to a published app through the Qlik Sense hub in a server deployment, but content that was published with the original app cannot be edited. To publish an app to Qlik Sense Enterprise SaaS, you must first create distribution policies, see *Distribution policies - introduction (page 617)*

> ⚠   *App extensions are not supported in Qlik Sense Enterprise SaaS. If you publish an app with an extension to a Qlik Sense Enterprise SaaS deployment, the extension will not be available there.*

You can only publish apps that are unpublished:

- To publish an app to more than one stream, you must first create a duplicate of the app.
- To republish an app, create a duplicate of the published app, edit the duplicate and publish it. Use the option **Replace existing app** to replace a published app. You can also import an exported app and replace the existing app with it.

If you publish an app from the hub, the app in the owner's **Work** folder will get a stream icon to indicate that it has been published. If you want to publish the app again, you must first make a duplicate of the published app.

> *You can duplicate an app if you have create and read access to the app and read access to the **Apps** section in the QMC. However, for security reasons, the script will only be duplicated if you also have read rights to the script. Access to the script enables editing or removal of section access, and, as a consequence, a possibility to load data that should not be accessible.*

When importing an app that is created in a local installation of Qlik Sense, the data connection storage can differ between the environment where the app is created and the server environment. If so, the data connection properties **Name** and **Connection string** must be updated to match the server environment. Before publishing the app, check the app in your **Work** section in the hub.

> *If the name of a data connection in the imported app is the same as the name of an existing data connection, the data connection will not be imported. This means that the imported app will use the existing data connection with an identical name, not the data connection in the imported app.*

Workflow: Apps developed on a Qlik Sense Desktop installation

The following workflow illustrates importing an app created from the hub in a Qlik Sense Desktop installation and publishing the app using the QMC in a Qlik Sense installation:
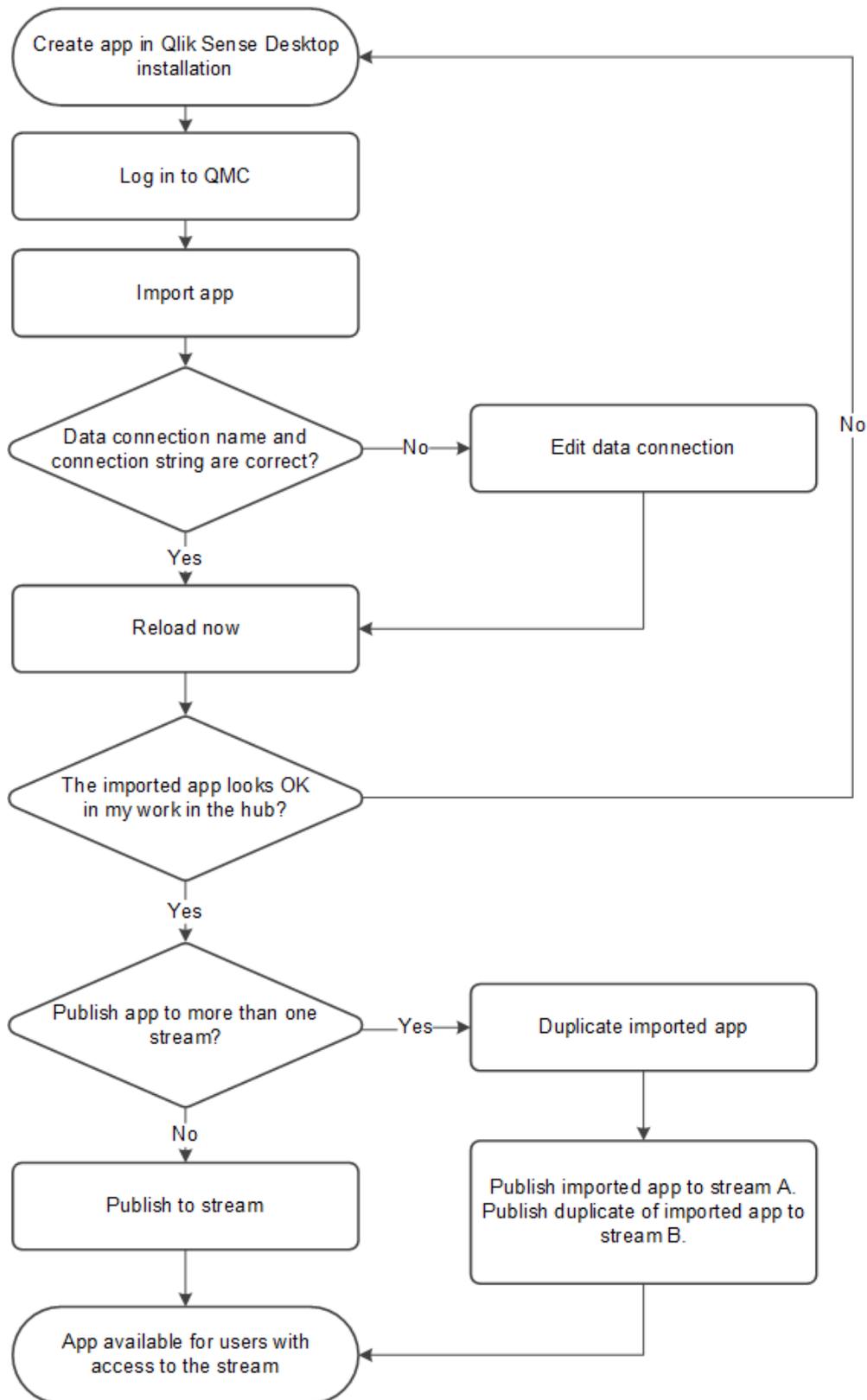
Workflow: Apps developed on Qlik Sense in a server deployment

The following workflow illustrates publishing an app from the QMC in a Qlik Sense installation:
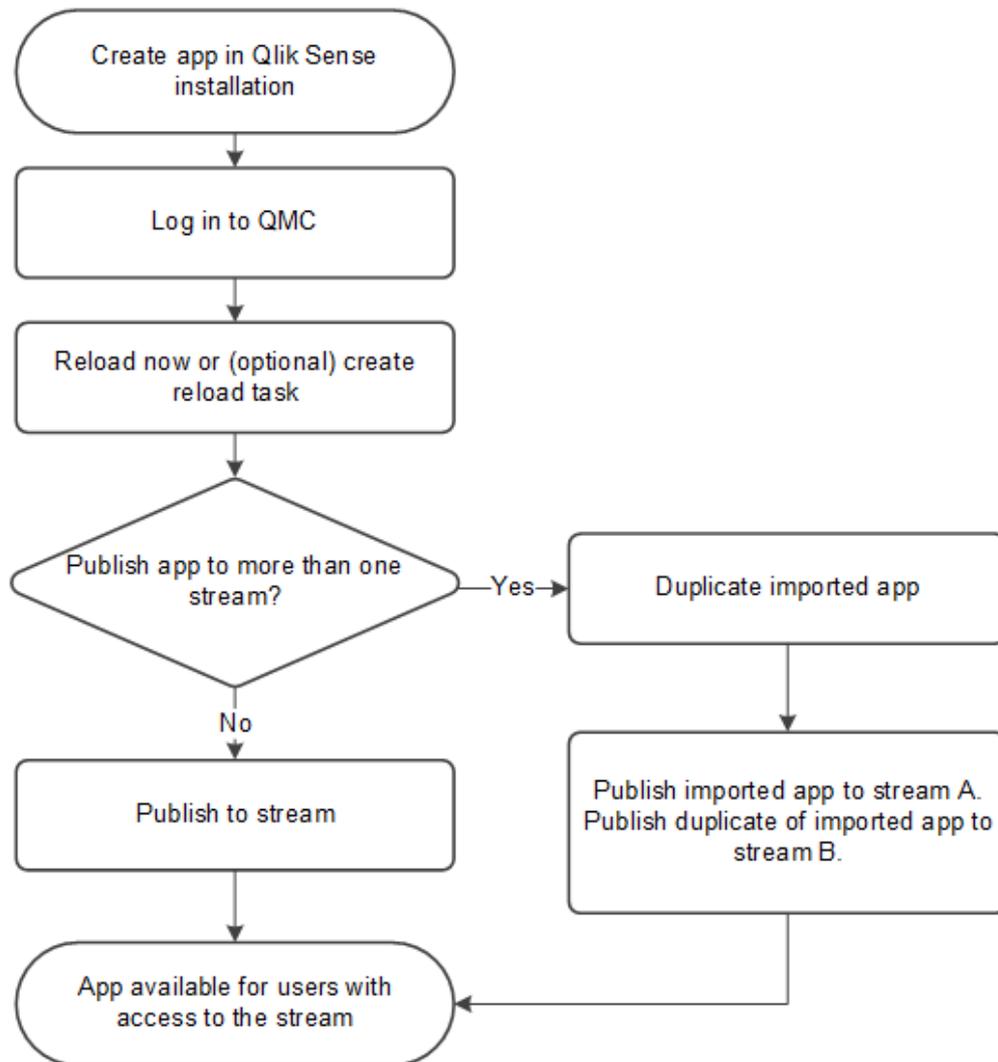
Importing apps

You can import an app if your browser supports HTML5 upload. App properties, such as custom attributes, are included when an app is uploaded.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Click ➕**Import** in the action bar.
   The **Import app** dialog opens.

4. Select a file to import.

5. Browse to the app (*qvf file*) you want to import and click **Open**.

   > *If the app includes an image with a long file name, so that the full path to the image is longer than 260 characters, the import will fail. Reduce the image file name if the path is too long.*

The browse dialog closes and the name of the qvf file is displayed in the **App name** field in the **Import app** dialog.

You can change the name of the app in the **App name** field. If the **App name** is not unique, a message is displayed with information on how many apps that already have this name.

> *If the name of a data connection in the imported app is the same as the name of an existing data connection, the data connection will not be imported. This means that the imported app will use the existing data connection with an identical name, not the data connection in the imported app.*

6. If you want to replace an app, select **Replace existing app**, select an app to replace, and optionally choose to import the app without data.
   For more information about replacing apps, see *Replacing apps (page 213)*.

7. Click **Import** in the dialog.
   The **Ongoing transports** dialog opens. Any other transports you have initiated are also displayed in the dialog.

   - A spinner is displayed during the file import.

   - Click ✖ to cancel the import.
     ⚠ and **Aborted** are displayed and the import stops.

   - Click **OK** to remove a failed item ⚠.
     The item is removed from the **Ongoing transports** dialog.

When the app is imported, ✔ is displayed and the app is added to the **Apps** overview. When all your transports have finished successfully, the **Ongoing transports** dialog closes. If there are any failed transports, the dialog is displayed until the overview page is refreshed.

> *When importing an app to a server, or exporting an app from a server, related content that is not stored in the .qvf file, such as images, is also moved. The related content is stored in a separate folder: %ProgramData%\Qlik\Sense\Repository\AppContent\<App ID>. Each app has its own app content folder, with the app ID as the folder name.*

> *Because of how the synchronization of data works in multi-node sites, apps containing images may display broken thumbnails or images inside the apps if opened right after being duplicated or imported. The broken images are restored when the synchronization is complete. To check if the images have been restored, refresh the browser window.*

Moving apps with ODBC data connections

When you move an app between Qlik Sense sites or Qlik Sense Desktop installations, data connections are not included. If the app contains ODBC data connections, you must create new connections, or use the ones that already exist at the new site. You also need to make sure that the related ODBC data sources exist on the new deployment. The ODBC data sources need to be named and configured identically, and point to the same databases or files.

Editing apps

You can edit apps that you have update rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the apps that you want to edit.
   You can also select apps from stream associations.
4. Click **Edit** in the action bar.The number next to **Edit** indicates the number of items in your selection that you are allowed to edit.
   The **App edit** page opens.
5. Edit the properties.

Identification

Identification properties

Property	Description
Name	The name of the app.
Owner	The owner of the app.
Created	The date and time that the app was created.
Last modified	The date and time that the app was last modified.
File size (MB)	The file size of the app.

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

*If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

   Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.
6. Click **Apply** in the action bar.

Successfully updated is displayed at the bottom of the page.

Deleting apps

You can delete apps that you have delete rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the apps that you want to delete.

4. Click **Delete** in the action bar.A **Delete** dialog is displayed.

5. Click **OK**.

> *When an app is deleted, the content in the app specific folder*
> *%ProgramData%\Qlik\Sense\Repository\AppContent\<App ID> is deleted along with the app.*
> *Generic content that is not specific to a single app, such as extensions, data connections, and items*
> *in **Content libraries**, is not deleted.*

Publishing apps from the QMC

You can create and publish apps to streams from the Qlik Sense hub, if you have the appropriate access rights. Apps can also be published from the QMC. To publish an app that is created in a Qlik Sense Desktop installation, you must first import it from the QMC. The security rules applied to the app, stream, or user, determine who can access the content and what the user is allowed to do. The app is locked when published. Content can be added to a published app through the Qlik Sense hub in a server deployment, but content that was published with the original app cannot be edited.

When you publish an app from the QMC, the owner's app is moved from the **Work** folder to the **Published** folder and is marked with a stream icon (≋) to indicate that it has been published.

- To publish an app to more than one stream, you must first create a duplicate of the app.
- To republish an app, create a duplicate of the published app, edit the duplicate and publish it. Use the option **Replace existing app** to replace a published app.

To publish an app to Qlik Sense Enterprise SaaS, you must first create distribution policies, see *Distribution policies - introduction (page 617)*

> ⚠ *App extensions are not supported in Qlik Sense Enterprise SaaS. If you publish an app with an*
> *extension to a Qlik Sense Enterprise SaaS deployment, the extension will not be available there.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the apps that you want to publish.
   The number next to **Publish** indicates the number of apps in your selection that you are allowed to publish.

4. Click **Publish** in the action bar.

> ℹ️ *The **Publish** button is not displayed if you do not have access to any streams.*

A dialog window opens.

5. In the **Publish app** dialog, do the following:

   a. Use the **Select a stream...** drop-down menu to select the stream that you want to publish to.

   b. In the **Name** text field, you can change the name of the app that you are about to publish. If **Multiple values** is displayed, you are publishing more than one app and you cannot change their names.

6. Optional: You can replace an already published app. This is only possible if you have selected a single app.

   a. Select **Replace existing app**.

   b. Click the **App to replace** box.

A dialog opens.

   c. Double-click the published app you want to replace.
The app is added to the **App to replace** field.

7. Click **OK** to publish. If you are replacing an already published app, click **Publish and replace** in the confirmation dialog that opens.
The dialog closes and **Successfully published selected app(s): x** is displayed, where x represents the number of apps that you just published. Also, the **Stream** column in the apps overview is updated to show the stream that the apps were published to and the published date is shown in the **Published** column.

Republishing apps

To republish an app that has been published from the QMC, you must create a duplicate of the app.

If you publish an app from the hub, the app in the owner's **Work** folder will get a stream icon to indicate that it has been published. If you want to publish the app again, you must first make a duplicate of the published app.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the published app you want to republish and click **Duplicate** in the action bar.
A duplicate of the app is added to the overview.

The duplicated app can now be edited and published. Use the option **Replace existing app** to replace a published app.

Moving published apps between streams in QMC

You can move published apps between streams from the Qlik Sense hub, if you have the appropriate access rights. You can also move apps between streams in QMC if you have:

- Read, update, and publish access rights for the apps.
- Publish access rights on their current stream.
- Publish access rights to the destination streams.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the apps you want to move to a new stream.

4. Click **Move**.

5. Select a destination stream and click **OK**.

The apps are now in the selected stream.

Replacing apps

You can choose to replace an app either by republishing the app or by importing and replacing an app.

You can choose to replace a published app when you publish an app from the QMC. When you have clicked **Publish** in the action bar, the option **Replace existing app** is available in the **Publish app** window.

When you publish an app from the QMC, the owner's app is moved from the **Work** folder to the **Published** folder and is marked with a stream icon (≋) to indicate that it has been published.

When you replace an app by importing an app, you can replace the whole app or import without the data. If you import without the app data, you replace everything in the app but the data and data model. Replacing an app with an imported app requires the following access rights:

- **Update** on the app to be replaced.
- If the app is published, **Publish** on the app to be replaced and **Publish** on the stream to which the app has been published.

Replacing an app with an imported file

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Click ⊕**Import** in the action bar.
   The **Import app** dialog opens.
4. Select a file to import.
5. Browse to the app (*qvf file*) you want to import and click **Open**.

   > ℹ️ *If the app includes an image with a long file name, so that the full path to the image is longer than 260 characters, the import will fail. Reduce the image file name if the path is too long.*

   The browse dialog closes and the name of the qvf file is displayed in the **App name** field in the **Import app** dialog.
   You can change the name of the app in the **App name** field. If the **App name** is not unique, a message is displayed with information on how many apps that already have this name.

   > ℹ️ *If the name of a data connection in the imported app is the same as the name of an existing data connection, the data connection will not be imported. This means that the imported app will use the existing data connection with an identical name, not the data connection in the imported app.*

6. Select **Replace existing app**.
7. Click **App to replace** and select the app.
8. If you want to import without data, select **Import without data**. Only visualizations will be replaced.
9. Click **Import** in the dialog.
   The **Ongoing transports** dialog opens. Any other transports you have initiated are also displayed in the dialog.

- A spinner is displayed during the file import.
- Click ✖ to cancel the import.

  ⚠️and **Aborted** are displayed and the import stops.

- Click **OK** to remove a failed item ⚠️.

  The item is removed from the **Ongoing transports** dialog.

When the app is replaced, ✔ is displayed and the app is added to the **Apps** overview. When all your transports have finished successfully, the **Ongoing transports** dialog closes. If there are any failed transports, the dialog is displayed until the overview page is refreshed.

> ℹ️ *When importing an app to a server, or exporting an app from a server, related content that is not stored in the .qvf file, such as images, is also moved. The related content is stored in a separate folder: %ProgramData%\Qlik\Sense\Repository\AppContent\<App ID>. Each app has its own app content folder, with the app ID as the folder name.*

Replacing the app content folder

App content that is not stored in the .qvf file, such as images, is stored separately in a folder: *%ProgramData%\Qlik\Sense\Repository\AppContent\<App ID>*. Each app has its own app content folder, with the app ID as the folder name.

- Existing files are kept.
- New files are added.
- New files replace existing ones with the same name.

Exporting apps

You can export apps. For example, you might want to use the app in a local version of Qlik Sense, or export the app to another Qlik Sense site. For an unpublished app, all content is exported. For a published app, only published and approved content that is part of the .qvf file is included in the export. The exported app is saved in the default download folder of your web browser.

When you export an app, you can optionally export the app without any data. When importing an app without data, you can replace apps with sheets and stories without impacting the data or data model.

> ℹ️ *When you export an app, extensions are not included in the export. This may result in some visualizations not being rendered when moving apps between different instances of Qlik Sense. The extensions can be obtained from the shared folder given during the installation, for example: \\<domain>\QlikShare\StaticContent\Extensions.*

> ℹ️ *The app file size displayed in the QMC differs from the file size on disk. This is because the size in the QMC only includes data objects, such as fields, tables, and document properties, and not visualizations, bookmarks, measures, etc, that are also included in the .qvf file.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the app that you want to export.

4. Click **More actions** in the action bar.
   A pop-up menu opens.

5. Click **Export**.

6. To export the app without data, clear **Export app with data**.

7. Click **Export**.
   The **Ongoing transports** dialog opens. Any other transports initiated by you are also displayed in the dialog.
   There is a maximum limit for simultaneous transports, and if the maximum is reached an error message is displayed.

   - A spinner is displayed during the file export. When the file export is complete, ✔ is displayed and the browser automatically starts to download the app to the default download folder of your web browser.

     > ⚠ *Do not close or log out from the QMC before the export and the download has finished – if you do the export cannot be completed and the app (qvf file) is lost.*

   - Click ✖ to cancel the export.
     ⚠ and **Aborted** are displayed and the export stops.

   - Click **OK** to remove a failed item ⚠.
     The item is removed from the **Ongoing transports** dialog.

   When the export and file download have finished, ✔ is displayed. When all your transports have finished successfully, the **Ongoing transports** dialog closes. If there are any failed transports, the dialog is displayed until the overview page is refreshed.

   > ℹ *When importing an app to a server, or exporting an app from a server, related content that is not stored in the .qvf file, such as images, is also moved. The related content is stored in a separate folder: %ProgramData%\Qlik\Sense\Repository\AppContent\<App ID>. Each app has its own app content folder, with the app ID as the folder name.*

Moving apps with ODBC data connections

When you move an app between Qlik Sense sites or Qlik Sense Desktop installations, data connections are not included. If the app contains ODBC data connections, you must create new connections, or use the ones that already exist at the new site. You also need to make sure that the related ODBC data sources exist on the new deployment. The ODBC data sources need to be named and configured identically, and point to the same databases or files.

Duplicating apps

When you duplicate an app, the duplicate includes all the content that you have reading rights to. For published apps, only published and approved content that is part of the .qvf file will be included in the duplicate.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the app that you want to duplicate.

   > *When duplicating an app, the folder that stores app related content not included in the .qvf file, such as images, is also duplicated. The path to the folder is %ProgramData%\Qlik\Sense\Repository\AppContent\<App ID>. Each app has its own app content folder, with the app ID as the folder name.*

4. Click **More actions** in the action bar and select **Duplicate** in the pop-up menu.

Successfully duplicated app is displayed and a duplicate of the app is added in the **Apps** overview table.

> *You can duplicate an app if you have create and read access to the app and read access to the **Apps** section in the QMC. However, for security reasons, the script will only be duplicated if you also have read rights to the script. Access to the script enables editing or removal of section access, and, as a consequence, a possibility to load data that should not be accessible.*

Creating reload tasks

You can create a reload task for an app from the apps overview page.

The creation of a new reload task can be initiated in more than one way:
- From the apps overview page
- From the **Associated items** on the **App edit** page
- From the tasks overview page
- From the hub by users with the appropriate permissions

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the app that you want to create a task for, click **More actions** in the far right of the action bar and select **Create new reload task** in the pop-up menu.
   Alternatively:

   a. Select the app that you want to create a reload task for and click **Edit** in the action bar.

   b. Select **Tasks** under **Associated items**.

    c. Click ➕ **Reload task** in the action bar on the tasks page.

Either way the **Edit reload task** page is displayed.

4. Edit the properties.

    a. You can change the task name in the **Name** field. By default the name is *Reload task of <App name >*.

    b. **App** displays the app that you selected from the overview. You can change which app you are creating the task for by clicking the **App** field. In the dialog that opens, double-click the app that you want this task to reload.

    c. You can change the **Execution** properties, see descriptions below. The task is **Enabled** ✔ by default. Clear the selection to disable the task.

    d. A task must have at least one trigger to be executed automatically. Manage the triggers by clicking **Actions▼** in the **Triggers** table heading and selecting one of the following:

- **Create new once-only trigger**, **Create new hourly trigger**, **Create new daily trigger**, **Create new weekly trigger**, or **Create new monthly trigger**. These are trigger shortcuts and the trigger that you select is added to the table instantly. The start value for the trigger is set to 5 minutes from when it was created and the trigger is enabled.

- **Create new scheduled trigger** or **Create new task event trigger** to create a new trigger of the selected type (see the property descriptions below). A dialog opens. Edit the trigger and click **OK** to close the dialog and add the trigger to the table.

- **Edit** if you want to open the edit dialog for the trigger that is selected in the table. Edit the trigger and click **OK** to close the dialog and save your changes.

- **Delete** if you want to delete the trigger that is selected in the table.

Clicking undo (↰) in the **Triggers** heading applies to all triggers you are currently editing.

    e. Optionally, apply tags.

    f. Optionally, apply custom properties.

Identification

All fields are mandatory and must not be empty.

Identification properties

Property	Description	Default value
Name	The name of the task.	Reload task of <App name>
App	The name of the app that the task is created for. Click in the field to open a dialog where you can select (by double-clicking) which app the task reloads.	<App name>

Execution

Execution properties

Property	Description	Default value
Enabled	The task is enabled when selected.	Selected
Partial reload	With partial reload, you can add new data without reloading all the existing tables in the data model. In a full reload, all tables are deleted and then the load script is run. A partial reload only adds new data and keeps the existing tables. Partial reloads have several benefits compared to full reloads: • Faster, because only data recently changed needs to be loaded. With large data sets the difference is significant. • Less memory is consumed, because less data is loaded. • More reliable, because queries to source data run faster, reducing the risk of network problems.	Unselected
Task session timeout (minutes)	The maximum period of time before a task is aborted. When a task is started, a session is started by the manager scheduler and the task is performed by one of the nodes. If the session times out, the manager scheduler forces the node to abort the task and remove the session.	1440
Max retries	The maximum number of times the scheduler tries to rerun a failed task.	0

Triggers (Scheduled)

Scheduled trigger properties

Property	Description
Trigger name	Name of the trigger. Mandatory.
Enabled	Status of the trigger. When selected, the trigger is active.
Time zone	The time zone of your operating system, at the time you create the trigger. When you save a trigger, the settings are kept, and if you move to a different time zone, the original values are still displayed. If you want to change the time zone and start time of a trigger, you need to do that manually. *For a trigger that was created before the introduction of the time zone setting, all times and dates are by default presented in Coordinated Universal Time (UTC).*

Property	Description
Daylight saving time	Way to account for daylight saving time. **Observe daylight saving time**: This option takes daylight saving time (DST) into account. If DST is in use in the selected time zone, the execution time and date are adjusted accordingly. **Permanent standard time**: This option does not take DST into account. If DST is in use in the selected time zone, the execution time and date are not adjusted. **Permanent daylight saving time**: This option takes DST into account. If a time zone uses DST, execution time and date are always according to DST, even during periods when DST is not in use. *For time zones not using DST, always select **Permanent standard time**.* **Example:** You created a trigger for an event at 10:00 AM, while you were working in Ottawa, Canada, in January. The time zone is (GMT-0500) Eastern Time (US & Canada) and DST is used between March and November. If you select **Observe daylight saving time**, a trigger set to start at 10:00 will always start at 10.00. If you select **Permanent standard time**, a trigger set to run at 10:00 will run at 10:00 in the winter but at 09:00 in the summer. If you select **Permanent daylight saving time**, a trigger set to run at 10:00 will run at 11:00 in the winter and at 10:00 in the summer.
Start	Start time and date: • Start time: **(hh:mm)** • Start date: **(YYYY-MM-DD)**

Property	Description

Schedule	Frequency of the trigger:
	
	• **Once**.
	
	• **Hourly**. Time period between executions of the trigger. Edit **Repeat after each** by typing the values for:
	    • **hour(s)** (default is 1)
	    • **minute(s)** (default is 0)
	
	• **Daily**. Time period between executions of the trigger. Type a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	
	• **Weekly**. Time period between executions of the trigger:
	    • Type a value for **Every week(s)** (default is 1).
	    • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	
	• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	
	<blockquote>*If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*</blockquote>
	• **Custom**: When you select **Custom**, two new fields are shown, **Filter** and **Increment**. These options offer great flexibility when scheduling a reload. See *Tasks - Custom option (page 229)* for details.

End	End time and date: • End time: **(hh:mm)** • End date: **(YYYY-MM-DD)** Select **Infinite** to create a trigger with no end date.

Triggers (Task event)

Task event trigger properties

Property	Description
Trigger name	Name of the trigger. Mandatory.
Type	Trigger type.

Property	Description
Enabled	Status of the trigger. When selected, the trigger is active.
Time constraint	Time frame (in minutes) that the other tasks in the task chain must be completed within. There is no effect if the trigger consists of only one task. *Creating a task chain (page 353)*
Tasks	
	Do the following: 1. Click ⊕ **Add task** to add a tasks that will function as a trigger condition. A **Status** list and an empty **Task** field is added. 2. Click the empty field to add a task. A task selection dialog is opened and displays a list of tasks with the following columns: **Name**, **App** connected to the task, and **Tags**, which is the task name. 3. Double-click the task to use as a trigger condition. The task is added to the trigger and the dialog is closed. 4. In the **Status** list, select whether the trigger condition is fulfilled on **TaskSuccessful** or **TaskFail**. > *A task with trigger condition **Task failed** is started not only when the preceding task finishes with status Failed, but also with status Skipped or Error (when the error occurs before reload). In Qlik Sense versions prior to February 2019, a preceding task with status Aborted also started a task with trigger condition Task failed. To enable this behavior, set "DisableLegacyTaskEventTriggerBehavior" to false in Scheduler.exe.config on all Scheduler nodes.* Repeat the steps above for all the tasks that you want to include in the trigger. A task can only be added once and is not displayed in the task selection dialog if it has already been added to the trigger. There is a logical AND between the tasks.

> *The tasks do not need to be executed in any specific order and the **Time constraint** is not static. If all tasks but one have completed when the end of the time frame is reached, the task that was first completed is no longer considered executed and the end of the time frame is recalculated. The trigger then waits for all tasks to be completed within the recalculated time frame.*

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

Custom properties

*If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

5. Click **Apply** to create and save the rule.
   Successfully added is displayed at the bottom of the page.

Editing reload tasks

You can edit reload tasks that you have update rights to from the app association page.

You can also edit reload tasks from the tasks overview page.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the apps that you want to edit tasks for and click **Edit** in the action bar.
4. Select **Tasks** under **Associated items**.
5. Select the tasks that you want to edit and click **Edit** in the action bar.
   The **Reload task edit** page is displayed.
6. Edit the properties.
   a. You can change the task name in the **Name** field.
   b. **App** displays the app that you selected from the overview. You can change which app you are creating the task for by clicking the **App** field. In the dialog that opens, double-click the app that you want this task to reload.
   c. You can change the **Execution** properties, see descriptions below.
   d. A task must have at least one trigger to be executed automatically. Manage the triggers by clicking **Actions**▼ in the **Triggers** table heading and selecting one of the following:
      - **Create new once-only trigger**, **Create new hourly trigger**, **Create new daily trigger**, **Create new weekly trigger**, or **Create new monthly trigger**. These are trigger shortcuts and the trigger that you select is added to the table instantly. The start value

for the trigger is set to 5 minutes from when it was created and the trigger is enabled.

- **Create new scheduled trigger** or **Create new task event trigger** to create a new trigger of the selected type (see the property descriptions below). A dialog opens. Edit the trigger and click **OK** to close the dialog and add the trigger to the table.
- **Delete** if you want to delete the trigger that is selected in the table.
- **Edit** if you want to open the edit dialog for the trigger that is selected in the table. Edit the trigger and click **OK** to close the dialog and save your changes.

e. Optionally, apply tags.

f. Optionally, apply custom properties.

Identification

All fields are mandatory and must not be empty.

Identification properties

Property	Description	Default value
Name	The name of the task.	Reload task of <App name>
App	The name of the app that the task is created for. Click in the field to open a dialog where you can select (by double-clicking) which app the task reloads.	<App name>

Execution

Execution properties

Property	Description	Default value
Enabled	The task is enabled when selected.	Selected
Partial reload	With partial reload, you can add new data without reloading all the existing tables in the data model. In a full reload, all tables are deleted and then the load script is run. A partial reload only adds new data and keeps the existing tables. Partial reloads have several benefits compared to full reloads: • Faster, because only data recently changed needs to be loaded. With large data sets the difference is significant. • Less memory is consumed, because less data is loaded. • More reliable, because queries to source data run faster, reducing the risk of network problems.	Unselected

Property	Description	Default value
Task session timeout (minutes)	The maximum period of time before a task is aborted. When a task is started, a session is started by the manager scheduler and the task is performed by one of the nodes. If the session times out, the manager scheduler forces the node to abort the task and remove the session.	1440
Max retries	The maximum number of times the scheduler tries to rerun a failed task.	0

Triggers (Scheduled)

Scheduled trigger properties

Property	Description
Trigger name	Name of the trigger. Mandatory.
Enabled	Status of the trigger. When selected, the trigger is active.
Time zone	The time zone of your operating system, at the time you create the trigger. When you save a trigger, the settings are kept, and if you move to a different time zone, the original values are still displayed. If you want to change the time zone and start time of a trigger, you need to do that manually. *For a trigger that was created before the introduction of the time zone setting, all times and dates are by default presented in Coordinated Universal Time (UTC).*

Property	Description
Daylight saving time	Way to account for daylight saving time. **Observe daylight saving time**: This option takes daylight saving time (DST) into account. If DST is in use in the selected time zone, the execution time and date are adjusted accordingly. **Permanent standard time**: This option does not take DST into account. If DST is in use in the selected time zone, the execution time and date are not adjusted. **Permanent daylight saving time**: This option takes DST into account. If a time zone uses DST, execution time and date are always according to DST, even during periods when DST is not in use. *For time zones not using DST, always select **Permanent standard time**.* **Example:** You created a trigger for an event at 10:00 AM, while you were working in Ottawa, Canada, in January. The time zone is (GMT-0500) Eastern Time (US & Canada) and DST is used between March and November. If you select **Observe daylight saving time**, a trigger set to start at 10:00 will always start at 10.00. If you select **Permanent standard time**, a trigger set to run at 10:00 will run at 10:00 in the winter but at 09:00 in the summer. If you select **Permanent daylight saving time**, a trigger set to run at 10:00 will run at 11:00 in the winter and at 10:00 in the summer.
Start	Start time and date: • Start time: **(hh:mm)** • Start date: **(YYYY-MM-DD)**

Property	Description

Schedule	Frequency of the trigger:
	
	• **Once**.
	
	• **Hourly**. Time period between executions of the trigger. Edit **Repeat after each** by typing the values for:
	    • **hour(s)** (default is 1)
	    • **minute(s)** (default is 0)
	
	• **Daily**. Time period between executions of the trigger. Type a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	
	• **Weekly**. Time period between executions of the trigger:
	    • Type a value for **Every week(s)** (default is 1).
	    • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	
	• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	
	       *If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*
	
	• **Custom**: When you select **Custom**, two new fields are shown, **Filter** and **Increment**. These options offer great flexibility when scheduling a reload. See *Tasks - Custom option (page 229)* for details.

End	End time and date: • End time: **(hh:mm)** • End date: **(YYYY-MM-DD)** Select **Infinite** to create a trigger with no end date.

Triggers (Task event)

Task event trigger properties

Property	Description
Trigger name	Name of the trigger. Mandatory.
Type	Trigger type.

Property	Description
Enabled	Status of the trigger. When selected, the trigger is active.
Time constraint	Time frame (in minutes) that the other tasks in the task chain must be completed within. There is no effect if the trigger consists of only one task. *Creating a task chain (page 353)*
Tasks	
	Do the following: 1. Click ⊕ **Add task** to add a tasks that will function as a trigger condition. A **Status** list and an empty **Task** field is added. 2. Click the empty field to add a task. A task selection dialog is opened and displays a list of tasks with the following columns: **Name**, **App** connected to the task, and **Tags**, which is the task name. 3. Double-click the task to use as a trigger condition. The task is added to the trigger and the dialog is closed. 4. In the **Status** list, select whether the trigger condition is fulfilled on **TaskSuccessful** or **TaskFail**. ⓘ *A task with trigger condition **Task failed** is started not only when the preceding task finishes with status Failed, but also with status Skipped or Error (when the error occurs before reload). In Qlik Sense versions prior to February 2019, a preceding task with status Aborted also started a task with trigger condition Task failed. To enable this behavior, set "DisableLegacyTaskEventTriggerBehavior" to false in Scheduler.exe.config on all Scheduler nodes.* Repeat the steps above for all the tasks that you want to include in the trigger. A task can only be added once and is not displayed in the task selection dialog if it has already been added to the trigger. There is a logical AND between the tasks.

ⓘ *The tasks do not need to be executed in any specific order and the **Time constraint** is not static. If all tasks but one have completed when the end of the time frame is reached, the task that was first completed is no longer considered executed and the end of the time frame is recalculated. The trigger then waits for all tasks to be completed within the recalculated time frame.*

Tags

Tags properties

Property	Description
Tags	If no tags are available, this property group is empty.
	Connected tags are displayed under the text box.

Custom properties

> If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.

7. Click **Apply** in the action bar to apply and save your changes.
   Successfully updated is displayed at the bottom of the page.

Tasks - Custom option

When creating a task, the option **Custom** offers great flexibility for the scheduling of a task. It is important to be familiar with the syntax for the respective fields, **Filter** and **Increment** to create well-functioning tasks. This topic details the options when using a **Custom** schedule.

Filter

What you set as a filter is when a task can be triggered, not the opposite. The filter defines the conditions for a task.

The default syntax for the filter is "* * – * * * * *". There should be no spaces in the filter other than between each position. The space character is used as a delimiter between the positions, and inserting one would most likely cause an error in the filter.

Positions

Left to right (first position is 0), each position is explained here.

Position 0 - Minute

Legend: 1–60. '*' = all

Which minute of an hour (0 - 60) that a task can be triggered.

Position 1 - Hour

Legend: 1–24. '*' = all

Which hour of a day (1-24) that a task can be triggered.

Position 2 - WeekDayPrefix

Legend: 1–4. '¤' = last. '–' = none

WeekDayPrefix works together with WeekDay by adding a prefix. With WeekDayPrefix, you can state that only the last (¤) Friday in a given month or first (1) Saturday in a given month that a task can be triggered.

Syntax: Position 3 - WeekDay
Legend: 0–6 (where Sunday is 0)

Which weekday that a task can be triggered.

Position 4 - WeeklyInterval

Legend: An integer. '*' = all

The task can be triggered every n:th week, where n is the number set in this position.

Position 5 - DayOfMonth

Legend: 1–31. '*' = all. '¤' = last

Which day of a month that a task can be triggered. Using last (¤), the task will be triggered on the last day of a month, which is checked dynamically depending on month (and leap year).

> *For Microsoft Windows users: You can add the last symbol (¤) by holding **Alt** and typing **0164** on the numeric keypad.*

Position 6 - Month

Legend: 1–12. '*' = all

Which month of a year that a task can be triggered.

Position 7 - MonthlyInterval

Legend: `an integer`. '*' = all

How many months that must pass before a task can be triggered.

For Minute, Hour, WeekDay, DayOfMonth and Month, you can use syntax with hyphen (–) to state "From - To". For WeekDayPrefix, WeeklyInterval, and MonthlyInterval, you must state each character to be used in the filter. This option can also be used by Minute, Hour, WeekDay, DayOfMonth, and Month.

Example: You only want to allow a task the first 15 minutes of each hour. You can either put '1–15' or '1,2,3,4,5,6,7,8,9,10,11,12,13,14,15' in the first position.

Increment
Default: "0 0 0 0"

If the default increment is used, that is "0 0 0 0", the task will only be triggered once.

Left to right (first position is 0) each position is explained here.

Position 0 - Minutes

How many minutes to increment.

Position 1 - Hours

How many hours to increment.

Position 2 - Days

How many days to increment.

Position 3 - Weeks

How many weeks to increment.

General guidelines

- An hourly task, with higher frequency than once per hour, should set Minutes to an appropriate figure.
- An hourly task, with a frequency of once every hour or less, should set Hours to an appropriate figure.
- A daily task should set Days to an appropriate figure.
- A weekly or monthly trigger should set Days to an appropriate figure if any filter exists because they are based on daily evaluations (such as run every Thursday and Saturday every 4 weeks, or the 5th, 10th, and 15th day every month).
- If no filter exists, the increment should match how often the task should trigger.

Examples

Here are a few examples on how to set up a task.

Certain hour and minutes

Premise: The task should only trigger between 11.15 and 11.59 (any day).

The following filter only allows a task to be triggered between 11.15 and 11.59 any given day of the year.

Filter: "15-59 11 - * * * * *"

Explanation: Position 0 is '15-59' which means it will only trigger during those minutes.

Position 1 is '11' which means it will only trigger during that hour.

Increment for this task is based on what is to be accomplished, but there are pitfalls. Most notably, if you are scheduling a task, and the start time is outside of 11.15 - 11.59, say 12.15, and the increment is set to advance one day at a time, this task will never trigger. Most likely the increment should be every n hours or every n minutes.

Using WeekDayPrefix

Premise: The task should only trigger the first Monday every month.

Filter: "* * 1 1 * * * *"

Explanation: Position 2 is set to '1' which means the first of the later given weekdays is allowed. Position 3 is set to '1' which means only Mondays (0 is Sunday) are allowed for this task.

This task should increment one day, that is,"0 0 1 0".

Certain date in a month

Case 1

Premise: Run the first every month.

Filter: "* * - * * 1 * *"

Explanation: Position 5 is set to '1' which means the only day number 1 in any given month is allowed for this task.

This task should increment one day, that is,"0 0 1 0".

Case 2

Premise: Run the last day every month.

Filter: "* * - * * ¤ * *"

Explanation: Position 5 is set to '¤' which means the only last day in any given month is allowed for this task.

This task should increment one day, that is,"0 0 1 0".

Case 3

Premise: Run the last day each year.

Filter: "* * - * * ¤ 12 *"

Explanation: Position 5 is set to '¤' which means the last day in any given month is allowed for this task. Position 6 is set to '12' which means only the 12th month (December) is allowed for this task.

This task should increment one day, that is,"0 0 1 0".

Certain weekdays

Premise: Run Monday and Wednesday every week.

Filter: "* * - 1,3 * * * *"

Explanation: Position 4 is set to '1,3' which means only Monday and Wednesday are allowed for this task (0 is Sunday).

This task should increment one day, that is, "0 0 1 0".

Using WeekDayPrefix, WeekDay, and Month

Premise: Run last Friday every other month.

Filter: "* * ¤ 5 * * 1,3,5,7,9,11 *"

Explanation: Position 3 is set to '¤' which means the last weekday given in Position 4. Position 4 is set to '5' which means Friday (Sunday is 0) is allowed for this task. Together they read 'Last Friday'. Position 6 is set to '1,3,5,7,9,11' which means only those months are allowed for this task.

This task should increment one day, that is, "0 0 1 0".

Creating and editing external program tasks

With external program tasks, you can trigger external processes, such as scripts or .exe files. Task chaining is supported and you can combine reload tasks with external program tasks.

Do the following:

1. In the QMC, open **Tasks**.
2. Click ✚ **External program task** to create a new external program task, or double-click an existing task to edit it.
3. Enter a task name.
4. Enter a path to the file to trigger.
5. Enter input parameters for the file to trigger, if any.
6. Optionally, edit the settings in the section **EXECUTION**.

    > ℹ️ *Task session timeout: The maximum period of time before a task is aborted. When a task is started, a session is started by the manager scheduler and the task is performed by one of the nodes. If the session times out, the manager scheduler forces the node to abort the task and remove the session.*

7. A task must have at least one trigger to be executed automatically. Manage the triggers by clicking **Actions**▼ in the **Triggers** table heading and selecting one of the following:

    • **Create new once-only trigger**, **Create new hourly trigger**, **Create new daily trigger**, **Create new weekly trigger**, or **Create new monthly trigger**. These are trigger shortcuts and the trigger that you select is added to the table instantly. The start value for the trigger is set to 5 minutes from when it was created and the trigger is enabled.

    • **Create new scheduled trigger** or **Create new task event trigger** to create a new trigger of the selected type (see the property descriptions below). A dialog opens. Edit the trigger and click **OK** to close the dialog and add the trigger to the table.

    • **Edit** if you want to open the edit dialog for the trigger that is selected in the table. Edit the trigger and click **OK** to close the dialog and save your changes.

    • **Delete** if you want to delete the trigger that is selected in the table.
    Clicking undo (↩) in the **Triggers** heading applies to all triggers you are currently editing.

Triggers (Scheduled)

Scheduled trigger properties

Property	Description
Trigger name	Name of the trigger. Mandatory.
Enabled	Status of the trigger. When selected, the trigger is active.
Time zone	The time zone of your operating system, at the time you create the trigger. When you save a trigger, the settings are kept, and if you move to a different time zone, the original values are still displayed. If you want to change the time zone and start time of a trigger, you need to do that manually. *For a trigger that was created before the introduction of the time zone setting, all times and dates are by default presented in Coordinated Universal Time (UTC).*
Daylight saving time	Way to account for daylight saving time. **Observe daylight saving time**: This option takes daylight saving time (DST) into account. If DST is in use in the selected time zone, the execution time and date are adjusted accordingly. **Permanent standard time**: This option does not take DST into account. If DST is in use in the selected time zone, the execution time and date are not adjusted. **Permanent daylight saving time**: This option takes DST into account. If a time zone uses DST, execution time and date are always according to DST, even during periods when DST is not in use. *For time zones not using DST, always select **Permanent standard time**.* **Example:** You created a trigger for an event at 10:00 AM, while you were working in Ottawa, Canada, in January. The time zone is (GMT-0500) Eastern Time (US & Canada) and DST is used between March and November. If you select **Observe daylight saving time**, a trigger set to start at 10:00 will always start at 10.00. If you select **Permanent standard time**, a trigger set to run at 10:00 will run at 10:00 in the winter but at 09:00 in the summer. If you select **Permanent daylight saving time**, a trigger set to run at 10:00 will run at 11:00 in the winter and at 10:00 in the summer.

Property	Description
Start	Start time and date: • Start time: **(hh:mm)** • Start date: **(YYYY-MM-DD)**

Schedule	Frequency of the trigger:
	
	• **Once**.
	
	• **Hourly**. Time period between executions of the trigger. Edit **Repeat after each** by typing the values for:
	    • **hour(s)** (default is 1)
	    • **minute(s)** (default is 0)
	
	• **Daily**. Time period between executions of the trigger. Type a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	
	• **Weekly**. Time period between executions of the trigger:
	    • Type a value for **Every week(s)** (default is 1).
	    • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	
	• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	
	    *If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*
	
	• **Custom**: When you select **Custom**, two new fields are shown, **Filter** and **Increment**. These options offer great flexibility when scheduling a reload. See *Tasks - Custom option (page 229)* for details.

End	End time and date: • End time: **(hh:mm)** • End date: **(YYYY-MM-DD)** Select **Infinite** to create a trigger with no end date.

Triggers (Task event)

Task event trigger properties

Property	Description
Trigger name	Name of the trigger. Mandatory.
Type	Trigger type.
Enabled	Status of the trigger. When selected, the trigger is active.
Time constraint	Time frame (in minutes) that the other tasks in the task chain must be completed within. There is no effect if the trigger consists of only one task. *Creating a task chain (page 353)*
Tasks	
	Do the following: 1. Click ➕ **Add task** to add a tasks that will function as a trigger condition. A **Status** list and an empty **Task** field is added. 2. Click the empty field to add a task. A task selection dialog is opened and displays a list of tasks with the following columns: **Name**, **App** connected to the task, and **Tags**, which is the task name. 3. Double-click the task to use as a trigger condition. The task is added to the trigger and the dialog is closed. 4. In the **Status** list, select whether the trigger condition is fulfilled on **TaskSuccessful** or **TaskFail**. ⓘ *A task with trigger condition **Task failed** is started not only when the preceding task finishes with status Failed, but also with status Skipped or Error (when the error occurs before reload). In Qlik Sense versions prior to February 2019, a preceding task with status Aborted also started a task with trigger condition Task failed. To enable this behavior, set "DisableLegacyTaskEventTriggerBehavior" to false in Scheduler.exe.config on all Scheduler nodes.* Repeat the steps above for all the tasks that you want to include in the trigger. A task can only be added once and is not displayed in the task selection dialog if it has already been added to the trigger. There is a logical AND between the tasks.

ⓘ *The tasks do not need to be executed in any specific order and the **Time constraint** is not static. If all tasks but one have completed when the end of the time frame is reached, the task that was first completed is no longer considered executed and the end of the time frame is recalculated. The trigger then waits for all tasks to be completed within the recalculated time frame.*

8. Optionally, add tags and custom properties.

9. Click **Apply** to save the task.

Creating and editing distribution tasks

With distribution tasks, you can trigger distribution of apps from client-managed Qlik Sense to Qlik Cloud.

Do the following:

1. In the QMC, open **Tasks**.

2. Click ➕ **Distribution task** to create a new distribution task, or double-click an existing task to edit it.

3. Enter a task name.

4. Select the app to distribute.

5. Enter input parameters for the file to trigger, if any.

6. Optionally, edit the settings in the section **EXECUTION**.

> ℹ️ *Task session timeout: The maximum period of time before a task is aborted. When a task is started, a session is started by the manager scheduler and the task is performed by one of the nodes. If the session times out, the manager scheduler forces the node to abort the task and remove the session.*

7. A task must have at least one trigger to be executed automatically. Manage the triggers by clicking **Actions▼** in the **Triggers** table heading and selecting one of the following:

    *   **Create new once-only trigger**, **Create new hourly trigger**, **Create new daily trigger**, **Create new weekly trigger**, or **Create new monthly trigger**. These are trigger shortcuts and the trigger that you select is added to the table instantly. The start value for the trigger is set to 5 minutes from when it was created and the trigger is enabled.

    *   **Create new scheduled trigger** or **Create new task event trigger** to create a new trigger of the selected type (see the property descriptions below). A dialog opens. Edit the trigger and click **OK** to close the dialog and add the trigger to the table.

    *   **Edit** if you want to open the edit dialog for the trigger that is selected in the table. Edit the trigger and click **OK** to close the dialog and save your changes.

    *   **Delete** if you want to delete the trigger that is selected in the table.
        Clicking undo (↩) in the **Triggers** heading applies to all triggers you are currently editing.

    Triggers (Scheduled)

Scheduled trigger properties

Property	Description
Trigger name	Name of the trigger. Mandatory.
Enabled	Status of the trigger. When selected, the trigger is active.

Property	Description
Time zone	The time zone of your operating system, at the time you create the trigger. When you save a trigger, the settings are kept, and if you move to a different time zone, the original values are still displayed. If you want to change the time zone and start time of a trigger, you need to do that manually. *For a trigger that was created before the introduction of the time zone setting, all times and dates are by default presented in Coordinated Universal Time (UTC).*
Daylight saving time	Way to account for daylight saving time. **Observe daylight saving time**: This option takes daylight saving time (DST) into account. If DST is in use in the selected time zone, the execution time and date are adjusted accordingly. **Permanent standard time**: This option does not take DST into account. If DST is in use in the selected time zone, the execution time and date are not adjusted. **Permanent daylight saving time**: This option takes DST into account. If a time zone uses DST, execution time and date are always according to DST, even during periods when DST is not in use. *For time zones not using DST, always select **Permanent standard time**.* **Example:** You created a trigger for an event at 10:00 AM, while you were working in Ottawa, Canada, in January. The time zone is (GMT-0500) Eastern Time (US & Canada) and DST is used between March and November. If you select **Observe daylight saving time**, a trigger set to start at 10:00 will always start at 10.00. If you select **Permanent standard time**, a trigger set to run at 10:00 will run at 10:00 in the winter but at 09:00 in the summer. If you select **Permanent daylight saving time**, a trigger set to run at 10:00 will run at 11:00 in the winter and at 10:00 in the summer.
Start	Start time and date: - Start time: **(hh:mm)** - Start date: **(YYYY-MM-DD)**

Property	Description

Schedule	Frequency of the trigger:
	
	• **Once**.
	
	• **Hourly**. Time period between executions of the trigger. Edit **Repeat after each** by typing the values for:
	    • **hour(s)** (default is 1)
	    • **minute(s)** (default is 0)
	
	• **Daily**. Time period between executions of the trigger. Type a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	
	• **Weekly**. Time period between executions of the trigger:
	    • Type a value for **Every week(s)** (default is 1).
	    • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	
	• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	
	    *If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*
	
	• **Custom**: When you select **Custom**, two new fields are shown, **Filter** and **Increment**. These options offer great flexibility when scheduling a reload. See *Tasks - Custom option (page 229)* for details.

End	End time and date: • End time: **(hh:mm)** • End date: **(YYYY-MM-DD)** Select **Infinite** to create a trigger with no end date.

Triggers (Task event)

Task event trigger properties

Property	Description
Trigger name	Name of the trigger. Mandatory.
Type	Trigger type.

Property	Description
Enabled	Status of the trigger. When selected, the trigger is active.
Time constraint	Time frame (in minutes) that the other tasks in the task chain must be completed within. There is no effect if the trigger consists of only one task. *Creating a task chain (page 353)*
Tasks	
	Do the following: 1. Click ➕ **Add task** to add a tasks that will function as a trigger condition. A **Status** list and an empty **Task** field is added. 2. Click the empty field to add a task. A task selection dialog is opened and displays a list of tasks with the following columns: **Name**, **App** connected to the task, and **Tags**, which is the task name. 3. Double-click the task to use as a trigger condition. The task is added to the trigger and the dialog is closed. 4. In the **Status** list, select whether the trigger condition is fulfilled on **TaskSuccessful** or **TaskFail**. *A task with trigger condition **Task failed** is started not only when the preceding task finishes with status Failed, but also with status Skipped or Error (when the error occurs before reload). In Qlik Sense versions prior to February 2019, a preceding task with status Aborted also started a task with trigger condition Task failed. To enable this behavior, set "DisableLegacyTaskEventTriggerBehavior" to false in Scheduler.exe.config on all Scheduler nodes.* Repeat the steps above for all the tasks that you want to include in the trigger. A task can only be added once and is not displayed in the task selection dialog if it has already been added to the trigger. There is a logical AND between the tasks.

*The tasks do not need to be executed in any specific order and the **Time constraint** is not static. If all tasks but one have completed when the end of the time frame is reached, the task that was first completed is no longer considered executed and the end of the time frame is recalculated. The trigger then waits for all tasks to be completed within the recalculated time frame.*

8. Optionally, add tags and custom properties.
9. Click **Apply** to save the task.

Distribution task rights can be controlled by the `ReloadTask_*` resource filter. .

Triggers

You use triggers to determine when tasks are to be executed. There are two types of triggers:

- Scheduled triggers
- Task event triggers

Scheduled triggers

With a scheduled trigger, you can schedule the number of task executions to be performed and the execution frequency. The number of task executions ranges from one to infinity, and the frequency ranges from hourly to monthly. You can apply scheduled triggers to both reload tasks and user sync tasks.

Example:

You want to create a scheduled trigger for a user sync task. The trigger is to be activated once every month.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select the user sync task that you want to create a trigger for and click **Edit**.
4. Under **Associated items**, select **Triggers**.
5. Click **Create associated trigger**.
   The **Trigger - Start on schedule** window is opened.
6. Fill in the trigger name and the start time and date.
7. For **Schedule**, select **Monthly**.
8. Select a date for the trigger and clear any other date selection.

   > *To ensure that a trigger is repeated every month, you should not select a date later than the 28th.*

9. If needed, set the end date and time. By default, there is no end date.

Task event triggers

With a task event trigger you set one or more conditions for when the trigger is activated. To create a condition, you select a task and the status of that task, either task successful or task failed. If that condition is met, as well as any other additional conditions, the trigger activates a reload of the app. Task event triggers can only be applied to reload tasks.

Example:

You have two apps that are closely related, and to make sure that the apps are in sync, the second app is only to reload if the first app has the status task successful.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select the reload task that you want to create a trigger for and click **Edit**.
4. In the **Triggers** heading bar, click **Actions**.
   A popup is displayed with different trigger options.
5. Select **Create new task event trigger**.
   The **Trigger - Start on task event** window is opened.
6. Fill in the trigger name and the time constraint.
7. Click **Add task**.
8. Click the **Task** field and select the task that the trigger is dependent on.
9. Select the status for the task, in this case **Task successful**.
   The trigger will only be activated if the task has the status **Task successful**.
10. Click **OK**.
    The new trigger is added to the triggers list.
11. Click **Apply**.

> *You can also trigger a reload task or sync task manually from the tasks overview page.*

Deleting reload tasks

You can delete tasks that you have delete rights to from the app association page.

> *You can also delete reload tasks from the tasks overview page.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the apps that you want to delete tasks from and click **Edit** in the action bar.
4. Select **Tasks** under **Associated items**.
   The **App association items** page with the **Reload tasks** overview is displayed.
5. Select the tasks to delete and click **Delete** in the action bar.
   A **Delete** dialog is displayed.
6. Click **OK**.

Starting reload tasks

You can manually start reload tasks from the app's association page.

> *You can also start reload tasks from the task overview page.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the apps that you want to start tasks for and click **Edit** in the action bar.

4. Select **Tasks** under **Associated items**.
    The **App associated items** page is displayed.

5. Select the tasks that you want to start and click **Start** in the action bar.

> *Tasks can also be started by triggers.*

Stopping reload tasks

You can manually stop reload tasks from the app's association page.

> *You can also stop reload tasks from the task overview page.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the apps that you want to stop tasks for and click **Edit** in the action bar.

4. Select **Tasks** under **Associated items**.
    The **App associations** page with the **Tasks** overview is displayed.

5. Select the tasks that you want to stop and click **Stop** in the action bar.

Reloading apps manually

You can reload apps manually to fully reload the data in an app from the source. Any old data is discarded.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Apps** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the app that you want to reload, click **More actions** and select **Reload now** in the pop-up menu.
    A feedback message is displayed.

4. Go to the **Tasks** overview page to find out the progress of the task. The **Name** column displays
    Manually triggered reload of [app name]. When the task has finished the **Status** column displays ✔
    Success.

5. Optional: The manually started reload app task is executed once only. Therefore, you probably want to
    delete this task from the task overview.

    a. Select the task and click **Delete**.
        A dialog is displayed.

b. Click **OK** to confirm the deletion.
The task is deleted from the overview.

Creating content libraries

A content library is a storage that enables the Qlik Sense users to add shared contents to their apps.

The user who creates the content library automatically becomes the owner of that library. The library and the library objects can be shared with others through security rules defined in the QMC.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Content libraries** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Click ➕ **Create new** in the action bar.

4. Edit the properties.

> *You can display or hide property groups using the panel to the far right.*

Identification

Identification properties

Property	Description
Name	The name of the content library. Mandatory.
Owner	The owner of the content library. This property does not exist until the content library is created.

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.*
	Connected tags are displayed under the text box.

Custom properties

> *If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

5. Click **Apply** in the action bar to create and save the content library.
   The **Create security rule** dialog opens.

6. Edit the security rule for administrative access of the content library:

   a. Edit the **Identification** properties:

Identification fields and values

Field	Value
Name	Enter the name of the content library. Mandatory.
Disabled	Select to disable the rule. The rule is enabled by default.
Description	Enter a description for the rule.

   b. Create the conditions for the rule in the **Basic** section:

   - Select which actions the rule should apply for.
   - Use the drop downs to create a condition that specifies which users the rule will apply to.
   - Click ✚ to add a condition. When using multiple conditions, you can group two conditions by clicking **Group**. After the conditions have been grouped, you have the option **Ungroup**. Additional subgrouping options are **Split** and **Join**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that AND is superior to OR.

Operator descriptions

Operator	Descriptions and examples
=	This operator is not case sensitive and returns True if the compared expressions are exactly equal. **Example:** `user.name = "a*"` The user named exactly a* is targeted by the rule.
like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name = "a*"` All users with names beginning with an a are targeted by the rule..
!=	This operator is not case sensitive and returns True if the attribute values in the compared expressions are equal. **Example:** `user.name=resource.name` All resources with the same name as the user are targeted by the rule.

Successfully added is displayed at the bottom of the page.

You have now created a new content library.

Editing content libraries

A content library is a storage that enables the Qlik Sense users to add shared contents to their apps.

The user who creates the content library automatically becomes the owner of that library. The library and the library objects can be shared with others through security rules defined in the QMC.

You can edit the content libraries that you have update rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Content libraries** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the library you want to edit.
4. Click **Edit** in the action bar.
5. Edit the properties.

Identification

Identification properties

Property	Description
Name	The name of the content library. Mandatory.
Owner	The owner of the content library. This property does not exist until the content library is created.

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.*
	Connected tags are displayed under the text box.

Custom properties

*If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

6. Click **Apply** in the action bar.

Successfully updated is displayed at the bottom of the page.

Deleting content libraries

You can delete content libraries that you have update rights to. When deleting a content library, all library objects are also deleted.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Content libraries** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the content libraries that you want to delete.
4. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
5. Click **OK**.

Uploading objects to content libraries

You can upload objects to the content libraries that you have update rights to. Qlik Sense only uses image files, but you can upload any file type with an extension that exists in the allow list for content libraries. The maximum file size is specified in the documentation for Qlik Sense on Windows.

> *The Qlik Sense Repository Service scans for script tags in XML files uploaded to AppContent or Content Library.*

You can choose to upload objects from the content libraries overview page or from the content library **Associated items**.
Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Content libraries** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

> *You can filter a column by using the filtering option:* ▾

3. Select the content library that you want to upload objects to and click **Upload**.
   Alternatively:
   Select the content library and click **Edit** in the action bar, then select **Contents** under **Associated items** and click ➕ **Upload** in the action bar on the **Contents** page.
   Either way, the **Upload static content** dialog opens.
4. Click **Browse**.
   A browse window opens.
5. Browse to the files you want to import and click **Open**.
   The browse window closes and the files are added to **Selected files** in the **Upload static content** dialog.
6. Click **Upload**.

The **Ongoing transports** dialog opens. Any other transports you have initiated are also displayed in the dialog.

- A spinner is displayed during the file import. **Duration** shows you how long the import has been ongoing.
- Click ✖ if you want to cancel the upload.
  ⚠ and **Aborted** is displayed and the upload stops.
- ↻ is displayed when an upload is queued. The upload starts when less than four upload processes are running.
- Click **Remove** if you want to remove a failed item ⚠.
  The item is removed.
- **Conflict error with existing file** is displayed if an identical file already exists in the content library:
  - Click **Overwrite** if you want to replace the existing file with the new file.
    The upload continues.
  - Click **Cancel** to stop the upload.
    The item is removed from the dialog and the existing item is kept in the library.

When the file is uploaded, ✔ is displayed for 15 seconds and the file is added to the selected **Content library**. When all your transports have finished successfully, the **Ongoing transports** dialog closes. If there are any failed transports, the dialog is displayed until the overview page is refreshed.

> *Click the **URL path** from the **Contents** overview if you want to view an uploaded file. The file is displayed in a new tab.*

Deleting objects from content libraries

You can delete objects from the content libraries that you have delete rights to.

> *If you delete a content library, all its objects are deleted.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Content libraries** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the content library that you want to delete objects from and click **Edit**.
   The content library edit page opens.
4. Select **Contents** under **Associated items**.
   The contents overview is displayed.
5. Select the files that you want to delete.
6. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.

7. Click **OK**.
    The files are deleted from the repository and removed from the contents overview.

Creating access rights for content libraries

A content library is a storage that enables the Qlik Sense users to add shared contents to their apps.

The user who creates the content library automatically becomes the owner of that library. The library and the library objects can be shared with others through security rules defined in the QMC.

You create security rules to give access rights for the content libraries.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Content libraries** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the content library that you want to create rules for.
4. Click **Edit**.
5. The content library edit page opens.
6. Select **Security rules** under **Associated items**.

    > ⓘ *The security rules overview is displayed.*

7. Click ➕ **Create associated rule** in the action bar.

    > ⓘ *The **Create security rule** dialog opens.*

8. Edit the security rule for administrative access of the content library:
    a. Edit the **Identification** properties:

        Identification fields and values

Field	Value
Name	Enter the name of the content library. Mandatory.
Disabled	Select to disable the rule. The rule is enabled by default.
Description	Enter a description for the rule.

    b. Create the conditions for the rule in the **Basic** section:
        1. Select which actions the rule should apply for.
        2. Use the drop downs to create a condition that specifies which users the rule will apply to.
        3. Click ➕ to add a condition. When using multiple conditions, you can group two conditions by clicking **Group**. After the conditions have been grouped, you have the option **Ungroup**. Additional subgrouping options are **Split** and **Join**. The default

operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that AND is superior to OR.

Operator descriptions

Operator	Descriptions and examples
=	This operator is not case sensitive and returns True if the compared expressions are exactly equal. **Example:** `user.name = "a*"` The user named exactly a* is targeted by the rule.
like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name = "a*"` All users with names beginning with an a are targeted by the rule.
!=	This operator is not case sensitive and returns True if the attribute values in the compared expressions are equal. **Example:** `user.name=resource.name` All resources with the same name as the user are targeted by the rule.

9. Click **Apply**.

> The dialog closes and the rule is added to the security rules overview.

> The security rule results in a corresponding security rule in the **Security rule** overview page.

You have now created the access rights for the selected content library.

Editing app objects

You can edit app objects that you have update rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **App objects** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the app objects you want to edit.

4. Click **Edit** in the action bar.
   The number next to **Edit** indicates the number of items in your selection that you are allowed to edit.

5. Edit the properties.

> 💡 *You can display or hide property groups using the panel to the far right.*

Identification

Identification properties

Property	Description
Name	The name of the app object. Mandatory.
Owner	The owner of the app object.

Tags

Tag properties

Property	Description
Tags	Click the text box to see the available tags. Start typing to reduce the list. Connected tags are listed under the text box.

6. Click **Apply** in the action bar.

Successfully updated is displayed at the bottom of the page.

Deleting app objects

You can delete app objects that you have delete rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **App objects** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the app objects that you want to delete.

4. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.

5. Click **OK**.

Managing on-demand apps

On-demand apps are generated in the Qlik Sense hub from navigation links that connect selection apps to template apps. The On-demand app service must be enabled to generate on-demand apps. You can create and publish selection and template apps to streams from the Qlik Sense hub, if you have the appropriate access rights. Selection and template apps can also be published to streams from the QMC, which is a part of Qlik Sense. Generated on-demand apps can also be published from the QMC or the Qlik Sense hub, if you have the appropriate access rights.

The security rules applied to the app, stream, or user, determine who can access the content and what the user is allowed to do. The app is locked when published. Content can be added to a published app through the Qlik Sense hub in a server deployment, but content that was published with the original app cannot be edited.

On-demand app service properties

Selection and template apps can be created without the On-demand app service being enabled, but the service must be enabled to create navigation links and generate on-demand apps. The On-demand app service is managed in the QMC. The following properties of the On-demand app service can be managed:

Property descriptions

Property	Description
Enable on-demand app service	Enables and disables the On-demand app service. The service is disabled by default. When the service is switched from enabled to disabled, any pending requests to generate on-demand apps are allowed to finish. But once the service has been disabled, no new requests to generate apps will be accepted.
Enable dynamic views	With dynamic views you can refresh charts from within your analytic tool environment. The on-demand app service must be turned on to enable dynamic views. Turn on dynamic views to allow app sheets to contain charts that are loaded from data sources on-demand. If you have apps whose sheets contain charts based on dynamic views and the **Dynamic views** setting is disabled for the tenant, the apps will continue to function with the following limitations: • All dynamic charts appear dimmed (and without data) to indicate that the dynamic view functionality has been disabled. • The sheet editor does not expose the dynamic view assets. All charts and features not related to dynamic views will continue to function normally.
Logging level	Specifies the level of detail written to the service log file.

Property	Description
Number of apps that can be generated at one time	Specifies the number of apps the service can generate at one time. The default is 1 and the maximum is 10. This setting affects the response time for an app generation, but the amount of data loaded must also be considered when setting the number of apps that can be generated at one time. When the data load sizes are moderate, a higher number of apps generated at one time will improve response time for each app. But when load sizes are large, the response can be slower than if the setting were lower and apps had to wait in queue to be generated. In a multi-node environment, the setting for the number of apps that can be generated at one time applies to all instances of the On-demand app services running in that environment. If multiple services use the same Qlik associative engine, the load on that Qlik associative engine could be the cumulative number of apps to generate at one time from the multiple instances of the service.
Number of days before purging historical data	Specifies the number of days certain historical data about on-demand apps is kept before the data is removed. Values can be 0-365. A setting of 0 means the data is never deleted. The default value is 90 days. The On-demand app service keeps data about navigation links and about requests to generate and reload on-demand apps. When an on-demand app navigation link is deleted, it is retained in a decommissioned state. When the number of days specified before purging is reached, data about the navigation link is removed. The On-demand app service also retains information about requests to generate and reload on-demand apps. When on-demand apps are deleted, the information about their reload requests is retained for the number of days specified before purging.
Allow anonymous user to generate apps	Allows anonymous users to generate on-demand apps from navigation points on published selection apps. This setting applies only on Qlik Sense systems that have set anonymous authentication. *Anonymous authentication (page 457)* An anonymous user can generate apps only from navigation links that are published automatically. If the generated app is not published automatically, the anonymous user would not have access to it.

Property	Description
The proxy user that will be used for generating apps on behalf of the anonymous users	Select a user to serve as a proxy user for anonymous users. Choose any registered user who can create on-demand app requests. The proxy user must also have read permission on the on-demand selection apps that are accessible to anonymous users. Do not select an administrative user (*INTERNAL\sa-xxx*) as the proxy or any user who has root admin privileges. ⚠ *When creating streams that will contain on-demand selection apps that can be used by anonymous users, you must set the security rule to permit read access to the on-demand app proxy user. Failure to include read access to the proxy user will cause all of the links in the app navigation bar to show as "Invalid".* Although a single user serves as the proxy for all anonymous users, each anonymous user is identified and distinguished by the On-Demand App Service. This allows each anonymous user access to the his generated apps but prevents other anonymous users from accessing those apps. Each anonymous user can access only apps she has generated.
Number of minutes to keep apps generated by anonymous users	Specifies the amount of time an app generated by an anonymous is kept before it is deleted. The default setting is 60 minutes. The time is measured from the last data load. There is also a retention time setting on navigation links. For an app generated by an anonymous user, the shorter of the two retention time settings is used. For example, when a navigation link with a retention time setting of 24 hours is used by an anonymous user and the setting for the **Number of minutes to keep apps generated by anonymous users** is set to 60 minutes, the app would be deleted 60 minutes after its last data load. If however the navigation link setting for retention time is 30 minutes, then the app generated by the anonymous user would be deleted 30 minutes after the last data load. ⚠ *If **Number of minutes to keep apps generated by anonymous users** is set to zero (0), then the apps are kept for the longest time possible, which is 365 days.*

Shutting down the On-demand app service

The On-demand app service is only turned off when Qlik Sense is shut down. To avoid turning off the service while requests are pending, you should notify users of the service that it will be turned off. To by sure you do not accidentally interrupt any app requests, you should disable the service and wait several minutes for any pending requests to finish before shutting down.

To find out if there are pending requests, a user with RootAdmin privileges can enter the following URL in a web browser's URL field:

https://yourhost.yourdomain.com/api/odag/v1/requests?state=qvhl&createdOnOrAfter=YYYY-MM-DDTHH:MI:SS.sssZ

where:

> *yourhost.yourdomain.com* is the URL for your Qlik Sense proxy.

and

> *YYY-MM-DDTHH:MI:SS.sssZ* is the timestamp of the first record in the most recent On-demand app service log file, which is the last time the service was started.

This will return an array of generating on-demand apps in JSON format. These are requests that have been started since the last time the On-demand app service was started but have not yet completed. If there are no pending requests, the response in the browser will appear as open and close square brackets:

> [ ]

When the service is restarted after the shutdown, it comes up in the state it was in when the shutdown occurred. If you disabled the service before shutting it down, you must enable it again after the service is restarted.

> ⚠ *If pending requests are cancelled because the On-demand app service has been forcibly shut down, those requests are lost and cannot be retrieved. They would have to be manually reentered when the service is restarted and enabled.*

On-demand app retention times

Retention times can be set for on-demand apps when a navigation link is created.

Retention times can be specified in hours or days, or they be set to never expire. All on-demand apps generated from the navigation link will be retained according to that setting. The age of a generated on-demand app is the difference between the current time and the time of the last data load. This calculation of an on-demand app's age is the same for published and unpublished apps. And if an on-demand app is published manually after it has been generated, the age calculation remains the same: it is based on the last data load of the generated app.

> ℹ *The retention time for apps generated by anonymous users is set in the On-Demand App Service. That setting overrides the retention time set on an on-demand app's navigation link. See the On-Demand App Service property **Number of minutes to keep apps generated by anonymous users property** above.*

The On-demand app service runs a sweep every ten minutes to remove on-demand apps whose retention period has expired. Because the sweep runs at 10-minute intervals, an on-demand app can remain active up to ten minutes longer than its retention setting. For example, if an app has a one-hour retention setting, and its retention period ends shortly after a sweep has run, it will remain active until the next sweep.

While the retention time is based on the navigation link's setting, the retention time does not change after the app is generated. If the owner of the navigation link changes the retention time, that change does not affect on-demand apps that have already been generated.

Ownership of on-demand apps

The owner of an on-demand app is the user who generated the app. That user does not become the owner until the app generation has completed. While an on-demand app is in the process of loading data, the owner is *INTERNAL\sa_api*. That is because the user normally does not have access to the data connection used by the template app. This means that the load script and all attached files (except images) are removed from the generated app where the user does not have access rights to the template app. Access to that data connection is restricted for security reasons.

If the on-demand app fails to generate completely, the QMC will show the owner of the app as *INTERNAL\sa_api*.

The ownership of generated apps changes when they are published. When a generated app is published, the owner of the app is the owner of the navigation link.

> *Anonymous users do not own generated apps because all apps generated by anonymous users must be published. An anonymous user cannot have access to an unpublished app. Apps generated by anonymous users are, however, tagged with identifiers associated with the anonymous user who generated them. That prevents an anonymous user from using apps generated by another anonymous user.*

Automatically publishing on-demand apps

Navigation links have a property that allows the link creator to specify a stream to which apps generated from the link are published automatically. The user creating the navigation links must have permission to publish to the target stream, and the user who generates the app must have read permission on the stream. If either permission is missing, the on-demand app will not generate.

> *Anonymous users can only use published apps, and they cannot publish the apps themselves. For those reasons, anonymous users can only generate apps from navigation links that publish apps automatically.*

A user who generates an on-demand app that is published to a stream cannot delete the app. Only the owner of the navigation link can delete the on-demand app from the stream.

Controlling reloads in a multi-node environment

Administrators can control where on-demand apps are reloaded in a multi-node environment. Load balancing rules are set by custom properties on the individual nodes. Custom properties can then be set on apps to direct them to use specific reload servers.

On-demand app generation is a three-step process:

1. The template app script is generated and validated, based on the current selections.
2. The template app is duplicated.
3. The app is reloaded by applying the script to the newly generated app.
   For duplication of the app, make sure to have a development node in the environment to create and duplicate apps. You can do this by setting **Node purpose** of the development node to **Development** or **Both**.

By default, on-demand apps are loaded on the reload nodes configured by the load balancing rules for the environment. However, custom properties can be set on template apps to control where apps linked to that template app are loaded.

Custom properties can also be applied to generated apps to direct them to specific reload nodes. The custom properties on generated apps can direct the apps to reload from different nodes than that which is specified for the template app from which they were generated. Custom properties are set for on-demand apps after they have been generated.

Managing streams

A stream enables users to read and/or publish apps, sheets, and stories. Users who have publish access to a stream create the content for that specific stream. The stream access pattern on a Qlik Sense site is determined by the security rules for each stream. By default, Qlik Sense includes two streams: **Everyone** and **Monitoring apps**.

An app can be published to only one stream. However, if you duplicate the app to create a copy, you can publish the copy to another stream. Apps can be moved between streams.

In the hub, streams with no apps—either empty streams or streams that do not show apps due to the existing security rules for a user—will not appear. After you publish an app, move it from another stream, or delete it, the list of streams will update dynamically and the stream will appear in the hub or be hidden depending on whether it contains at least one app. Changes outside of the hub, for example in QMC, will not trigger an update to the stream list in the hub.

> *All authenticated users have read and publish rights to the **Everyone** stream and all anonymous users read-only rights. Three of the predefined admin roles (RootAdmin, ContentAdmin, and SecurityAdmin), have read and publish rights to the Monitoring apps stream.*

> *It is not recommended to create rules that allow users to edit published apps in streams.*

Creating streams

You create a stream to let users read and/or publish apps, sheets, and stories. The security rules for a stream determine the privileges a user has in the stream. A stream must have at least one app for it to appear in the hub. Empty streams, or streams that do not show apps due to the existing security rules for a user, will not appear.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Streams** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Click ➕ **Create new** in the action bar.

4. Edit the properties.

Identification

Identification properties

Property	Description
Name	The name of the stream.
Owner	The owner of the stream. This property does not exist until the stream is created.

Tags

Tags properties

Property	Description
Tags	💡 *If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

Custom properties

> ℹ️ *If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

5. Click **Apply** in the action bar to create and save the stream.
   The **Create security rule** dialog opens.

6. Create security rules for the stream and click **Apply**.

> ℹ️ *When a stream is deleted, all associated security rules are deleted together with the stream. The associated security rules are available under **Associated items**.*

Editing streams

You can edit streams that you have update rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Streams** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
   Select the streams that you want to edit.
3. Click **Edit** in the action bar.
4. Edit the properties.

Identification

Identification properties

Property	Description
Name	The name of the stream.
Owner	The owner of the stream. This property does not exist until the stream is created.

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

Custom properties

> *If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

5. Click **Apply** in the action bar to apply and save changes.

Successfully updated is displayed at the bottom of the page.

Deleting streams

You can delete streams that you have delete rights to.

> ⚠ *Do not delete the **Monitoring apps** stream. If the stream is deleted, it is irrevocably gone. (RootAdmins, ContentAdmins, and SecurityAdmins can delete the stream.)*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Streams** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the streams that you want to delete.

4. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.

5. Click **OK**.

Creating access rights for streams

You create security rules to give access rights to the streams.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Streams** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the stream you want to create rules for and click **Edit**.
   The stream edit page opens.

4. Select **Security rules** under **Associated items**.
   The system rules overview is displayed.

5. Click ✚**Create associated rule** in the action bar.
   The **Create security rule** dialog opens.

6. Edit the security rule for administrative access of the stream:

   a. Edit the **Identification** properties:

      Identification properties

Field	Values
Name	Enter the name of the stream. Mandatory.
Disabled	Select to disable the rule. The rule is enabled by default.
Description	Enter a description for the rule.

   b. Edit the **Basic** properties:

      Operator descriptions

Field	Value
Operator	**Descriptions and examples**
=	This operator is not case sensitive and returns True if the compared expressions are exactly equal. **Example:** user.name = "a*" The user named exactly a* is targeted by the rule.

Field	Value
like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name like "a*"` All users with names beginning with an a are targeted by the rule..
!=	This operator is not case sensitive and returns True if the values in the compared expressions are not equal. **Example:** `user.name != resource.name` All resources that do not have the same name as the user are targeted by the rule.

7. Optionally, edit the **Advanced** properties and create the **Conditions** for the rule:
    1. Add a condition.
    2. Use the **Context** list to specify where the rule applies.
8. Click **Apply**.
   The dialog closes and the rule is added to the stream's security rules overview.

> *The security rule is also displayed on the **Security rules** overview page.*

> *When a stream is deleted, all associated security rules are deleted together with the stream. The associated security rules are available under **Associated items**.*

Managing data connections and extensions

Data connections

Data connections enable you to select and load data from a data source. All data connections are managed centrally from the QMC. Data connections are created in the Qlik Sense data load editor. The user who creates a data connection automatically becomes the owner of that connection and is, by default, the only user who can access the data connection. The data connection can be shared with others through security rules defined in the QMC.

When you import an app developed on Qlik Sense Desktop, existing data connections are imported to the QMC. When you export an app from a server, existing data connections are not exported with the app.

> *If the name of a data connection in the imported app is the same as the name of an existing data connection, the data connection will not be imported. This means that the imported app will use the existing data connection with an identical name, not the data connection in the imported app.*

Default security rules

Data folder connections are restricted by a default rule in the QMC. This security rule restricts the creation of data folder connections to the RootAdmin, ContentAdmin, and SecurityAdmin users. If you want to give a specific user permission to create data folder connections, create a new rule for that specific user. Do not change the default security rule because this can create security vulnerabilities, which could allow users to browse the folder structure.

Creating access rights for data connections (page 264)

Analytic connections

With analytic connections you are able to integrate external analysis with your business discovery. An analytic connection extends the expressions you can use in load scripts and charts by calling an external calculation engine (when you do this, the calculation engine acts as a server-side extension (SSE)). For example, you could create an analytic connection to R, and use statistical expressions when you load the data.

Analytic connections support up to 200 parameters.

Extensions

Extensions can be several different things: A widget library, a custom theme, or a visualization extension, used to visualize data, for example, in an interactive map where you can select different regions.

Editing data connections

Data connections are created in the Qlik Sense data load editor or when you use the **Add data** option. The user who created a data connection automatically becomes the owner of that connection and is by default the only user who can access the data connection.

You can edit data connections that you have update rights to. Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Data connections** on the QMC start page or from the **Start▼** drop-down menu to display the overview.

3. Select the data connections that you want to edit.

   > *If you select several data connections, you cannot view, edit or add security rules.*

4. Click **Edit** in the action bar.

5. Edit the properties.
   You can display or hide property groups using the panel to the far right.

Identification

Identification properties

Property	Description
Name	The name of the data connection.
Owner	The user name of the owner of the data connection.
Connection string	The connection string for the data connection. Typically, includes the name of the data source, drivers, and path.
Type	The type of data connection. Standard data connections include ODBC, OLEDB, and Folder.
User ID	The user ID that is used in the connection string.
Password	The password associated with the user ID used in the connection string.
	The password is saved encrypted.

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.*
	Connected tags are displayed under the text box.

Custom properties

*If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

6. Click **Apply** in the action bar.

Successfully updated data connection properties is displayed at the bottom of the page.

Deleting data connections

You can delete data connections that you have delete rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Data connections** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the data connections that you want to delete.

4. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.

5. Click **OK**.

Creating access rights for data connections

You create security rules to give access rights to the data connections. Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Data connections** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the data connection that you want to create rules for and click **Edit**.
   The data connection edit page opens.

4. Select **Security rules** under **Associated items**.

5. Click ➕**Create associated rule** in the action bar.
   The **Create security rule** dialog opens.

6. Edit the security rule for administrative access of the data connection:

   a. Edit the **Identification** properties:

   Identification fields and values

Field	Value
Name	Enter the name of the data connection. Mandatory.
Disabled	Select to disable the rule. The rule is enabled by default.
Description	Enter a description for the rule.

   b. In the **Advanced** section, use the drop-down to specify the context to which the rule will apply.

   c. In the **Basic** section, select the conditions for the rule using the following operators:

   Operator descriptions

Operator	Descriptions and examples
=	This operator is not case sensitive and returns True if the compared expressions are exactly equal. **Example:** `user.name = "a*"` The user named exactly a* is targeted by the rule.

like	This operator is not case sensitive and returns True if the compared expressions are equal.
	Example:
	`user.name like "a*"` All users with names beginning with an a are targeted by the rule.
!=	This operator is not case sensitive and returns True if the values in the compared expressions are not equal.
	Example:
	`user.name != resource.name` All resources that do not have the same name as the user are targeted by the rule.

7. Click **Apply**.
    The dialog closes and the rule is added to the security rules overview.

> *The security rule results in a corresponding security rule in the **Security rule** overview page.*

You have now created the access rights for the selected data connection.

Importing extensions

By default, only the RootAdmin user has the access rights to import extensions. You need to define security rules to enable others to import extensions. By default, all Qlik Sense users have access to all extensions that you add. Revise the security rule named *Extension* if you want to limit the access.

> ⚠️ *If you import an extension that already exists in QMC, when prompted, replace the existing file with the new one by clicking **Replace**, or click ✖ to cancel.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Extensions** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Click ➕ **Import** in the action bar.
4. The **Import extension file** dialog opens. Select a zip file to import.
    Remember to enter the password for the zip file if it is password protected.
5. Click **Open** in the file explorer window.
6. Click **Import**.

> *Extensions are saved to \\QlikShare\StaticContent\Extensions. The maximum file size is specified under Limitations in the following topic:* [Attaching data files and adding the data to the app](#)*. If the import of an extension fails, check the log files at %ProgramData%Qlik/Sense/Log/Repository/System.*

Extension names

If an extension already exists in QMC, upon import, you can replace it with the new one. When you replace an existing extension, the old files are overwritten by the new ones, however, the GUID of the extension and any associated items, for example, custom security rules, are not affected. If you choose not to replace the extension, you can rename the new extension by, at minimum, renaming the .qext file within the .zip file. However, to avoid name duplication later on, it is recommended that the .zip file, as well as the .qext file and the relevant .js files within the .zip file, all use the same file name.

By default, an extension that is imported is displayed in the **Extensions** overview. The name of the extension will be the same as the name of the .qext file. However, in the Qlik Sense hub, the extension is displayed with its regular file name that can also be changed by editing the Name field in the .qext file.

If you want to only display the file name in the **Extensions** overview, you must remove the *com-qliktech-* part from the .js file and the .qext file in the extension zip file.

> *A user can only change the name of an imported extension in the Dev Hub.*

> *Avoid importing widget libraries from the QMC, because when you do, no check is performed for duplicate library IDs and widget IDs. Import from the Dev Hub instead, where the check is performed automatically .*

Editing extensions

You can edit extensions that you have update rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Extensions** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select the extensions that you want to edit.
4. Click **Edit** in the action bar.
5. Edit the properties.

Identification

Identification properties

Property	Description
Name	The name of the extension is obtained from the file name of the extension definition file (*.qext*) in the uploaded zip file and cannot be modified.
Owner	The user name of the owner of the extension. ⓘ *This property is only visible when editing an extension.*

Tags

Tags properties

Property	Description
Tags	💡 *If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

Custom properties

ⓘ *If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

6. You can also edit the fields under **Associated items**.

Associated items

Associated items properties

Property	Description
User access	The preview shows a grid of the target resources and the source users who have access to the selected items.
Security rules	Displays the security rules for the extension.

7. Click **Apply** in the action bar.

Successfully updated is displayed at the bottom of the page.

The web browser caches the extensions for up to six hours. Users can manually clear the cache to access a new version of an extension.

Deleting extensions

You can delete extensions that you have delete rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Extensions** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select the extensions that you want to delete.
4. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
5. Click **OK**.

Creating an analytic connection

With analytic connections you are able to integrate external analysis with your business discovery. An analytic connection extends the expressions you can use in load scripts and charts by calling an external calculation engine (when you do this, the calculation engine acts as a server-side extension (SSE)). For example, you could create an analytic connection to R, and use statistical expressions when you load the data.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
   If you have more than one server, use the central server.
2. Select **Analytic connections** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Click ➕ **Create new** in the action bar.
4. Edit the properties.

Identification

Identification properties

Property	Description
Name	Name of the analytic connection. Must be unique and must not start with numbers. Mapping/alias to the plugin that will be used from within the expressions in the app using the plugin functions, for example, SSEPython for a Python plugin or R for an R plugin.
Host	Host of the analytic connection, for example, *localhost* if on the same machine or *mymachinename.qlik.com* if located on another machine.

Property	Description
Port	Port to use when connecting.
Certificate file path	The full path to the certificate: *C:\ProgramData\Qlik\Sense\Repository\Exported Certificates\<server name>*. The path should point to the folder containing both the client and server certificates and keys. This path just points to the folder where the certificates are located. You have to make sure that they are actually copied to that folder. The names of the three certificate files must be the following: *root_cert.pem*, *sse_client_cert.pem*, *sse_client_key.pem*. Only mutual authentication (server and client authentication) is allowed. ⓘ *It is optional to set the certificate file path, but the connection is insecure without a path.*
Reconnect timeout (seconds)	Default value: 20
Request timeout (seconds)	Default value: 0

Custom properties

> ⓘ *If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

5. Click **Apply** in the action bar to create and save the analytic connection.

> ⓘ ***Successfully added** is displayed at the bottom of the page.*

> ⓘ *Changes made to the settings in the QMC will override the settings in the Settings.ini file.*

Editing an analytic connection

With analytic connections you are able to integrate external analysis with your business discovery. An analytic connection extends the expressions you can use in load scripts and charts by calling an external calculation engine (when you do this, the calculation engine acts as a server-side extension (SSE)). For example, you could create an analytic connection to R, and use statistical expressions when you load the data.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Analytic connections** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select the analytic connections that you want to edit and click **Edit** in the action bar.
4. Edit the properties.

Identification properties

Property	Description
Name	Name of the analytic connection. Must be unique and must not start with numbers. Mapping/alias to the plugin that will be used from within the expressions in the app using the plugin functions, for example, SSEPython for a Python plugin or R for an R plugin.
Host	Host of the analytic connection, for example, *localhost* if on the same machine or *mymachinename.qlik.com* if located on another machine.
Port	Port to use when connecting.
Certificate file path	The full path to the certificate: *C:\ProgramData\Qlik\Sense\Repository\Exported Certificates\<server name>*. The path should point to the folder containing both the client and server certificates and keys. This path just points to the folder where the certificates are located. You have to make sure that they are actually copied to that folder. The names of the three certificate files must be the following: *root_cert.pem*, *sse_client_cert.pem*, *sse_client_key.pem*. Only mutual authentication (server and client authentication) is allowed. ⓘ *It is optional to set the certificate file path, but the connection is insecure without a path.*
Reconnect timeout (seconds)	Default value: 20
Request timeout (seconds)	Default value: 0

Custom properties

> ⓘ *If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

5. Click **Apply** in the action bar to save the analytic connection.

Successfully updated is displayed at the bottom of the page.

> **ⓘ** *Changes made to the settings in the QMC will override the settings in the Settings.ini file.*

Securing analytic connections

Consider the following best practices to strengthen the security of your Qlik Sense environment when using an analytic connection:

- Install and run the server-side extension (SSE) plugin in a separate, isolated environment without administrator rights. To minimize harm from a malicious script, be aware of which user account is starting the plugin and what access rights this user has in the machine and in the domain.
- For enhanced security, the EvaluateScript functionality can be disabled by setting the configuration parameter `allowScript` to false in the SSE plugin configuration file. This will prevent arbitrary scripts from being executed and allow only predefined functions to be run by the SSE plugin.
- Application developers creating Qlik Sense apps are advised to set any variables used in an SSE expression to a restricted format; for example, you can restrict a variable format to only numeric values.

Managing users

All user data is stored in the Qlik Sense Repository Service (QRS) database. You create user directory connectors in the QMC to be able to synchronize and retrieve the user data from a configured directory service. When a user logs in to Qlik Sense or the QMC, the user data is automatically retrieved.

Managing users in Qlik Sense involves:

- Creating new user directory connectors
- Synchronizing with user directories
- Managing access types
- Changing ownership of resources
- Removing resources owned by users
- Connecting administrative roles to a user
- Inactivating users
- Deleting users

Setting up a user directory connector and schedule by task

When you create a new instance of a User Directory Connector (UDC), a scheduled user synchronization task is created by default and initial synchronization is performed within five minutes. The user directory connector must be configured and operational to function.

If needed, you can change the default trigger for the user synchronization task and add more triggers. You can synchronize the user data manually from the user directory connectors overview.

The following workflow illustrates setting up a new user directory connector.

Flowchart:
- Log in to QMC
- Select User directory connectors (UDC)
- Create new UDC
- Configure UDC ← Check repository system log
- Check if UDC is operational — No → Check repository system log
- Yes
- Initial sync within 5 minutes
- Select Tasks
- Adapt user sync task by editing trigger
- Select Users and verify that users are imported
- User directory connector scheduled by task
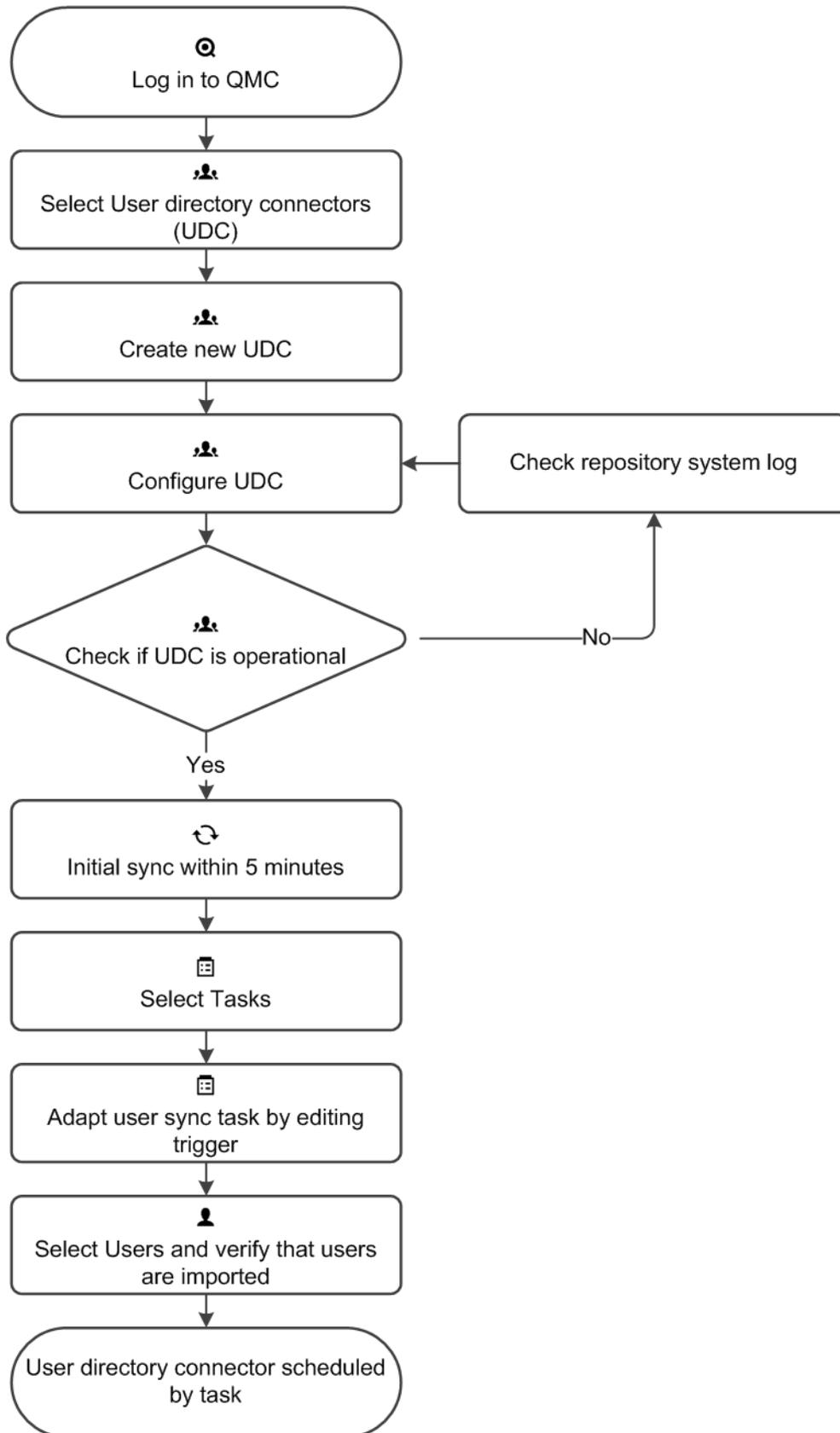
ODBC example

Each data source has a different configuration and the following are two examples (csv and SQL) of adding an ODBC user directory connector.

ODBC example (csv)

Do the following:

1. Verify that the Microsoft Access Text Driver is installed.
2. Set up an ODBC source on the server. You need to store the data in two separate csv files, for example, in this location: *%ProgramData%\Qlik\Sense\temp*.

   > *The temp folder is not included in the default installation. You need to create the temp folder, if not already done by another QMC administrator.*

   Table1.csv contains the users and *Table2.csv* the user attributes. The values in the csv files are comma separated.

   Example:

   Table1.csv contents:
   ```
   userid,name
   JoD,John Doe
   ```

   Table2.csv contents:
   ```
   userid,type,value
   JoD,email,jod@gmail.com
   ```
3. Open the QMC: *https://<QPS server name>/qmc*
4. Select **User directory connectors** on the QMC start page or from the **Start**▼ drop-down menu to display the overview. Create a new user directory connector (ODBC) and edit the properties.

   Identification
   All fields are mandatory and must not be empty.

   Identification properties

Property	Description
Name	The name of the UDC configuration, defined from the QMC.
Type	The UDC type.

   User sync settings

User sync property descriptions and values

Property	Description	Default value
Sync user data for existing users	• When selected, only the existing users are synchronized. An existing user is a user who has logged in to Qlik Sense and/or been previously synchronized from the configured directory service. • When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service. ℹ️ *The user attributes are only synced when a user logs in to the hub. Even if you delete the user in the QMC, the active session is still valid for the user that has been deleted. If the hub is only refreshed, the user is added to the database, but without any attributes.*	Selected

Connection

Property	Description	Default value
User directory name	The name of the user directory. Must be unique, otherwise the connector will not be configured. The name must not contain spaces.	-
Users table name	The name of the table containing the users. Include the file extension in the table name, for example: *Table.csv*.	-
Attributes table name	The name of the table containing the user attributes. Include the file extension in the table name, for example: *Table.csv*.	-

Property	Description	Default value

Visible connection string	The visible part of the connection string that is used to connect to the data source. Specify one of the following:
	
	• A full connection string, for example: *Driver={Microsoft Access Text Driver (*.txt, *.csv)};Extensions=asc,csv,tab,txt;Dbq=%ProgramData%\Qlik\Sense\temp*
	
	    ○ *Driver* must point to a driver currently on the machine. In the **ODBC Data Source Administrator**, check which driver to specify. Search for "data source" to find the application.
	    ○ *Dbq*: Path to the folder where the csv files are stored.
	
	• A pointer to an established System DSN, for example, *dsn=MyDSN;*
	
	ℹ️ *The two connection strings are concatenated into a single connection string when making the connection to the database.*
		-

Encrypted connection string	The encrypted part of the connection string that is used to connect to the data source. Typically, this string contains user name and password. ℹ️ *The two connection strings are concatenated into a single connection string when making the connection to the database.*	-
Synchronization timeout (seconds)	The timeout for reading data from the data source.	240

Example:

User table name: *Table1.csv*
Attributes table name: *Table2.csv*
Visible connections string: *Driver={Microsoft Access Text Driver (*.txt, *.csv)};Extensions=asc,csv,tab,txt;Dbq=%ProgramData%\Qlik\Sense\temp*

5. Click **Apply** to apply your changes.

6. Go to the **User directory connectors** overview and check if the user directory is displayed as **Configured** and **Operational**.

> ℹ️ *If the User directory name is not unique the connector will not be configured. If not operational, check the repository system log in:*
> *%ProgramData%\Qlik\Sense\Log\Repository\Trace.*

You have added an ODBC data source and initial synchronization will be performed within five minutes (by default).

ODBC example (SQL)

Do the following:

1. Create an SQL database with users. The database must consist of two tables, one with the users and one with the attributes of the users.

   Example:

   Table1: SQL users

   SQL users

Index	Value
1	ID,userid,name
2	1,JoD,John Doe

   Table2: SQL attributes

   SQL attributes

Index	Value
1	userid,type,value
2	JoD,email,jod@gmail.com

   > ℹ️ *If the user IDs are unique, the ID column is redundant.*

2. Install an SQL driver on the server, for example, SQL Server Native Client 11.0.

3. Open the QMC: *https://<QPS server name>/qmc*

4. Select **User directory connectors** on the QMC start page or from the **Start**▼ drop-down menu to display the overview. Create a new user directory connector (ODBC) and edit the properties.

   Identification
   All fields are mandatory and must not be empty.

Identification properties

Property	Description
Name	The name of the UDC configuration, defined from the QMC.
Type	The UDC type.

User sync settings

User sync properties, descriptions, and default values

Property	Description	Default value
Sync user data for existing users	• When selected, only the existing users are synchronized. An existing user is a user who has logged in to Qlik Sense and/or been previously synchronized from the configured directory service. • When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service. ⓘ *The user attributes are only synced when a user logs in to the hub. Even if you delete the user in the QMC, the active session is still valid for the user that has been deleted. If the hub is only refreshed, the user is added to the database, but without any attributes.*	Selected

Connection

Connection properties, descriptions and default values

Property	Description	Default value
User directory name	The name of the user directory. Must be unique, otherwise the connector will not be configured. The name must not contain spaces.	-

Property	Description	Default value
Users table name	The name of the table containing the users, for example, *UsersTable*. *When setting up an Oracle ODBC user directory connector, the **Users table name** and **Attributes table name** must be prefaced by the owner of those tables. For example: OWNER.USERS instead of only USERS.*	-
Attributes table name	The name of the table containing the user attributes, for example, *AttributesTable*. *When setting up an Oracle ODBC user directory connector, the **Users table name** and **Attributes table name** must be prefaced by the owner of those tables. For example: OWNER.USERS instead of only USERS.*	-

Property	Description	Default value

Visible connection string	The visible part of the connection string that is used to connect to the data source. Specify one of the following:
	
	• A full connection string, for example: *Driver={SQL Server Native Client 11.0};Server=localhost;Database=Users;Trusted_Connection=yes;*
	
	  1. *Driver* must point to a driver currently on the machine. In the **ODBC Data Source Administrator**, check which driver to specify. Search for "data source" to find the application.
	  2. *Server* must point to the server that you want to connect to.
	  3. *Database* must point to the database where the tables are.
	  4. *Trusted_Connection=yes* may be required, depending on the setup. In this example it is required.
	
	• A pointer to an established System DSN, for example, *dsn=MyDSN;*
	
	ℹ️ *The two connection strings are concatenated into a single connection string when making the connection to the database.*
		-

Encrypted connection string	The encrypted part of the connection string that is used to connect to the data source. Typically, this string contains user name and password. ℹ️ *The two connection strings are concatenated into a single connection string when making the connection to the database.*	-
Synchronization timeout (seconds)	The timeout for reading data from the data source.	240

Example:

User table name: *UsersTable*

Attributes table name: *AttributesTable*

Visible connections string: *Driver={SQL Server Native Client 11.0};Server=localhost;Database=Users;Trusted_Connection=yes;*

5. Click **Apply** to apply your changes.

6. Go to the **User directory connectors** overview and check if the user directory is displayed as **Configured** and **Operational**.

> ℹ️ *If the User directory name is not unique the connector will not be configured. If not operational, check the repository system log in:*
> *%ProgramData%\Qlik\Sense\Log\Repository\Trace.*

You have added an ODBC data source and initial synchronization will be performed within five minutes (by default).

ODBC example (Access)

Each data source has a different configuration and the following is an example (txt) of adding an ODBC user directory connector.

> ℹ️ *When loading .txt files using Microsoft Access Text Driver (*.txt, *.csv), you must use the connector type **Access (via ODBC)** instead of **ODBC**.*

Access (via ODBC) for txt and csv files

Do the following:

1. Verify that the Microsoft Access Text Driver is installed.

2. Set up an ODBC source on the server. You need to store the data in two separate txt files, for example, in this location: *%ProgramData%\Qlik\Sense\Temp*.

> ℹ️ *The temp folder is not included in the default installation. You need to create the temp folder, if not already done by another QMC administrator.*

Users.txt contains the users, and *Attributes.txt* the user attributes.

Example:

```
 Users.txt contains:
userid,name
JoD,John Doe


 Attributes.txt contains:
userid,type,value
JoD,email,jod@gmail.com
```

3. Open the QMC: *https://<QPS server name>/qmc*

---

4. Select **User directory connectors** on the QMC start page or from the **Start▼** drop-down menu to display the overview. Create a new user directory connector: **Access (via ODBC)** and edit the properties.

Identification

All fields are mandatory and must not be empty.

Identification properties

Property	Description
Name	The name of the UDC configuration, defined from the QMC.
Type	The UDC type.

User sync settings

User sync property descriptions and values

Property	Description	Default value
Sync user data for existing users	• When selected, only the existing users are synchronized. An existing user is a user who has logged in to Qlik Sense and/or been previously synchronized from the configured directory service. • When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service. ⓘ *The user attributes are only synced when a user logs in to the hub. Even if you delete the user in the QMC, the active session is still valid for the user that has been deleted. If the hub is only refreshed, the user is added to the database, but without any attributes.*	Selected

Connection

Connection property descriptions and values

Property	Description	Default value
User directory name	The name of the user directory. Must be unique, otherwise the connector will not be configured. The name must not contain spaces.	-
Users table name	The text file containing the users. Include the file extension in the table name, for example: *File.txt/File.csv*.	-

Property	Description	Default value
Attributes table name	The text file containing the user attributes. Include the file extension in the table name, for example: *File.txt/File.csv*.	-

Visible connection string	The visible part of the connection string that is used to connect to the data source. Specify one of the following:
	
	• A full connection string, for example: *Driver={Microsoft Access Text Driver (*.txt, *.csv)};Extensions=asc,csv,tab,txt;Dbq=C:\ProgramData\Qlik\Se nse\Temp*
	
	> ⓘ *In the default **Visible connection string**: Driver= {Microsoft Access Driver (*.mdb, *.accdb)};DBQ=C:\Database.accdb, you must replace name of the driver with Driver={Microsoft Access Text Driver (*.txt, *.csv)};DBQ=C:\ProgramData\Qlik\Sense\Temp, to be able to use txt and csv files.*
	
	   ○ *Driver* must point to a driver currently on the machine. In the **ODBC Data Source Administrator**, check which driver to specify. Search for "data source" to find the application.
	   ○ *DBQ*: Path to the folder where the txt files are stored.
	• A pointer to an established System DSN, for example, *dsn=MyDSN;*
	
	> ⓘ *The two connection strings are concatenated into a single connection string when making the connection to the database.*
		-

Encrypted connection string	The encrypted part of the connection string that is used to connect to the data source. Typically, this string contains user name and password. > ⓘ *The two connection strings are concatenated into a single connection string when making the connection to the database.*	-
Synchronizatio n timeout (seconds)	The timeout for reading data from the data source.	240

Example:

User table name: *Users.txt*
Attributes table name: *Attributes.txt*
Visible connections string: *Driver={Microsoft Access Text Driver (*.txt, *.csv)};Extensions=asc,csv,tab,txt;DBQ=C:\ProgramData\Qlik\Sense\Temp*

5. Click **Apply** to apply your changes.

6. Go to the **User directory connectors** overview and check if the user directory is displayed as **Configured** and **Operational**.

> *If the User directory name is not unique the connector will not be configured. If not operational, check the repository system log in:*
> *%ProgramData%\Qlik\Sense\Log\Repository\Trace.*

You have added an ODBC data source and initial synchronization will be performed within five minutes (by default).

Using Additional LDAP filter to retrieve specific users

You can create a user directory connector that will retrieve only specific users when synchronizing with user directories. To achieve this you use the property **Additional LDAP filter** when creating a new GenericLDAP or Active Directory user directory connector.

Example:

Enter a query in the **Additional LDAP filter** text field found in the **Advanced** property group. For example, you might want to import:

- all users named John: *(&(objectClass=user)(name=John*))*
- a specific user: *(&(objectClass=user)(sAMAccountName=userid))*
- more than one specific users: *(&(objectCategory=person)(objectClass=user)(|(sAMAccountName=userid)(sAMAccountName=userid)))*

Creating a user directory connector

You can create a new User Directory Connector (UDC).

> *The user directory must contain fewer than 1 000 000 (one million) total users and attributes. For large user directories, we recommend that you always select **Sync user data for existing users** in the **User sync settings** property group. Adding large numbers of users and user attributes may cause reloads of the Monitoring apps to fail.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **User directory connectors** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Click ➕ **Create new** in the action bar.
   The dialog with available user directory connector types is displayed.

4. Select the type for the new user directory connector and also the source. The following types are available:

   - Generic LDAP
   - Advanced LDAP
   - Active Directory
   - ApacheDS
   - ODBC
   - Access (through ODBC)
   - Excel (through ODBC)
   - SQL (through ODBC)
   - Teradata (through ODBC)

   > ℹ️ *No UDC is required for a local user to log on to Qlik Sense. However, for the local user to be able to access apps, you need to allocate access. With a user-based license, you can use professional or analyzer access rules. With a token-based license, you can use user or login access rules to allocate access. Alternatively, a local user can first log on to be recognized as a user, and then be allocated tokens.*

5. Edit the properties.

   Identification

   All fields are mandatory and must not be empty.

   Identification properties

Property	Description
Name	The name of the UDC configuration, defined from the QMC.
Type	The UDC type.

User sync settings

User sync properties

Property	Description	Default value
Sync user data for existing users	• When selected, only the existing users are synchronized. An existing user is a user who has logged in to Qlik Sense and/or been previously synchronized from the configured directory service. • When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service. You can create a filter to **Active Directory**, **ApacheDS**, **Generic LDAP**, or **Advanced LDAP**, if you only want to synchronize a selection of users. *The user attributes are only synced when a user logs in to the hub. Even if you delete the user in the QMC, the active session is still valid for the user that has been deleted. If the hub is only refreshed, the user is added to the database, but without any attributes.*	Selected

*Decide how the synchronization is performed by selecting or clearing **Sync user data for existing users**, in the property group **User sync settings**.*

Connection (Generic LDAP, Advanced LDAP, Active Directory, and ApacheDS)

Connection properties

Property	Description	Default value
User directory name	Must be unique, otherwise the connector will not be configured. The name of the UDC instance (to be compared to the domain name of an Active Directory). Together with the user's account name, this name makes a user unique. *Not entered manually for Active Directory.*	-

Property	Description	Default value
Path	The URI used to connect to the directory server. To support SSL, specify the protocol as LDAPS instead. ⓘ *Custom ports are not supported.*	ldap://company.domain.com
User name	The optional user ID used to connect to the directory server. If this is empty, the user running the Qlik Sense repository is used to log on to the directory server.	-
Password	The optional password for the user.	-

ⓘ *When a user creates an Active Directory connector, the connector will only work if the user running the Qlik Sense services is allowed to access the directory server. If the user running the Qlik Sense services is not allowed to access the directory server, a user name and a password that allows access to the directory server must be provided.*

Connection (ODBC) and (via ODBC)

ⓘ *When loading .txt files using Microsoft Access Text Driver (*.txt, *.csv), you must use the connector type **Access (via ODBC)** instead of **ODBC**.*

Connection properties

Property	Description	Default value
User directory name	The name of the user directory. Must be unique, otherwise the connector will not be configured. The name must not contain spaces.	-
Users table name	The name of the table containing the users. Include the file extension in the table name, for example: *Table.csv*. ⓘ *When setting up an Oracle ODBC user directory connector, the **Users table name** and **Attributes table name** must be prefaced by the owner of those tables. For example: OWNER.USERS instead of only USERS.*	-

Property	Description	Default value
Attributes table name	The name of the table containing the user attributes. Include the file extension in the table name, for example: *Table.csv*. ⓘ *When setting up an Oracle ODBC user directory connector, the **Users table name** and **Attributes table name** must be prefaced by the owner of those tables. For example: OWNER.USERS instead of only USERS.*	-

Visible connection string	The visible part of the connection string that is used to connect to the data source. Specify one of the following:
	
	• A full connection string, for example: *Driver={SQL Server Native Client 11.0};Server=localhost;Database=Users;Trusted_Connection=yes;*
	
	  1. *Driver* must point to a driver currently on the machine. In the **ODBC Data Source Administrator**, check which driver to specify. Search for "data source" to find the application.
	  2. *Server* must point to the server that you want to connect to.
	  3. *Database* must point to the database where the tables are.
	  4. *Trusted_Connection=yes* may be required, depending on the setup. In this example it is required.
	
	• A pointer to an established System DSN, for example, *dsn=MyDSN;*
	
	ⓘ *The two connection strings are concatenated into a single connection string when making the connection to the database.*
		-

Property	Description	Default value
Encrypted connection string	The encrypted part of the connection string that is used to connect to the data source. Typically, this string contains user name and password. **Example:** Assume that you have a connection string as follows: *Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;Uid=Admin;Pwd=verySecretAdminPassword;* You do not want to store that connection string in the database as it is, because the secret password would then be visible to others. To protect the password, do the following: Save the first part: *Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;* in the **Visible connection string** field, and the second part: *Uid=Admin;Pwd=verySecretAdminPassword;* in the **Encrypted connection string** field. The second part is then stored encrypted in the database and is not shown when you open the UDC again for editing. > *The two connection strings are concatenated into a single connection string when making the connection to the database.*	-
Synchronization timeout (seconds)	The timeout for reading data from the data source.	240

Advanced (Generic LDAP, Active Directory, and ApacheDS)
The **Advanced** property group contains the advanced LDAP connector properties in the Qlik Sense system.

Advanced properties

Property	Description	Default value
Additional LDAP filter	Used as the LDAP query to retrieve the users in the directory.	-
Synchronization timeout (seconds)	The timeout for reading data from the data source.	240

Property	Description	Default value
Page size of search	Determines the number of posts retrieved when reading data from the data source. When the specified number of posts have been found, search is stopped and the results are returned. When search is restarted, it continues where it left off. *If the user synchronization is unsuccessful, try setting the value to '0' (zero), which is equal to not doing a paged search.*	2000 (For ApacheDS: 1000)
Use optimized query	This property allows Qlik Sense to optimize the query for directories containing many groups in proportion to the number of users retrieved. *To be able to use the optimization, the directory must be set up so that the groups refer to the users. If the directory is not set up correctly, the optimized query will not find all groups connected to the users.* This property is only visible for Generic LDAP and Active directory search, (Active Directory always uses optimization).	Not selected
Authentication type	Optional. Authentication type to connect to LDAP. The values can be comma separated. Values: *Secure*, *Encryption*, *SecureSocketsLayer*, *ReadonlyServer*, *FastBind*, *Signing*, *Sealing*, *Delegation*, *ServerBind*. *To support "LDAP Channel Binding and LDAP Signing in Active Directory and Generic LDAP UDCs", use the following Authentication type values: Secure,Signing.*	*FastBind* or *Anonymous*, based on the credentials settings.

*Use the **Additional LDAP filter** in the property group **Advanced** to apply a filter that retrieves only a selection of the users.*

Advanced (Advanced LDAP)

The **Advanced** property group contains the advanced LDAP connector properties in the Qlik Sense system.

LDAP advanced properties

Property	Description	Default value
Page size	Determines the number of posts retrieved when reading data from the data source. When the specified number of posts have been found, search is stopped and the results are returned. When search is restarted, it continues where it left off. *If the user synchronization is unsuccessful, try setting the value to '0' (zero), which is equal to not doing a paged search.*	2000 (For ApacheDS: 1000)
Use optimized query	This property allows Qlik Sense to optimize the query for directories containing many groups in proportion to the number of users retrieved. *To be able to use the optimization, the directory must be set up so that the groups refer to the users. If the directory is not set up correctly, the optimized query will not find all groups connected to the users.* This property is only visible for Generic LDAP, Advanced LDAP, and Active directory search (Active Directory always uses optimization).	Not selected
Timeout (seconds)	The timeout for reading data from the data source.	400
Authentication type	Authentication type to connect to LDAP. Options: *Anonymous*, *Basic*, *Negotiate*, *NTLM*, *Digest*, *Sicily*, *DPA*, *MSN*, *External*, *Kerberos*.	-

Property	Description	Default value
Flags	Flags to mention LDAP connection session settings. Multiple values can be specified, comma separated. *Tcpkeepalive*: Enables TCP keep-alive. *Autoreconnect*: Enables Autoreconnect. *Rootdsecache*: Enables the internal RootDSE cache. *Sealing*: Enables Kerberos encryption. *Secure socket layer or ssl*: Enables secure socket layer on the connection. *Signing*: Enables Kerberos encryption. *Connectionless*: Specifies whether the connection is UDP. *No_fqdn*: Use this flag if host in the **Host** field is given as an IP address. *noclientcert*: Skip the default callback function used to specify client certificates when establishing an SSL connection. *NoCertVerify*: Skip server certificate verification when an SSL connection is established. *Don't use NoCertVerify and Certdebug together.* *Certdebug*: Get specific server certificate validation errors, if any, for debugging. *AllProps*: Fetch all attributes of the LDAP object.	-
Locator flags	Locator flag for DC locator. Multiple values can be specified, comma separated. *None* *ForceRediscovery* *DirectoryServiceRequired* *DirectoryServicePreferred* *GCRequired* *PdcRequired* *IPRequired* *KdcRequired* *TimeServerRequired* *WriteableRequired* *GoodTimeServerPreferred* *AvoidSelf* *OnlyLdapNeeded* *IsFlatName* *IsDnsName* *ReturnDnsName* *ReturnFlatName*	-

Property	Description	Default value
Search LDAP filter	Optional LDAP filter query.	-
Protocol version	LDAP protocol version to use.	3
Simple authentication and security layer (SASL) method	SASL Binding method: *gssapi* *external* *gss-spnego* *digest-md5*	-
Certificate path	Path of the client certificates to send for authentication.	-

Use the **Additional LDAP filter** in the property group **Advanced** to apply a filter that retrieves only a selection of the users.

Directory entry attributes (Generic LDAP and Advanced LDAP)

The directory entry attributes are case-sensitive.

Directory entry attribute properties

Property	Description	Default value
Type	The attribute name that identifies the type of directory entry (only users and groups are used by the LDAP UDC).	objectClass
User identification	The attribute value of the directory entry that identifies a user.	inetOrgPerson
Group identification	The attribute value of the directory entry that identifies a group.	group
Account name	The unique user name (within the UDC) that the user uses to log in.	sAMAccountName
Email	The attribute name that holds the emails of a directory entry (user).	mail
Display name	The full name of either a user or a group directory entry.	name

Property	Description	Default value
Group membership	The attribute indicates direct groups that a directory entry is a member of. Indirect group membership is resolved during the user synchronization. This setting, or the one below, **Members of directory entry**, is allowed to be empty, which means that the group membership is resolved using only one of the two settings.	memberOf
Members of directory entry	The attribute name that holds a reference to the direct members of this directory entry. See also the **Group membership** setting, above.	member
Custom attributes (only Advanced LDAP)	Extra LDAP object attributes to be retrieved. The custom attributes can be used in security rules and license assignment rules. Separate multiple custom attributes with commas. For an example of using custom attributes, see Qlik Sense Enterprise on Windows: How to sync custom attributes from Active Directory with Advanced LDAP.	-

Directory entry attributes (ApacheDS)

(i)	*The directory entry attributes are case-sensitive.*

Entry properties

Property	Description	Default value
Type	The attribute name that identifies the type of directory entry (only users and groups are used by the ApacheDS UDC).	objectClass
User identification	The attribute value of the directory entry that identifies a user.	inetOrgPerson
Group identification	The attribute value of the directory entry that identifies a group.	groupOfNames
Account name	The unique user name (within the UDC) that the user uses to log in.	uid
Email	The attribute name that holds the emails of a directory entry (user).	mail
Display name	The full name of either a user or a group directory entry.	cn

Property	Description	Default value
Group membership	The attribute name that indicates direct groups that a directory entry is a member of. Indirect group membership is resolved during the user synchronization. This setting or the one below, **Members of directory entry**, is allowed to be empty, which means that the group membership is resolved using only one of the two settings.	-
Members of directory entry	The attribute name that holds a reference to the direct members of this directory entry. See also the **Group membership** setting, above.	member

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.*
	Connected tags are displayed under the text box.

Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

6. Click **Apply** in the action bar to create and save the user directory connector.
   Successfully added is displayed at the bottom of the page.

You have now created a new user directory connector and a new *User synchronization task* is created by default for the new user directory connector.

The User Directory Connector (UDC) is not operational is displayed if the configuration of the connector properties does not enable communication with the user directory. Check the *UserManagement_Repository* log at this location: *%ProgramData%\Qlik\Sense\Log\Repository\Trace*.

The User Directory Connector (UDC) is not configured is displayed if the **User directory name** is already used or if the field is empty.

Editing a user directory connector

You can edit a user directory connector. You cannot edit more than one user directory connector at a time.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **User directory connectors** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the user directory connector that you want to edit and click **Edit** in the action bar.
   The edit page opens.

4. Edit the properties.

Identification

All fields are mandatory and must not be empty.

Identification properties

Property	Description
Name	The name of the UDC configuration, defined from the QMC.
Type	The UDC type.

User sync settings

User sync properties

Property	Description	Default value
Sync user data for existing users	• When selected, only the existing users are synchronized. An existing user is a user who has logged in to Qlik Sense and/or been previously synchronized from the configured directory service. • When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service. You can create a filter to **Active Directory**, **ApacheDS**, **Generic LDAP**, or **Advanced LDAP**, if you only want to synchronize a selection of users. *The user attributes are only synced when a user logs in to the hub. Even if you delete the user in the QMC, the active session is still valid for the user that has been deleted. If the hub is only refreshed, the user is added to the database, but without any attributes.*	Selected

*Decide how the synchronization is performed by selecting or clearing **Sync user data for existing users**, in the property group **User sync settings**.*

Connection (Generic LDAP, Advanced LDAP, Active Directory, and ApacheDS

Connection properties

Property	Description	Default value
User directory name	Must be unique, otherwise the connector will not be configured. The name of the UDC instance (to be compared to the domain name of an Active Directory). Together with the user's account name, this name makes a user unique. *Not entered manually for Active Directory.*	-
Path	The URI used to connect to the directory server. To support SSL, specify the protocol as LDAPS instead. *Custom ports are not supported.*	ldap://company.domain.com
User name	The optional user ID used to connect to the directory server. If this is empty, the user running the Qlik Sense repository is used to log on to the directory server.	-
Password	The optional password for the user.	-

When a user creates an Active Directory connector, the connector will only work if the user running the Qlik Sense services is allowed to access the directory server. If the user running the Qlik Sense services is not allowed to access the directory server, a user name and a password that allows access to the directory server must be provided.

Connection (ODBC) and (via ODBC)

When loading .txt files using Microsoft Access Text Driver (.txt, *.csv), you must use the connector type **Access (via ODBC)** instead of **ODBC**.*

Connection properties

Property	Description	Default value
User directory name	The name of the user directory. Must be unique, otherwise the connector will not be configured. The name must not contain spaces.	-
Users table name	The name of the table containing the users. Include the file extension in the table name, for example: *Table.csv*. *When setting up an Oracle ODBC user directory connector, the **Users table name** and **Attributes table name** must be prefaced by the owner of those tables. For example: OWNER.USERS instead of only USERS.*	-
Attributes table name	The name of the table containing the user attributes. Include the file extension in the table name, for example: *Table.csv*. *When setting up an Oracle ODBC user directory connector, the **Users table name** and **Attributes table name** must be prefaced by the owner of those tables. For example: OWNER.USERS instead of only USERS.*	-

Property	Description	Default value

Visible connection string	The visible part of the connection string that is used to connect to the data source. Specify one of the following:
	
	• A full connection string, for example: *Driver={SQL Server Native Client 11.0};Server=localhost;Database=Users;Trusted_ Connection=yes;*
	
	  1. *Driver* must point to a driver currently on the machine. In the **ODBC Data Source Administrator**, check which driver to specify. Search for "data source" to find the application.
	
	  2. *Server* must point to the server that you want to connect to.
	
	  3. *Database* must point to the database where the tables are.
	
	  4. *Trusted_Connection=yes* may be required, depending on the setup. In this example it is required.
	
	• A pointer to an established System DSN, for example, *dsn=MyDSN;*
	
	> *The two connection strings are concatenated into a single connection string when making the connection to the database.*
		-

Property	Description	Default value
Encrypted connection string	The encrypted part of the connection string that is used to connect to the data source. Typically, this string contains user name and password. **Example:** Assume that you have a connection string as follows: *Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;Uid=Admin;Pwd=verySecretAdminPassword;* You do not want to store that connection string in the database as it is, because the secret password would then be visible to others. To protect the password, do the following: Save the first part: *Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;* in the **Visible connection string** field, and the second part: *Uid=Admin;Pwd=verySecretAdminPassword;* in the **Encrypted connection string** field. The second part is then stored encrypted in the database and is not shown when you open the UDC again for editing. *The two connection strings are concatenated into a single connection string when making the connection to the database.*	-
Synchronization timeout (seconds)	The timeout for reading data from the data source.	240

Advanced (Generic LDAP, Active Directory, and ApacheDS)
The **Advanced** property group contains the advanced LDAP connector properties in the Qlik Sense system.

Advanced properties

Property	Description	Default value
Additional LDAP filter	Used as the LDAP query to retrieve the users in the directory.	-
Synchronization timeout (seconds)	The timeout for reading data from the data source.	240

Property	Description	Default value
Page size of search	Determines the number of posts retrieved when reading data from the data source. When the specified number of posts have been found, search is stopped and the results are returned. When search is restarted, it continues where it left off. 💡 *If the user synchronization is unsuccessful, try setting the value to '0' (zero), which is equal to not doing a paged search.*	2000 (For ApacheDS: 1000)
Use optimized query	This property allows Qlik Sense to optimize the query for directories containing many groups in proportion to the number of users retrieved. ⚠️ *To be able to use the optimization, the directory must be set up so that the groups refer to the users. If the directory is not set up correctly, the optimized query will not find all groups connected to the users.* This property is only visible for Generic LDAP and Active directory search, (Active Directory always uses optimization).	Not selected
Authentication type	Optional. Authentication type to connect to LDAP. The values can be comma separated. Values: *Secure*, *Encryption*, *SecureSocketsLayer*, *ReadonlyServer*, *FastBind*, *Signing*, *Sealing*, *Delegation*, *ServerBind*. ℹ️ *To support "LDAP Channel Binding and LDAP Signing in Active Directory and Generic LDAP UDCs", use the following Authentication type values: Secure,Signing.*	*FastBind* or *Anonymous*, based on the credentials settings.

💡 *Use the **Additional LDAP filter** in the property group **Advanced** to apply a filter that retrieves only a selection of the users (only applicable for LDAP and Active Directory).*

Advanced (Advanced LDAP)

The **Advanced** property group contains the advanced LDAP connector properties in the Qlik Sense system.

LDAP advanced properties

Property	Description	Default value
Page size	Determines the number of posts retrieved when reading data from the data source. When the specified number of posts have been found, search is stopped and the results are returned. When search is restarted, it continues where it left off. *If the user synchronization is unsuccessful, try setting the value to '0' (zero), which is equal to not doing a paged search.*	2000 (For ApacheDS: 1000)
Use optimized query	This property allows Qlik Sense to optimize the query for directories containing many groups in proportion to the number of users retrieved. *To be able to use the optimization, the directory must be set up so that the groups refer to the users. If the directory is not set up correctly, the optimized query will not find all groups connected to the users.* This property is only visible for Generic LDAP, Advanced LDAP, and Active directory search (Active Directory always uses optimization).	Not selected
Timeout (seconds)	The timeout for reading data from the data source.	400
Authentication type	Authentication type to connect to LDAP. Options: *Anonymous*, *Basic*, *Negotiate*, *NTLM*, *Digest*, *Sicily*, *DPA*, *MSN*, *External*, *Kerberos*.	-

Property	Description	Default value
Flags	Flags to mention LDAP connection session settings. Multiple values can be specified, comma separated. *Tcpkeepalive*: Enables TCP keep-alive. *Autoreconnect*: Enables Autoreconnect. *Rootdsecache*: Enables the internal RootDSE cache. *Sealing*: Enables Kerberos encryption. *Secure socket layer or ssl*: Enables secure socket layer on the connection. *Signing*: Enables Kerberos encryption. *Connectionless*: Specifies whether the connection is UDP. *No_fqdn*: Use this flag if host in the **Host** field is given as an IP address. *noclientcert*: Skip the default callback function used to specify client certificates when establishing an SSL connection. *NoCertVerify*: Skip server certificate verification when an SSL connection is established. *Don't use NoCertVerify and Certdebug together.* *Certdebug*: Get specific server certificate validation errors, if any, for debugging. *AllProps*: Fetch all attributes of the LDAP object.	-
Locator flags	Locator flag for DC locator. Multiple values can be specified, comma separated. *None* *ForceRediscovery* *DirectoryServiceRequired* *DirectoryServicePreferred* *GCRequired* *PdcRequired* *IPRequired* *KdcRequired* *TimeServerRequired* *WriteableRequired* *GoodTimeServerPreferred* *AvoidSelf* *OnlyLdapNeeded* *IsFlatName* *IsDnsName* *ReturnDnsName* *ReturnFlatName*	-

Property	Description	Default value
Search LDAP filter	Optional LDAP filter query.	-
Protocol version	LDAP protocol version to use.	3
Simple authentication and security layer (SASL) method	SASL Binding method: *gssapi* *external* *gss-spnego* *digest-md5*	-
Certificate path	Path of the client certificates to send for authentication.	-

Use the **Additional LDAP filter** in the property group **Advanced** to apply a filter that retrieves only a selection of the users.

Directory entry attributes (Generic LDAP and Advanced LDAP

The directory entry attributes are case-sensitive.

Directory entry attribute properties

Property	Description	Default value
Type	The attribute name that identifies the type of directory entry (only users and groups are used by the LDAP UDC).	objectClass
User identification	The attribute value of the directory entry that identifies a user.	inetOrgPerson
Group identification	The attribute value of the directory entry that identifies a group.	group
Account name	The unique user name (within the UDC) that the user uses to log in.	sAMAccountName
Email	The attribute name that holds the emails of a directory entry (user).	mail
Display name	The full name of either a user or a group directory entry.	name

Property	Description	Default value
Group membership	The attribute indicates direct groups that a directory entry is a member of. Indirect group membership is resolved during the user synchronization. This setting, or the one below, **Members of directory entry**, is allowed to be empty, which means that the group membership is resolved using only one of the two settings.	memberOf
Members of directory entry	The attribute name that holds a reference to the direct members of this directory entry. See also the **Group membership** setting, above.	member
Custom attributes (only Advanced LDAP)	Extra LDAP object attributes to be retrieved. The custom attributes can be used in security rules and license assignment rules. Separate multiple custom attributes with commas. For an example of using custom attributes, see ⤷ Qlik Sense Enterprise on Windows: How to sync custom attributes from Active Directory with Advanced LDAP.	-

Directory entry attributes (ApacheDS)

> ℹ️ *The directory entry attributes are case-sensitive.*

Entry properties

Property	Description	Default value
Type	The attribute name that identifies the type of directory entry (only users and groups are used by the ApacheDS UDC).	objectClass
User identification	The attribute value of the directory entry that identifies a user.	inetOrgPerson
Group identification	The attribute value of the directory entry that identifies a group.	groupOfNames
Account name	The unique user name (within the UDC) that the user uses to log in.	uid
Email	The attribute name that holds the emails of a directory entry (user).	mail
Display name	The full name of either a user or a group directory entry.	cn

Property	Description	Default value
Group membership	The attribute name that indicates direct groups that a directory entry is a member of. Indirect group membership is resolved during the user synchronization. This setting or the one below, **Members of directory entry**, is allowed to be empty, which means that the group membership is resolved using only one of the two settings.	-
Members of directory entry	The attribute name that holds a reference to the direct members of this directory entry. See also the **Group membership** setting, above.	member

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

5. Click **Apply** in the action bar to create and save the user directory connector.
   Successfully added is displayed at the bottom of the page.

You have now edited a user directory connector.

The User Directory Connector (UDC) is not operational is displayed if the configuration of the connector properties does not enable communication with the user directory. Check the *UserManagement_Repository* log at this location: *%ProgramData%\Qlik\Sense\Log\Repository\Trace*.

The User Directory Connector (UDC) is not configured is displayed if the **User directory name** is already used or if the field is empty.

Updating user directory types

You can change the user directory types that are available. To do this you need to update the source files before you create a new user directory connector.

If you remove the source file that a user directory connector is based on, it will not be operational.

Do the following:

1. Add or remove the user directory type source file located
   in: *%ProgramFiles%\Qlik\Sense\Repository\UserDirectoryConnectors*.
2. Open the QMC: *https://<QPS server name>/qmc*

3. Select **User directory connectors** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

4. Click **Update user directory types** in the action bar at the bottom of the page.
   Successfully updated user directory types from source is displayed at the bottom of the page.

You have now made the user directory types available for the user directory connectors.

Deleting user directory connectors and users

You can delete a user directory connector that you have delete rights to.

You have two deletion options:

- Deleting only the user directory connector
- Deleting the user directory connector and all the users that are imported from the user directory

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **User directory connectors** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

   > (i)   *You cannot delete more than one user directory connector at a time.*

3. Select the user directory connector that you want to delete.

4. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.

5. Optionally, select **Delete all users imported from this user directory**.

   > ⚠   *Deletion of the users cannot be undone.*

   Deleting the users moves the ownership of the owned resources to a service account (the sa_repository user).

6. Click **OK**.

Synchronizing with user directories

You can synchronize the user data from the user directories.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **User directory connectors** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Verify that the user directory connector is **Configured** and **Operational**.

> ⚠️ *If the user directory connector is not **Configured** or **Operational**, synchronization cannot be performed. The value of the **User directory** must be unique; otherwise the connector cannot be configured. Check the UserManagement_Repository log at this location: %ProgramData%\Qlik\Sense\Log\Repository\Trace.*

4. Before you start the synchronization you might want to check if all or only the existing users will be synchronized. Select the user directory connector, click **Edit** and look at the setting **Sync user data for existing users** under **User sync settings**:

    - When selected, only the existing users are synchronized. An existing user is a user who has logged in to Qlik Sense and/or been previously synchronized from the configured directory service.

    - When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service. You can create a filter to **Active Directory**, **ApacheDS**, **Generic LDAP**, or **Advanced LDAP**, if you only want to synchronize a selection of users.

> ℹ️ *The user attributes are only synced when a user logs in to the hub. Even if you delete the user in the QMC, the active session is still valid for the user that has been deleted. If the hub is only refreshed, the user is added to the database, but without any attributes.*

5. Go back to the overview by clicking on **User directory connectors** in the top left corner.

6. Select the user directory that you want to synchronize.

7. Click **Sync** in the in the action bar. **Starting synchronization of the selected user directories** is displayed at the bottom of the page. During the synchronization the **Status** column displays:

    a. **External fetch**

    b. **Database store**

    c. **Idle**

8. When **Idle** is displayed, verify that **Last successfully finished sync** date and time is updated.

> ℹ️ *If the status is displayed as **Idle** and **Last started sync** is more recent than **Last successfully finished sync**, the synchronization has failed.*

You have now synchronized the user data from the selected user directories. Select **Users** from the start page to display the updated user table.

Managing professional access

You allocate professional access to an identified user to give the user unlimited access to streams, apps, and other resources within a Qlik Sense site.

If you want to release a license to use it elsewhere, you can deallocate professional access. If the access type has been used within the last seven days, the access type is put in quarantine. If it has not been used within the last seven days, the professional access is removed and the license is released immediately.

You can reinstate quarantined professional access, to the same user, within seven days.

Allocating professional access

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select **Professional access allocations** in the panel to the right.
4. Click ➕ **Allocate** in the action bar.
   The **Users** dialog opens.
5. Select users in the list and click **Allocate**.

   > ℹ️ **Allocate** *is disabled if the number of licenses available for allocation is lower than the number of selected users.*

   The dialog is closed and the users are added in the **Professional access allocations** overview table.

Deallocating professional access

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select **Professional access allocations** in the panel to the right.
4. Select the users whose access you want to deallocate and click **Deallocate** in the action bar.
   A confirmation dialog is displayed..
5. Click **OK**.
   - The **Status** is changed to **Quarantined** if the user has logged in within the last seven days.
   - If the user has not logged in within the last seven days, the user is removed from the overview and the license is released.

Reinstating professional access

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select **Professional access allocations** in the panel to the right.
4. Select users with the status **Quarantined** and click **Reinstate** in the action bar.
   The status is changed to **Allocated**.

Creating a professional access rule

A professional access rule defines which users who have professional access to streams and apps.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select **Professional access rules** in the panel to the right.
4. Click ⊕ **Create new** in the action bar.
5. Edit the properties.

Identification

Identification properties

Property name	Description
Disabled	Select to disable the rule. By default, the rule is enabled.
Name	Name of the rule.
Description	Description of the rule.

Basic

Basic properties

Property name	Description
Resource filter	Definition of the types of resources for which the rule will be evaluated.
Actions	Actions that the rule will grant.

Advanced

Advanced properties

Property name	Description
Conditions	Resource conditions, user conditions, and combined conditions that need to be met for the rule to apply.
Validate rule	Click to validate the rule syntax.

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

6. Click **Apply** to create and save the user access rule.

Successfully added is displayed at the bottom of the page.

Editing a professional access rule

A professional access rule defines which users who have professional access to streams and apps. You can edit existing rules.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select **Professional access rules** in the panel to the right.
4. Select the rule you want to edit.
5. Click **Edit** in the action bar.
6. Edit the properties.

Identification

Identification properties

Property name	Description
Disabled	Select to disable the rule. By default, the rule is enabled.
Name	Name of the rule.
Description	Description of the rule.

Basic

Basic properties

Property name	Description
Resource filter	Definition of the types of resources for which the rule will be evaluated.
Actions	Actions that the rule will grant.

Operator descriptions and examples

Operator	Descriptions and examples
=	This operator is not case sensitive and returns True if the compared expressions are exactly equal. **Example:** user.name = "a*" The user named exactly a* is targeted by the rule.

like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name like "a*"` All users with names beginning with an a are targeted by the rule..
!=	This operator is not case sensitive and returns True if the values in the compared expressions are not equal. **Example:** `user.name != resource.name` All resources that do not have the same name as the user are targeted by the rule.

When using multiple conditions, you can group two conditions by clicking **Group**. After the conditions have been grouped, you have the option **Ungroup**. Additional subgrouping options are **Split** and **Join**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that AND is superior to OR.

Advanced

Advanced properties

Property name	Property
Conditions	Resource conditions, user conditions, and combined conditions that need to be met for the rule to apply.
Validate rule	Click to validate the rule syntax. Resource conditions, user conditions, and combined conditions that need to be met for the rule to apply.

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

Users

User properties

Property name	Description
Name	Name of the user.
Permitted action	Action that the user is allowed to perform.

7. Click **Apply** to save the updates.

Successfully added is displayed at the bottom of the page.

Managing analyzer access

You allocate analyzer access to an identified user to give the user access to streams, apps, and other resources within a Qlik Sense site.

If you want to release a license to use it elsewhere, you can deallocate analyzer access. If the access type has been used within the last seven days, the access type is put in quarantine. If it has not been used within the last seven days, the analyzer access is removed and the license is released immediately.

You can reinstate quarantined analyzer access, to the same user, within seven days.

Allocating analyzer access

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select **Analyzer access allocations** in the panel to the right.
4. Click ➕ **Allocate** in the action bar.
    The **Users** dialog opens.
5. Select users in the list and click **Allocate**.

    > ⓘ   *Allocate is disabled if the number of licenses available for allocation is insufficient for the number of selected users.*

    The dialog is closed and the users are added in the **Analyzer access allocations** overview table.

Deallocating analyzer access

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select **Analyzer access allocations** in the panel to the right.

4. Select the users whose access you want to deallocate and click **Deallocate** in the action bar.
    A confirmation dialog is displayed..

5. Click **OK**.

    - The **Status** is changed to **Quarantined** if the user has logged in within the last seven days.

    - If the user has not logged in within the last seven days, the user is removed from the overview and the license is released.

Reinstating analyzer access

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select **Analyzer access allocations** in the panel to the right.

4. Select users with the status **Quarantined** and click **Reinstate** in the action bar.
    The status is changed to **Allocated**.

Creating an analyzer access rule

An analyzer access rule defines which users who have analyzer access to streams and apps.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select **Analyzer access rules** in the panel to the right.

4. Click ⊕ **Create new** in the action bar.

5. Edit the properties.

Identification

Identification properties

Property name	Description
Disabled	Select to disable the rule. By default, the rule is enabled.
Name	Name of the rule.
Description	Description of the rule.

Basic

Basic properties

Property name	Description
Resource filter	Definition of the types of resources for which the rule will be evaluated.
Actions	Actions that the rule will grant.

Advanced

Advanced properties

Property	Description
Conditions	Resource conditions, user conditions, and combined conditions that need to be met for the rule to apply.
Validate rule	Click to validate the rule syntax.

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

6. Click **Apply** to create and save the user access rule.
   Successfully added is displayed at the bottom of the page.

Editing an analyzer access rule

An analyzer access rule defines which users who have analyzer access to streams and apps. You can edit existing rules.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select **Analyzer access rules** in the panel to the right.
4. Select the rule you want to edit.
5. Click **Edit** in the action bar.
6. Edit the properties.

   ### Identification

   Identification properties

Property name	Description
Disabled	Select to disable the rule. By default, the rule is enabled.
Name	Name of the rule.
Description	Description of the rule.

Basic

Basic properties

Property name	Description
Resource filter	Definition of the types of resources for which the rule will be evaluated.
Actions	Actions that the rule will grant.

Operator descriptions

Operator	Descriptions and examples
=	This operator is not case sensitive and returns True if the compared expressions are exactly equal. **Example:** `user.name = "a*"` The user named exactly a* is targeted by the rule.
like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name like "a*"` All users with names beginning with an a are targeted by the rule..
!=	This operator is not case sensitive and returns True if the values in the compared expressions are not equal. **Example:** `user.name != resource.name` All resources that do not have the same name as the user are targeted by the rule.

When using multiple conditions, you can group two conditions by clicking **Group**. After the conditions have been grouped, you have the option **Ungroup**. Additional subgrouping options are **Split** and **Join**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that AND is superior to OR.

Advanced

Advanced properties

Property name	Property
Conditions	Resource conditions, user conditions, and combined conditions that need to be met for the rule to apply.

Validate rule	Click to validate the rule syntax. Resource conditions, user conditions, and combined conditions that need to be met for the rule to apply.

Tags

Tags properties

Property	Description
Tags	If no tags are available, this property group is empty.
	Connected tags are displayed under the text box.

Users

User properties

Property name	Description
Name	Name of the user.
Permitted action	Action that the user is allowed to perform.

7. Click **Apply** to save the updates.

Successfully added is displayed at the bottom of the page.

Creating and editing an analyzer capacity rule

An analyzer capacity rule defines which users who have analyzer capacity access to streams and apps.

Do the following:

1. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
2. Select **Analyzer capacity rules** in the panel to the right.
3. Do one of the following:
   - Click ⊕ **Create new** in the action bar.
   - Select a rule and click **Edit**.
4. Edit the properties.

Identification

By default, the rule is enabled.

Basic

Basic properties

Property name	Description
Resource filter	Definition of the types of resources for which the rule will be evaluated.
Actions	Actions that the rule will grant.

Advanced

Advanced properties

Field	Value
Conditions	Resource conditions, user conditions, and combined conditions that need to be met for the rule to apply.
Validate rule	Click to validate the rule syntax.

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.*
	Connected tags are displayed under the text box.

5. Click **Apply** to save the analyzer capacity rule.

Managing user access

You allocate user access to an identified user to give the user unlimited access to streams, apps, and other resources within a Qlik Sense site.

If you want to release tokens to use them elsewhere, you can deallocate user access. If the access type has been used within the last seven days, the access type is put in quarantine. If it has not been used within the last seven days, the user access is removed and the tokens are released immediately.

You can reinstate quarantined user access, to the same user, within seven days. Then the user is given access again without using more tokens.

Allocating user access

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select **User access allocations** in the panel to the right.

4.   Click ⊕ **Allocate** in the action bar.
     The **Users** dialog opens.

5.   Select users in the list and click **Allocate**.

> ⓘ   *Allocate is disabled if the number of tokens available for allocation is insufficient for the number of selected users.*

The dialog is closed and the users are added in the **User access allocations** overview table.

Deallocating user access

Do the following:

1.   Open the QMC: *https://<QPS server name>/qmc*

2.   Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3.   Select **User access allocations** in the panel to the right.

4.   Select the users whose access you want to deallocate and click **Deallocate** in the action bar.
     A confirmation dialog is displayed..

5.   Click **OK**.

     - The **Status** is changed to **Quarantined** if the user has logged in within the last seven days.
     - If the user has not logged in within the last seven days, the user is removed from the overview and the tokens are released.

     Also, the information on the **Tokens** page is updated.

Reinstating user access

Do the following:

1.   Open the QMC: *https://<QPS server name>/qmc*

2.   Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3.   Select **User access allocations** in the panel to the right.

4.   Select users with the status **Quarantined** and click **Reinstate** in the action bar.
     The status is changed to **Allocated**. Also, the information on the **Tokens** page is updated.

Creating an analyzer access rule

An analyzer access rule defines which users who have analyzer access to streams and apps.

Do the following:

1.   Open the QMC: *https://<QPS server name>/qmc*

2.   Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3.   Select **Analyzer access rules** in the panel to the right.

4. Click ⊕ **Create new** in the action bar.
5. Edit the properties.

Identification

Identification properties

Property name	Description
Disabled	Select to disable the rule. By default, the rule is enabled.
Name	Name of the rule.
Description	Description of the rule.

Basic

Basic properties

Property name	Description
Resource filter	Definition of the types of resources for which the rule will be evaluated.
Actions	Actions that the rule will grant.

Advanced

Advanced properties

Property	Description
Conditions	Resource conditions, user conditions, and combined conditions that need to be met for the rule to apply.
Validate rule	Click to validate the rule syntax.

Tags

Tags properties

Property	Description
Tags	💡 *If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

6. Click **Apply** to create and save the user access rule.
   Successfully added is displayed at the bottom of the page.

Creating a user access rule

A user access rule defines which users that have access to the available tokens.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select **User access rules** in the panel to the right.
4. Click ➕ **Create new** in the action bar.
5. Edit the properties.

Identification

Identification properties

Property name	Description
Disabled	Select to disable the rule. By default, the rule is enabled.
Name	Name of the rule.
Description	Description of the rule.

Basic

Identification properties

Property name	Description
Resource filter	Definition of the types of resources for which the rule will be evaluated.
Actions	Actions that the rule will grant.

Advanced

Advanced properties

Property name	Description
Conditions	Resource conditions, user conditions, and combined conditions that need to be met for the rule to apply.
Validate rule	Click to validate the rule syntax.

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

6. Click **Apply** to create and save the user access rule.
    Successfully added is displayed at the bottom of the page.

> *If a user access rule is deleted, and there are currently users with tokens allocated due to this rule, these tokens will not automatically be unallocated. They have to be unallocated manually.*

The users named in the rule have access to the application as long as access tokens are available.

Editing a user access rule

A user access rule defines which users that have access to the available tokens. You can edit existing rules.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select **User access rules** in the panel to the right.
4. Select the rule you want to edit.
5. Click **Edit** in the action bar.
6. Edit the properties.

Identification

Identification properties

Property name	Description
Disabled	Select to disable the rule. By default, the rule is enabled.
Name	Name of the rule.
Description	Description of the rule.

Basic

Basic properties

Property name	Description
Resource filter	Definition of the types of resources for which the rule will be evaluated.
Actions	Actions that the rule will grant.

Operator descriptions

Operator	Descriptions and examples

=	This operator is not case sensitive and returns True if the compared expressions are exactly equal. **Example:** `user.name = "a*"` The user named exactly a* is targeted by the rule.
like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name like "a*"` All users with names beginning with an a are targeted by the rule..
!=	This operator is not case sensitive and returns True if the values in the compared expressions are not equal. **Example:** `user.name != resource.name` All resources that do not have the same name as the user are targeted by the rule.
When using multiple conditions, you can group two conditions by clicking **Group**. After the conditions have been grouped, you have the option **Ungroup**. Additional subgrouping options are **Split** and **Join**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that AND is superior to OR.	

Advanced

Advanced properties

Property name	Property
Conditions	Resource conditions, user conditions, and combined conditions that need to be met for the rule to apply.
Validate rule	Click to validate the rule syntax. Resource conditions, user conditions, and combined conditions that need to be met for the rule to apply.

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

Users

User properties

Property name	Description
Name	The name of the user.
Permitted action	The action that the user is allowed to perform.

7. Click **Apply** to save the updates.
   Successfully added is displayed at the bottom of the page.

> *If a user access rule is deleted, and there are currently users with tokens allocated due to this rule, these tokens will not automatically be released. They have to be released manually.*

The users named in the rule have access to the application as long as access tokens are available.

Deleting user access rules

You can delete user access rules that you have delete rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
3. Select **User access rules** in the panel to the right.
4. Select the rules that you want to delete.
5. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
6. Click **OK**.

Creating login access rules

A login access pass allows an identified or anonymous user to access the hub for a maximum of 60 continuous minutes per 28-day period. If the user exceeds the 60-minute time limitation, the user connection does not time out. Instead, another login access pass is used. If no more login access passes are available, the session is discontinued.

When you create a new login access rule, you set the following:

- The number of tokens that you want to allocate, providing for a number of login access passes.
- The license rule specifying which users the login access rule is available for.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **License management** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select **Login access rules** in the panel to the right.

4. Click ⊕ **Create new** in the action bar.

5. Edit the properties.

Identification

The **Name** is the name of the login access group.

Tokens

Allocated tokens represents the number of tokens that the login access group can use.

6. Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

> 🛈   The **Create license rule** *dialog opens, see Creating a license rule (page 329).*

If the number of available tokens is not enough, an error dialog is displayed. Reduce the **Number of tokens** and click **Apply** again.

Editing login access rules

You can edit login access rules that you have update rights to, and make changes to the following:

- The number of allocated tokens, providing for a number of login access passes.
- The license rule specifying which users the login access rule is available for.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select **Login access rules** in the panel to the right.

4. Select the login access rule you want to edit and click **Edit** in the action bar.

5. Edit the properties.

Identification

The **Name** is the name of the login access group.
You can change the name for the login access:

Tokens

Allocated tokens represents the number of tokens that the login access group can use.
You can change the number of tokens you want to allocate. The message below the field displays the number of login access passes that the number of tokens provide after you have clicked **Apply**.
Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

6. You can also edit the fields under **Associated items**:
   User access
   User access is available from **Associated items** when you edit a resource.
   The preview shows a grid of the target resources and the source users who have access to the selected items.
   Depending on rights, you can either edit or view a user, a resource, or an associated rule.
   License rules
   Editing a license rule (page 331)
7. Click **Apply**.
8. If the number of available tokens is not enough, an error dialog is displayed. Reduce the **Number of tokens** and click **Apply** again.

Deleting login access rules

You can delete login access rules that you have delete rights to, to release tokens. By doing this access to streams and apps are removed for the users in the login access group.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
3. Select **Login access rules** in the panel to the right to display the overview.
4. Select the login access rules that you want to delete.
5. Click **Delete** in the action bar.A **Delete** dialog is displayed.
6. Click **OK**.
   - Tokens are released immediately if the login access contains enough numbers of unused login access passes.
   - Used login access passes will not be released until 28 days after last use.

   Example:

   You have allocated 3 tokens, providing for 30 login access passes. 11 login access passes have been used. If you delete the login access, 1 token is released immediately and 2 tokens will not be released until 28 days after last use. This means that the second token is released 28 days after last use of the 10th login access pass and the third token is released 28 days after last use of the 11th login access pass.
   Also, the information on the **Tokens** page is updated.

Login access: Token consumption example

With a token-based Qlik Sense license, you buy tokens and allocate and reallocate the tokens to adapt to changing usage needs over time. You allocate tokens to either named individuals who need frequent access to the system, or to groups of users who use the system less frequently.

Allocating tokens

There are two alternatives for token allocation: user access or login access.

Token allocation descriptions

Token allocation	Access pass description
1 token = 1 user access pass	Assigned to a unique and identified named user with unlimited use of Qlik Sense as authorized by your organization's security policies and rules.
1 token = 10 login access passes	Used for infrequent or anonymous access. The login access pass provides full access to Qlik Sense but for a limited time.

Login access passes

User access passes are straightforward: one token is used for a dedicated user. Login access passes can be shared between different users, and therefore there are more possible scenarios that may require explanation. The following example shows how login access passes are consumed and later returned to the pool for new consumption.

Login access pass descriptions

Day #	Login access pass consumption	Description
Day 0		Let's assume that you allocate one token to a group. This gives the group 10 available login access passes.
Day 1		A user assigned to that group logs into Qlik Sense, which immediately consumes one login access pass.

Day 1		When the user remains active after the first 60 minutes, a second login access pass is consumed. This hourly process continues until the session ends, which can happen in three different ways: • The user logs out. • The user closes the browser (not just the tab). • The user is inactive longer than the timeout in the QMC. (Virtual proxy setting **Session inactivity timeout (minutes)**, 30 minutes by default.)
Day 15		A couple of weeks later, the user logs in again and this time uses Qlik Sense for under an hour to do a presentation using both a tablet and a laptop connected to a presentation screen. Because she is an identified user (that is, not anonymous), this only uses one login access pass. In fact, an identified user can access Qlik Sense on up to five concurrent devices during their session with no additional login access passes being consumed. This does not apply in the case of anonymous users as, by their very nature, the sessions cannot be linked together.

| Day 25 | | More than a week later, the user logs in again, using a fourth pass. However, this time she logs out after 30 minutes and then logs in and out again a few minutes later to quickly verify some information. Since the connection to the server occurs within the same hour, only one login access pass is consumed. |

In this example, it is clear that a login access suits the user best, rather than a user access. Nearly a month has gone by and only four login access passes have been consumed. Therefore, two users with this profile could be supported at the cost of one token.

Returning login access passes to the session pool

This section explains how login access passes are returned to the pool. Each login access pass becomes available again 28 days after it was first used.

Login pass consumption descriptions

Day #	Login access pass consumption	Description
Day 29		When 28 days have passed since the start of the scenario above, the first two login access passes become available for use again.
Day 43		When 28 days have passed from the time of the user's second login, that login access pass becomes available for use again.
Day 54		Finally, when 28 days have passed from the last login, all login access passes are available.
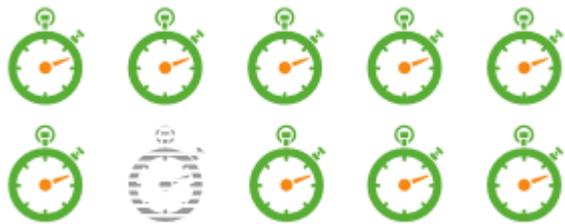
Estimating the number of tokens you need

To estimate the appropriate number of tokens, you need to identify the needs of different users. Front line managers, business analysts, executives, data engineers, and general knowledge workers all have different needs.

For the sake of simplicity, assume that the users in this example on average consume four login access passes per month. In addition, you need a buffer, because you do not know the exact number of times a user will actually log in each month. In this example, the buffer is 20%.

As mentioned earlier, 1 token equals 10 login access passes. The number of tokens needed could then be calculated as follows:

*[The number of people] * [Estimated number of login access passes per person] * [buffer] /10 = Tokens needed*

Assume that there are 103 users. The calculation would then be as follows:

*103 * 4 * 1,2 /10 = 49.4*

You cannot buy a fraction of a token, so round this up to 50 tokens.

Creating a license rule

You create a license rule to specify for which users a login access rule is available. It is possible to have a login access rule without a license rule, but in that case, the login access rule is applied globally across the system, and that is not recommended.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select **Login access rules** in the panel to the right.
4. Select a login access rule and click **Edit**.

   > ℹ️ *To create a new login access rule, see: Creating login access rules (page 323).*

5. Under **Associated items**, select **License rules**.
6. Click **Create associated rule**.
7. Edit the license rules as needed:

a. **Identification**

Login access identification rules

Rule	Description
Disabled	Rule toggle. (Disabled by default)
Name	The name of the login access rule. (Mandatory)
Description	The description of the rule.

b. **Basic**

If you change the **Resource filter**, the rule may not work as intended.

The option **Allow access** is automatically selected.

Operator descriptions

Operator	Descriptions and examples
=	This operator is not case sensitive and returns True if the compared expressions are exactly equal. **Example:** `user.name = "a*"` The user named exactly a* is targeted by the rule.
like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name like "a*"` All users with names beginning with an a are targeted by the rule.
!=	This operator is not case sensitive and returns True if the values in the compared expressions are not equal. **Example:** `user.name != resource.name` All resources that do not have the same name as the user are targeted by the rule.

c. **Advanced**

Define the resource, user, or combined **Conditions** that the rule should apply to.

8. Optionally, edit the **Advanced** properties and create the **Conditions** for the rule.

9. Click **Apply** to create and save the license rule.
The license rule was successfully added to the associated items is displayed at the bottom of the page.

Editing a license rule

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select **Login access rules** in the panel to the right.
4. Select a login access rule and click **Edit**.
5. Under **Associated items**, select **License rules**.
6. Select a license rule and click **Edit**.

   Edit the license rule as needed:

   a. **Identification**

   Login access identification rules

Rule	Description
Disabled	Rule toggle. (Disabled by default)
Name	The name of the login access rule. (Mandatory)
Description	The description of the rule.

   b. **Basic**

   If you change the **Resource filter**, the rule may not work as intended.

   > ℹ️ *The option **Allow access** is automatically selected.*

   Operator descriptions and examples

Operator	Descriptions and examples
=	This operator is not case sensitive and returns True if the compared expressions are exactly equal. **Example:** `user.name = "a*"` The user named exactly a* is targeted by the rule.

like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name like "a*"` All users with names beginning with an a are targeted by the rule.
!=	This operator is not case sensitive and returns True if the values in the compared expressions are not equal. **Example:** `user.name != resource.name` All resources that do not have the same name as the user are targeted by the rule.

   c. **Advanced**

     Conditions allow you to define the resource, user, or combined **conditions** that the rule should apply to.

7. Optionally, edit the **Advanced** properties and create the **Conditions** for the rule.
8. Click **Apply** to create and save the license rule.

Successfully updated the associated license rule is displayed at the bottom of the page.

Starting user sync tasks

You can manually start user synchronization tasks from the user directory connector's association page.

> 💡 *You can also start user synchronization tasks from the task overview page or by a scheduled trigger.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **User directory connectors** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select the user directory connector that you want to start tasks for and click **Edit** in the action bar.

> ℹ️ *The panel to the far left lists your selections.*

4. Select **Tasks** under **Associated items**.
   The **User synchronization tasks** overview is displayed.
5. Select the tasks that you want to start and click **Start** in the action bar.
   x out of x items were successfully instructed to start is displayed at the bottom of the page.

Editing user sync tasks

You can edit user synchronization tasks from the user directory connector association page.

> *You can also edit user synchronization tasks from the tasks overview page.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **User directory connectors** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select the user directory connector that you want to edit tasks for and click **Edit** in the action bar.
4. Select **Tasks** under **Associated items**, select the tasks you want to edit and click **Edit** in the action bar. The **User synchronization task edit** page is displayed.
5. Edit the properties.

   ### Identification

   All fields are mandatory and must not be empty.

   Identification properties

Property	Description	Default value
Name	The name of the task.	Auto-generated from the user directory connector name when creating a new user directory connector.
Enabled	The task is enabled when selected.	Enabled

   Select or clear **Enabled** to enable or disable the task.

   ### Tags

   Tags properties

Property	Description
Tags	> *If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

6. Click **Apply** in the action bar to apply and save your changes.
   Successfully updated is displayed at the bottom of the page.

> *Triggers for a task are displayed under **Associated items**, where you also can choose to create new triggers.*

Creating triggers for user sync tasks - scheduled

You can create one or more scheduled triggers for a task. The trigger executes the task once, or repeats the task within a time period defined by start and end, or repeats the task infinitely.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the task you want to add a trigger on and click **Edit** in the action bar at the bottom of the page.

4. Select **Triggers** under **Associated items**.
    The **Triggers** overview is displayed.

5. Click ✚ **Create associated trigger** in the action bar.
    The **Trigger - Start on schedule** dialog is displayed.

6. Edit the fields in the dialog to set the trigger conditions.

Scheduled trigger properties

Property	Description
Trigger name	Name of the trigger. Mandatory.
Enabled	Status of the trigger. When selected, the trigger is active.
Time zone	The time zone of your operating system, at the time you create the trigger. When you save a trigger, the settings are kept, and if you move to a different time zone, the original values are still displayed. If you want to change the time zone and start time of a trigger, you need to do that manually. *For a trigger that was created before the introduction of the time zone setting, all times and dates are by default presented in Coordinated Universal Time (UTC).*

Property	Description
Daylight saving time	Way to account for daylight saving time. **Observe daylight saving time**: This option takes daylight saving time (DST) into account. If DST is in use in the selected time zone, the execution time and date are adjusted accordingly. **Permanent standard time**: This option does not take DST into account. If DST is in use in the selected time zone, the execution time and date are not adjusted. **Permanent daylight saving time**: This option takes DST into account. If a time zone uses DST, execution time and date are always according to DST, even during periods when DST is not in use. ⓘ *For time zones not using DST, always select **Permanent standard time***. **Example:** You created a trigger for an event at 10:00 AM, while you were working in Ottawa, Canada, in January. The time zone is (GMT-0500) Eastern Time (US & Canada) and DST is used between March and November. If you select **Observe daylight saving time**, a trigger set to start at 10:00 will always start at 10.00. If you select **Permanent standard time**, a trigger set to run at 10:00 will run at 10:00 in the winter but at 09:00 in the summer. If you select **Permanent daylight saving time**, a trigger set to run at 10:00 will run at 11:00 in the winter and at 10:00 in the summer.
Start	Start time and date: • Start time: **(hh:mm)** • Start date: **(YYYY-MM-DD)**

Property	Description

Schedule	Frequency of the trigger:
	
	 • **Once**.
	
	 • **Hourly**. Time period between executions of the trigger. Edit **Repeat after each** by typing the values for:
	    • **hour(s)** (default is 1)
	    • **minute(s)** (default is 0)
	
	 • **Daily**. Time period between executions of the trigger. Type a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	
	 • **Weekly**. Time period between executions of the trigger:
	    • Type a value for **Every week(s)** (default is 1).
	    • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	
	 • **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	
	     💡 *If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*
	
	 • **Custom**: When you select **Custom**, two new fields are shown, **Filter** and **Increment**. These options offer great flexibility when scheduling a reload. See *Tasks - Custom option (page 229)* for details.

End	End time and date: • End time: **(hh:mm)** • End date: **(YYYY-MM-DD)** Select **Infinite** to create a trigger with no end date.

7. Click **Apply** to create and save the trigger.
   The dialog is closed, **Successfully added** is displayed and the new trigger is listed in the overview under **Associated items**.

Editing triggers for user sync tasks

You can edit a trigger for a user synchronization task.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the task you want to edit a trigger on and click **Edit** in the action bar at the bottom of the page.
4. Select **Triggers** at **Associated items**.
    The **Triggers** overview is displayed.
5. Select the trigger you want to edit and click **Edit** in the action bar at the bottom of the page.
    The dialog **Trigger - Start on schedule** is displayed.
6. Edit the fields in the dialog to change the trigger conditions.

Scheduled trigger properties

Property	Description
Trigger name	Name of the trigger. Mandatory.
Enabled	Status of the trigger. When selected, the trigger is active.
Time zone	The time zone of your operating system, at the time you create the trigger. When you save a trigger, the settings are kept, and if you move to a different time zone, the original values are still displayed. If you want to change the time zone and start time of a trigger, you need to do that manually.
	ⓘ *For a trigger that was created before the introduction of the time zone setting, all times and dates are by default presented in Coordinated Universal Time (UTC).*

Property	Description
Daylight saving time	Way to account for daylight saving time. **Observe daylight saving time**: This option takes daylight saving time (DST) into account. If DST is in use in the selected time zone, the execution time and date are adjusted accordingly. **Permanent standard time**: This option does not take DST into account. If DST is in use in the selected time zone, the execution time and date are not adjusted. **Permanent daylight saving time**: This option takes DST into account. If a time zone uses DST, execution time and date are always according to DST, even during periods when DST is not in use. *For time zones not using DST, always select **Permanent standard time**.* **Example:** You created a trigger for an event at 10:00 AM, while you were working in Ottawa, Canada, in January. The time zone is (GMT-0500) Eastern Time (US & Canada) and DST is used between March and November. If you select **Observe daylight saving time**, a trigger set to start at 10:00 will always start at 10.00. If you select **Permanent standard time**, a trigger set to run at 10:00 will run at 10:00 in the winter but at 09:00 in the summer. If you select **Permanent daylight saving time**, a trigger set to run at 10:00 will run at 11:00 in the winter and at 10:00 in the summer.
Start	Start time and date: • Start time: **(hh:mm)** • Start date: **(YYYY-MM-DD)**

Property	Description

Schedule	Frequency of the trigger:
	
	• **Once**.
	
	• **Hourly**. Time period between executions of the trigger. Edit **Repeat after each** by typing the values for:
	   • **hour(s)** (default is 1)
	   • **minute(s)** (default is 0)
	
	• **Daily**. Time period between executions of the trigger. Type a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	
	• **Weekly**. Time period between executions of the trigger:
	   • Type a value for **Every week(s)** (default is 1).
	   • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	
	• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	
	    *If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*
	
	• **Custom**: When you select **Custom**, two new fields are shown, **Filter** and **Increment**. These options offer great flexibility when scheduling a reload. See *Tasks - Custom option (page 229)* for details.

End	End time and date: • End time: **(hh:mm)** • End date: **(YYYY-MM-DD)** Select **Infinite** to create a trigger with no end date.

7. Click **Apply** in the action bar at the bottom of the page to save the changes.

The dialog is closed and **Successfully updated** is displayed.

Stopping user sync tasks

You can stop a user synchronization tasks from the user directory connector association page.

You can also stop user synchronization tasks from the task overview page.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **User directory connectors** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the user directory connector that you want to start a task for and click **Edit** in the action bar.

4. Select **Tasks** under **Associated items**.
   The **User synchronization tasks** overview is displayed.

5. Select the tasks that you want to stop and click **Stop** in the action bar.
   x out of x items were successfully instructed to stop is displayed at the bottom of the page.

Deleting user sync tasks

User synchronization tasks are deleted when you delete the user directory connector (UDC). You cannot delete the user sync task independently.

Deleting user directory connectors and users (page 306)

Editing users

You can edit users that you have update rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Users** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

> *You can filter a column by using the filtering option:* ⌐▼

3. Select the users that you want to edit.

4. Click **Edit** in the action bar.

5. Edit the properties.

   Identification

Identification properties

Property	Description
Name	The name of the user.
User directory	The user directory that the user is associated with.
User ID	The user ID associated with the user.
Blocked	Block (inactivate) a user. By default, not selected.
Delete prohibited	Prevent the deletion or inactivation of a user with the admin role RootAdmin. By default, not selected.

Property	Description
Admin roles	The QMC administration roles associated with the user. Click the text box to display the available admin roles. ⓘ *You can add new, non-existent admin roles, but they will not be valid until they have been properly defined.*

Tags

Tags properties

Property	Description
Tags	💡 *If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

Custom properties

When a custom property has been activated for a resource, you can use the list to select a custom property value.

Custom properties

Property	Description
Custom properties	If no custom properties are available, this property group is not displayed at all (or displayed but empty). You must make a custom property available for this resource type before it is displayed here.

6. Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

Successfully updated is displayed at the bottom of the page.

Inactivating users

You can choose to actively block (inactivate) users. If you do this, they are marked as **Blocked** in the **Users** overview page. Users can also become inactivated automatically by Qlik Sense, if they have been removed from the directory that Qlik Sense is connected to. If this happens, they are marked as **Removed externally** in the **Users** overview page.

Inactive users remain owners of objects that they have created or been assigned ownership of. They will also retain any custom properties assigned to them.

If an inactivated user attempts to log in to Qlik Sense, the user is notified to contact the system administrator.

> *You cannot inactivate (block or remove externally) a RootAdmin user who is **Delete prohibited**. To inactivate the RootAdmin user, you must first clear the **Delete prohibited** selection.*

> *If a user is deleted, the ownership of objects owned by that user is moved to the sa_repository user. All other information, such as custom properties, regarding the user is deleted along with the user.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Users** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the users that you want to inactivate.
4. Click **Edit** in the action bar.
   The **User edit** page opens.
5. Select **Blocked**.
6. Click **Apply** in the action bar to apply and save your changes.

Deleting users

You can delete users from the Qlik Sense system, if you have the required delete rights. Deleting a user means the following:

- The user will not be part of the Qlik Sense system.
- The user will not be granted access from the security evaluation.
- The ownership of the user's objects is moved to the *sa_repository* user. All other information regarding the user, such as custom properties, is deleted along with the user.

> *Users that are deleted from the directory service that Qlik Sense connects to are automatically inactivated in the QMC.*

> *When you delete a user directory connector, you can choose to delete all the users that are imported from the user directory.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Users** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the users that you want to delete.

   > *You can filter a column by using the filtering option:* ▽▼

4. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.

5. Click **OK**.

Creating a root administrator user

The first user that accesses the QMC and adds the server license, obtains the role root administrator (RootAdmin) for the Qlik Sense system. This user has full access rights to all resources in the site: security rules, streams, nodes, and so on. Additional users can be assigned as RootAdmin or other admin roles with different administrative rights.

> *The root administrator cannot change or delete the security rules that are delivered with the Qlik Sense system. These security rules are listed in the **Security rules** overview page with **Type** set to **Default**.*

Managing admin roles for a user

Qlik Sense user properties are retrieved from the user directories and cannot be edited in the QMC. However you can assign, remove or change admin roles for a user.

The QMC looks for changes in the user roles definitions every 20 seconds.

> *From the **Streams** overview, you can edit users that have access rights to a stream. Select the stream, click **Users** from the property groups, select the users and click **Edit**.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Users** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the users that you want to disconnect or change admin roles for.

4. Click **Edit** in the action bar.
   The **User edit** page opens.

5. Select **Identification** under **Properties**.

6. Click ⊕ in the **Admin roles** attribute and type the name of the admin role that you want to connect to in the text box that appears, or click ⊕ in the text box of the role that you want to disconnect.
   The **Admin roles** text field is case sensitive but the QMC suggests roles as you type. Select one of the roles.

   > *Like in Qlik Sense, if a user does not have access to a resource in the QMC, the user cannot access it in the QMC interface. For example, if you change a user's role from RootAdmin to DeploymentAdmin, the user can no longer access the apps, sheets, streams, or data connection pages in the QMC.*

> *You cannot change the admin role of a RootAdmin user who is **Delete prohibited**. To change the role, you must first clear the **Delete prohibited** selection.*

7. Click **Apply** in the action bar to apply and save your changes.

> *Some of the resources available in the QMC have additional security built around them to prevent disclosing sensitive information to unprivileged users. When defining custom admin roles in the QMC, administrators need to ensure that adequate security rules are configured for users assigned to these roles. An example: Read access to the* `UserDirectory_*` *resource is required to access the **Audit** section in the QMC.*

Changing ownership of resources

By default, the creator of a resource is the owner. The ownership can be changed when you edit the resource.

> *Only admins with the required administration rights can change the ownership of a resource.*

Do the following:

1. From the resource overview, select the resource for which you want to change owner and click **Edit**.
2. Start typing in the **Owner** field.
   Users that match your criteria are displayed.
3. Select the user who you want to assign as the new owner. You can only assign ownership to a user who exists in the Qlik Sense system.
4. Click **Apply**.
   Successfully updated is displayed.

Managing items owned by users

You can manage the resources owned by users from **Owned items** under **Associated items** on the **User edit** page.

Viewing owned items

You can view items owned by a user.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Users** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

   > *You can filter a column by using the filtering option:*

3. Select the user whose items you want to view.
4. Click **Edit** in the action bar.

The **User edit** page opens.

5. Click **Owned items** under **Associated items**.
    The **Owned items** overview opens.

Editing items owned by users

You can edit items owned by a user.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Users** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

    > *You can filter a column by using the filtering option:* ⌐▼

3. Select the user whose items you want to edit.

4. Click **Edit** in the action bar.
    The **User edit** page opens.

5. Click the **Owned items** under **Associated items**.
    The **User associated items** overview opens.

6. Select the item that you want to edit.

7. Click **Edit** in the action bar.
    The edit page for the selected item type opens.

8. Edit the properties.

9. Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

Successfully updated is displayed at the bottom of the page.

Deleting items owned by users

You can delete items owned by a specific user that you have delete rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Users** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the user whose items you want to view.

4. Click **Delete** in the action bar.
    The **User edit** page opens.

5. Click the **Owned items** under **Associated items**.
    The **User associated items** overview opens.

6. Select the items that you want to delete.

7. Click **Delete**.
    A **Delete** dialog is displayed. If a resource is deleted, all load balancing rules and security rules associated with that resource are deleted automatically.

8. Click **OK**.

Defining customized roles in the QMC

Best practice in Qlik Sense is to define security rules for groups of users. One method of doing this is to use the built-in QMC functionality for defining administrative roles and then assign these roles to users.

Another method is to group users into types of users using properties, either properties supplied from directory services or custom properties.

Both methods are describe in the next topics.

Providing administrators with access using roles

Qlik Sense is delivered with predefined sets of (default) rules for administrators. These predefined sets of rules are referred to as admin roles.

Legend (page 454)

Administration roles are defined using security rules. You can edit existing administration (admin) roles or define and add new roles using the security rules editor.

Security rules example: Creating custom admin roles (page 595)

Providing users with access using user types

Whereas the administration roles are used to define access to the QMC, user types can be defined for the users of Qlik Sense. User types are defined using the security rules editor together with property-value conditions for either one of the following or both:

- User properties
- Custom properties

If you have an existing Active Directory (AD) group that corresponds precisely to the type of users that you want to create a role for, you can define conditions for that group and give the security rule an appropriate name. For example, if you have an AD group called *Developers* you can create a security rule called *Developers* that provides the appropriate security rules. Otherwise, you can create a custom property called *User roles* and give it values such as *Developers*, *Testers*, *Contributors* and *Consumers*. You can then apply the custom properties to the users and then apply the appropriate security rules to the custom property values.

Security rules example: Applying Qlik Sense access rights for user types (page 600)

Managing tasks and triggers

Tasks

Tasks are used to perform a wide variety of operations and can be chained together in just any pattern. The tasks are handled by the Qlik Sense Scheduler Service (QSS). There are four types of tasks:

- Reload
- User synchronization
- External program
- Distribution

The reload task fully reloads the data in an app from the source. Any old data is discarded. You can create new reload tasks.

A user synchronization task imports the users and the users' information from a user directory. When you create a new instance of a user directory connector (UDC) a synchronization task with a scheduled trigger is created by the system.

The external program task triggers a third-party program. The external program task cannot be edited, nor used for task chaining.

Triggers

Execution of a task is initiated by a trigger or manually from the tasks overview page. You can create additional triggers to execute the task, and there are two types of triggers:

- Scheduled
- Task event

Scheduled triggers can be applied to both reload tasks and user synchronization tasks. Task event triggers can only be applied to reload tasks.

The triggers for a reload task are available directly on the **Task edit** page.

The triggers for a user synchronization task are accessed from the **Associated items** tab on the **Task edit** page, where the **Triggers** overview lists all the available triggers for the selected task.

Creating reload tasks from tasks

You can create a reload task to an app from the tasks overview page.

The creation of a new reload task can be initiated in more than one way:
- From the apps overview page
- From the **Associated items** on the **App edit** page
- From the tasks overview page
- From the hub by users with the appropriate permissions

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Click ⊕ **Create new** in the action bar.
   The **Reload task edit** page is displayed.
4. Edit the properties.
   a. Type the name of the reload task in the **Name** field.
   b. Click **Select app** in the **App name** field.
      A dialog opens. In the dialog, double-click the app that you want to reload by this task.
      The dialog closes and the selected app is displayed in the **App name** field.
   c. You can change the **Execution** properties, see descriptions below. The task is **Enabled** ✔ by default. Clear the selection to disable the task.

d. A task must have at least one trigger to be executed automatically. Manage the triggers by clicking **Actions▼** in the **Triggers** table heading and selecting one of the following:

- **Create new once-only trigger**, **Create new hourly trigger**, **Create new daily trigger**, **Create new weekly trigger**, or **Create new monthly trigger**. These are trigger shortcuts and the trigger that you select is added to the table instantly. The start value for the trigger is set to 5 minutes from when it was created and the trigger is enabled.

- **Create new scheduled trigger** or **Create new task event trigger** to create a new trigger of the selected type (see the property descriptions below). A dialog opens. Edit the trigger and click **OK** to close the dialog and add the trigger to the table.

- **Delete** if you want to delete the trigger that is selected in the table.

- **Edit** if you want to open the edit dialog for the trigger that is selected in the table. Edit the trigger and click **OK** to close the dialog and save your changes.

e. Optionally, apply tags.

f. Optionally, apply custom properties.

Identification

All fields are mandatory and must not be empty.

Identification properties

Property	Description	Default value
Name	The name of the task.	Reload task of <App name>
App	The name of the app that the task is created for. Click in the field to open a dialog where you can select (by double-clicking) which app the task reloads.	<App name>

Execution

Execution properties

Property	Description	Default value
Enabled	The task is enabled when selected.	Selected

Property	Description	Default value
Partial reload	With partial reload, you can add new data without reloading all the existing tables in the data model. In a full reload, all tables are deleted and then the load script is run. A partial reload only adds new data and keeps the existing tables. Partial reloads have several benefits compared to full reloads: • Faster, because only data recently changed needs to be loaded. With large data sets the difference is significant. • Less memory is consumed, because less data is loaded. • More reliable, because queries to source data run faster, reducing the risk of network problems.	Unselected
Task session timeout (minutes)	The maximum period of time before a task is aborted. When a task is started, a session is started by the manager scheduler and the task is performed by one of the nodes. If the session times out, the manager scheduler forces the node to abort the task and remove the session.	1440
Max retries	The maximum number of times the scheduler tries to rerun a failed task.	0

Triggers (Scheduled)

Scheduled trigger properties

Property	Description
Trigger name	Name of the trigger. Mandatory.
Enabled	Status of the trigger. When selected, the trigger is active.
Time zone	The time zone of your operating system, at the time you create the trigger. When you save a trigger, the settings are kept, and if you move to a different time zone, the original values are still displayed. If you want to change the time zone and start time of a trigger, you need to do that manually. ⓘ *For a trigger that was created before the introduction of the time zone setting, all times and dates are by default presented in Coordinated Universal Time (UTC).*

Property	Description
Daylight saving time	Way to account for daylight saving time. **Observe daylight saving time**: This option takes daylight saving time (DST) into account. If DST is in use in the selected time zone, the execution time and date are adjusted accordingly. **Permanent standard time**: This option does not take DST into account. If DST is in use in the selected time zone, the execution time and date are not adjusted. **Permanent daylight saving time**: This option takes DST into account. If a time zone uses DST, execution time and date are always according to DST, even during periods when DST is not in use. *For time zones not using DST, always select **Permanent standard time**.* **Example:** You created a trigger for an event at 10:00 AM, while you were working in Ottawa, Canada, in January. The time zone is (GMT-0500) Eastern Time (US & Canada) and DST is used between March and November. If you select **Observe daylight saving time**, a trigger set to start at 10:00 will always start at 10.00. If you select **Permanent standard time**, a trigger set to run at 10:00 will run at 10:00 in the winter but at 09:00 in the summer. If you select **Permanent daylight saving time**, a trigger set to run at 10:00 will run at 11:00 in the winter and at 10:00 in the summer.
Start	Start time and date: • Start time: **(hh:mm)** • Start date: **(YYYY-MM-DD)**

Property	Description

Schedule	Frequency of the trigger:
	
	• **Once**.
	
	• **Hourly**. Time period between executions of the trigger. Edit **Repeat after each** by typing the values for:
	    • **hour(s)** (default is 1)
	    • **minute(s)** (default is 0)
	
	• **Daily**. Time period between executions of the trigger. Type a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	
	• **Weekly**. Time period between executions of the trigger:
	    • Type a value for **Every week(s)** (default is 1).
	    • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	
	• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	
	    *If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*
	
	• **Custom**: When you select **Custom**, two new fields are shown, **Filter** and **Increment**. These options offer great flexibility when scheduling a reload. See *Tasks - Custom option (page 229)* for details.

End	End time and date: • End time: **(hh:mm)** • End date: **(YYYY-MM-DD)** Select **Infinite** to create a trigger with no end date.

Triggers (Task event)

Task event trigger properties

Property	Description
Trigger name	Name of the trigger. Mandatory.
Type	Trigger type.

Property	Description
Enabled	Status of the trigger. When selected, the trigger is active.
Time constraint	Time frame (in minutes) that the other tasks in the task chain must be completed within. There is no effect if the trigger consists of only one task. *Creating a task chain (page 353)*
Tasks	
	Do the following:

1. Click ⊕ **Add task** to add a tasks that will function as a trigger condition.
   A **Status** list and an empty **Task** field is added.
2. Click the empty field to add a task.
   A task selection dialog is opened and displays a list of tasks with the following columns: **Name**, **App** connected to the task, and **Tags**, which is the task name.
3. Double-click the task to use as a trigger condition.
   The task is added to the trigger and the dialog is closed.
4. In the **Status** list, select whether the trigger condition is fulfilled on **TaskSuccessful** or **TaskFail**.

> *A task with trigger condition **Task failed** is started not only when the preceding task finishes with status Failed, but also with status Skipped or Error (when the error occurs before reload). In Qlik Sense versions prior to February 2019, a preceding task with status Aborted also started a task with trigger condition Task failed. To enable this behavior, set "DisableLegacyTaskEventTriggerBehavior" to false in Scheduler.exe.config on all Scheduler nodes.*

Repeat the steps above for all the tasks that you want to include in the trigger. A task can only be added once and is not displayed in the task selection dialog if it has already been added to the trigger. There is a logical AND between the tasks.

> *The tasks do not need to be executed in any specific order and the **Time constraint** is not static. If all tasks but one have completed when the end of the time frame is reached, the task that was first completed is no longer considered executed and the end of the time frame is recalculated. The trigger then waits for all tasks to be completed within the recalculated time frame.*

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.*
	Connected tags are displayed under the text box.

Custom properties

*If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

Click **Apply** in the action bar to apply and save your changes.
5. **Successfully added** is displayed at the bottom of the page.

Creating a task chain

You can chain your tasks in just any pattern. This example describes how to create a task chain that reloads the data in three different apps, but task chaining is also available for external program tasks and distribution tasks.

- Task 1 reloads app A, every hour.
- Task 2 reloads app B, daily.
- Task 3 reloads app C, if Task 1 and Task 2 is executed within 120 minutes.

Do the following:

1. Create a new reload task for app A:
   a. Open the QMC: *https://<QPS server name>/qmc*
   b. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
   c. Click ⊕ **Create new** in the action bar.
   The **Reload task edit** page is displayed.
   d. Type *Task 1* in the **Name** field.
   e. Click **Select app** in the **App name** field. In the dialog that opens double-click app A.
   The dialog closes and the **App name** field displays app A.
   f. Leave the **Execution** properties as is.
   g. Click **Actions**▼ in the **Triggers** table heading and select **Create new hourly trigger**.
   The trigger is added to the **Triggers** table and the start value for the trigger is set to 5 minutes from when it was created.
   h. Click **Apply**.
Successfully added is displayed.

2. The next step is to create the reload task for app B:

   a. Click **<** **Tasks** in the selections panel to the left.
      The **Tasks** overview is displayed.

   b. Click **⊕** **Create new** in the action bar.
      The **Reload task edit** page is displayed.

   c. Type *Task 2* in the **Name** field.

   d. Click **Select app** in the **App name** field. In the dialog that opens double-click app B.
      The dialog closes and the **App name** field displays app B.

   e. Leave the **Execution** properties as is.

   f. Click **Actions▼** in the **Triggers** table heading and select **Create new daily trigger**.

   g. Double-click the trigger, set **Time to start** to *12:00* and click **OK**.
      The dialog closes.

   h. Click **Apply**.

   Successfully added is displayed.

3. The next step is to create the reload task for app C:

   a. Click **<Tasks** in the selections panel to the left.
      The **Tasks** overview is displayed.

   b. Click **⊕** **Create new** in the action bar.
      The **Reload task edit** page is displayed.

   c. Type *Task 3* in the **Name** field.

   d. Click **Select app** in the **App name** field. In the dialog that opens double-click app C.
      The dialog closes and the **App name** field displays app C.

   e. Leave the **Execution** properties as is.

   f. Click **Actions▼** in the **Triggers** table heading and select **Create new task event trigger**.
      The dialog **Trigger - Start on other task** opens.

   g. In the **Trigger name** field type, for example, *My trigger*.

   h. The trigger is **Enabled** by default.

   i. Set the **Time constraint** to *120* minutes.

   j. Click **Add task**; click the empty field that appears and then double-click Task 1 in the dialog that opens and keep **Task successful** in the drop-down.

   k. Click **Add task**; click the empty field that appears and then double-click Task 2 in the dialog that opens and keep **Task successful** in the drop-down.

   l. Click **OK**.
      The trigger dialog is closed.

   m. Click **Apply**.

   Successfully added is displayed.

You now have created a task chain and the task is added to the task overview where you can click 🔗 to view the task chain.

Creating a circular task chain

You can create a reload task that triggers itself (a circular task chain). This example describes how to create a simple circular task chain. You can chain your tasks in just any pattern.

Do the following:

1. If the app you want to create a circular task chain for has no task applied, start by creating a new reload task for the app:

    a. Select ➕ **Create new** from **Tasks** overview.

    > 💡 *Alternatively, select ➕* ***Create new*** *from* ***Apps*** *overview >* ***Edit*** *>* ***Associated items*** *>* ***Tasks***.

    a. Create the task.

    b. Click **Apply**.
    Successfully added is displayed.

2. Continue editing the task to create the circular task chain:

    a. Select **Triggers** > **Actions** > **Create new task event trigger**.

    b. Type a **Trigger name**.

    c. Click ➕ **Add task event**.
    The **Trigger** dialog opens.

    d. Click the empty field to the right of **Task successful** and double-click the same task that you are currently editing in the dialog that opens.
    The task is added to the **Trigger** dialog.

    e. Use the drop-down list to select whether the trigger condition is fulfilled upon **Task successful** or **Task failed**.

    f. Click **OK**.
    The dialog closes.

    g. Click **Apply**.

    Successfully updated is displayed.

You now have created a circular task chain and the task is added to the task overview. From the overview you can click 🔗 to view the task chain.

Viewing task chains

You can create task chains in various patterns by creating reload tasks and triggers for apps. From the task overview page you can access the task chain dialog to get information about tasks that will trigger a reload of the selected task.

> ℹ️ *A task can trigger itself in a circular task chain.*

Do the following:fmaster

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

   > *You can filter a column by using the filtering option:* ▭▼

3. Click 🔗 on a selected task.
   The **Task chain** dialog opens. The selected task is highlighted and the arrow on the left side of the dialog points to the selected task in the tasks overview page. The dialog displays information about the task chaining and you can manage the tasks by performing a number of actions, as follows:

   - **Preceding tasks** displays the tasks that initiates the selected task when completed. This can be a single task or a number of tasks that must all be completed within a set time period. Click ▶ to expand the list and collapse by clicking ▼.

   - **Following tasks** displays the tasks that will be initiated when the selected task is completed. The selected task can trigger another task on its own or together with other tasks. Click ▶ to expand the list and collapse by clicking ▼.

     > *Two levels of following tasks are displayed.*

   - Click ↻ in the dialog heading if you want to update the task status, that is displayed to the left of each task:

     ••• Never started: Task has never been started.

     ↻ Triggered: A request has been sent to the scheduler to run the task.

     ↻ Started: Task has started.

     ⧗ Queued: Task is queued and will be started when preceding tasks have been processed. Queuing is controlled by the value of **Max concurrent reloads**, see *Editing schedulers (page 420)*.

     ↻ Abort initiated: Manager scheduler has received the abort request but has not started processing it.

     ↻ Aborting: Manager scheduler has started processing the abort request.

     ⊠ Aborted: Task has been aborted.

     ✔ Success: Task execution was successful.

     ✗ Failed: Task has been sent to worker scheduler for execution but failed to complete. For example, a reload can fail because of missing Read rights to the data connections or an error in the reload script.

     ••• Skipped: Start of the task has been requested, but the task execution has for some reason not started. For example, the task might not be enabled.

     ↻ Retrying: Start of the task failed and a new attempt has started.

     ✗ Error: Task has not been successfully sent to worker scheduler for execution and returned an error. For example, an error can occur when there is no available worker scheduler to execute the task, or the application is already being updated by another task.

••• Reset: State that the manager scheduler sets to tasks during startup, if their current status is non-terminal, that is, if they have states like Triggered, Started, or Queued, where execution has not yet ended.

- Click **Start** next to the task to manually start a task.
- Click **Stop** next to the task to manually stop a task.
- Click outside the dialog if you want to close the dialog.
- Double-click a task in the dialog.
  The tasks overview page is displayed and the task you double-clicked is selected. You can click 🔗 to display the task chain applied to that task.

You now have viewed the task chaining summary for a task.

Editing tasks

You can edit tasks that you have update rights to. The following describes how to edit tasks from the task overview page.

> *You can edit tasks that are associated with an app or a user directory from the **Apps** and **User directory connectors**, respectively. Select the app or user directory connector from the appropriate overview, click the **Tasks** tab, select the task and then click **Edit**.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select the task that you want to edit.
4. Click **Edit** in the action bar at the bottom of the page.
5. Edit the properties.
   Select or clear **Enabled** to enable or disable the task.

> *You can enable or disable several tasks at the same time from the **Tasks** overview page.*

Identification

All fields are mandatory and must not be empty.

Identification properties

Property	Description	Default value
Name	The name of the task.	Reload task of <App name>

Property	Description	Default value
App	The name of the app that the task is created for. Click in the field to open a dialog where you can select (by double-clicking) which app the task reloads.	<App name>

Execution

Execution properties

Property	Description	Default value
Enabled	The task is enabled when selected.	Selected
Partial reload	With partial reload, you can add new data without reloading all the existing tables in the data model. In a full reload, all tables are deleted and then the load script is run. A partial reload only adds new data and keeps the existing tables. Partial reloads have several benefits compared to full reloads: • Faster, because only data recently changed needs to be loaded. With large data sets the difference is significant. • Less memory is consumed, because less data is loaded. • More reliable, because queries to source data run faster, reducing the risk of network problems.	Unselected
Task session timeout (minutes)	The maximum period of time before a task is aborted. When a task is started, a session is started by the manager scheduler and the task is performed by one of the nodes. If the session times out, the manager scheduler forces the node to abort the task and remove the session.	1440
Max retries	The maximum number of times the scheduler tries to rerun a failed task.	0

Triggers (Scheduled)

Scheduled trigger properties

Property	Description
Trigger name	Name of the trigger. Mandatory.
Enabled	Status of the trigger. When selected, the trigger is active.

Property	Description
Time zone	The time zone of your operating system, at the time you create the trigger. When you save a trigger, the settings are kept, and if you move to a different time zone, the original values are still displayed. If you want to change the time zone and start time of a trigger, you need to do that manually. *For a trigger that was created before the introduction of the time zone setting, all times and dates are by default presented in Coordinated Universal Time (UTC).*
Daylight saving time	Way to account for daylight saving time. **Observe daylight saving time**: This option takes daylight saving time (DST) into account. If DST is in use in the selected time zone, the execution time and date are adjusted accordingly. **Permanent standard time**: This option does not take DST into account. If DST is in use in the selected time zone, the execution time and date are not adjusted. **Permanent daylight saving time**: This option takes DST into account. If a time zone uses DST, execution time and date are always according to DST, even during periods when DST is not in use. *For time zones not using DST, always select **Permanent standard time**.* **Example:** You created a trigger for an event at 10:00 AM, while you were working in Ottawa, Canada, in January. The time zone is (GMT-0500) Eastern Time (US & Canada) and DST is used between March and November. If you select **Observe daylight saving time**, a trigger set to start at 10:00 will always start at 10.00. If you select **Permanent standard time**, a trigger set to run at 10:00 will run at 10:00 in the winter but at 09:00 in the summer. If you select **Permanent daylight saving time**, a trigger set to run at 10:00 will run at 11:00 in the winter and at 10:00 in the summer.
Start	Start time and date: - Start time: **(hh:mm)** - Start date: **(YYYY-MM-DD)**

Property	Description

Schedule	Frequency of the trigger:
	
	• **Once**.
	
	• **Hourly**. Time period between executions of the trigger. Edit **Repeat after each** by typing the values for:
	
	   • **hour(s)** (default is 1)
	
	   • **minute(s)** (default is 0)
	
	• **Daily**. Time period between executions of the trigger. Type a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	
	• **Weekly**. Time period between executions of the trigger:
	
	   • Type a value for **Every week(s)** (default is 1).
	
	   • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	
	• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	
	   *If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*
	
	• **Custom**: When you select **Custom**, two new fields are shown, **Filter** and **Increment**. These options offer great flexibility when scheduling a reload. See *Tasks - Custom option (page 229)* for details.

End	End time and date: • End time: **(hh:mm)** • End date: **(YYYY-MM-DD)** Select **Infinite** to create a trigger with no end date.

Triggers (Task event)

Task event trigger properties

Property	Description
Trigger name	Name of the trigger. Mandatory.
Type	Trigger type.

Property	Description
Enabled	Status of the trigger. When selected, the trigger is active.
Time constraint	Time frame (in minutes) that the other tasks in the task chain must be completed within. There is no effect if the trigger consists of only one task. *Creating a task chain (page 353)*
Tasks	
	Do the following:

1. Click ⊕ **Add task** to add a tasks that will function as a trigger condition.
   A **Status** list and an empty **Task** field is added.
2. Click the empty field to add a task.
   A task selection dialog is opened and displays a list of tasks with the following columns: **Name**, **App** connected to the task, and **Tags**, which is the task name.
3. Double-click the task to use as a trigger condition.
   The task is added to the trigger and the dialog is closed.
4. In the **Status** list, select whether the trigger condition is fulfilled on **TaskSuccessful** or **TaskFail**.

> *A task with trigger condition **Task failed** is started not only when the preceding task finishes with status Failed, but also with status Skipped or Error (when the error occurs before reload). In Qlik Sense versions prior to February 2019, a preceding task with status Aborted also started a task with trigger condition Task failed. To enable this behavior, set "DisableLegacyTaskEventTriggerBehavior" to false in Scheduler.exe.config on all Scheduler nodes.*

Repeat the steps above for all the tasks that you want to include in the trigger. A task can only be added once and is not displayed in the task selection dialog if it has already been added to the trigger. There is a logical AND between the tasks.

> *The tasks do not need to be executed in any specific order and the **Time constraint** is not static. If all tasks but one have completed when the end of the time frame is reached, the task that was first completed is no longer considered executed and the end of the time frame is recalculated. The trigger then waits for all tasks to be completed within the recalculated time frame.*

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

Custom properties

> *If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

User synchronization task properties

All fields are mandatory and must not be empty.

Identification properties

Property	Description	Default value
Name	The name of the task	Auto-generated from the user directory connector name when creating a new user directory connector.
Enabled	The task is enabled when selected.	Enabled

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

> *If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

6. Click **Apply** in the action bar to apply and save your changes.

Successfully updated is displayed at the bottom of the page.

Deleting tasks

You can delete tasks that you have delete rights to.

> *You can delete tasks that are associated with an app or a user directory from the **Apps** and **User directory connectors**, respectively.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the tasks that you want to delete.

   > *You can filter a column by using the filtering option:* ⌧▼

4. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.

5. Click **OK**.

> *You can also delete a task from the association page when you edit an app or a user directory connector.*

Enabling tasks

You can enable tasks from the task edit page or from the task overview page. The following describes how to enable tasks from the task overview page.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the tasks that you want to enable.

4. Click **More actions** in the action bar.
   A pop-up menu opens. The number displayed next to **Enable** indicates the number of items to enable.

5. Click **Enable**.
   The **Enabled** column in the tasks overview displays ✔.

You have now enabled the tasks.

> *You can also enable a task under the property **Execution** when you edit the task.*

Disabling tasks

You can disable tasks from the task edit page or from the task overview page. The following describes how to disable tasks from the task overview page.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select the tasks that you want to enable.
4. Click **More actions** in the action bar.
   A pop-up menu opens. The number displayed next to **Disable** indicates the number of items to disable.
5. Click **Disable**.

The **Enabled** column in the tasks overview is empty.

> *You can also disable a task from the properties tab when you edit the task.*

Starting tasks

You can manually start tasks. The following describes how to start tasks from the task overview page.

> *You can start tasks that are associated with an app or a user directory from the **Apps** and **User directory connectors**, respectively. Select the app or user directory connector from the appropriate overview, click **Tasks**, select the task and then click **Start**.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

> *You can filter a column by using the filtering option:* ▭▼

3. Select the task that you want to start. The number displayed next to **Start**, in the action bar at the bottom of the page, indicates the number of items in your selection that you are allowed to start.
4. Click **Start**.
   X items were successfully instructed to start is displayed at the bottom of the page.

> *Tasks can also be started by triggers.*

Stopping tasks

You can manually stop tasks. The following describes how to start tasks from the task overview page.

> *You can stop tasks that are associated with an app or a user directory from the **Apps** and **User directory connectors** respectively. Select the app or user directory connector from the appropriate overview, click **Tasks**, select the task and then click **Stop**.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

> *You can filter a column by using the filtering option:* ⌐▼

3. Select the tasks that you want to stop. The number displayed next to **Stop** indicates the number of items to stop.

4. Click **Stop** in the action bar at the bottom of the page.
   <number> items were successfully instructed to stop is displayed at the bottom of the page.

Managing system notifications

System notifications let you create and send notifications to the Qlik Sense Mobile Client Managed app on a mobile device. As an administrator, you create a notification and trigger its distribution to selected users or groups of users through the Qlik Sense Mobile Client Managed app on their mobile devices. The system notification is a free-form text, which allows you to notify users with any valuable information regarding Qlik Sense applications they have access to.

System notifications are handled by Qlik Notifier Service and Qlik Mobility Registrar that are automatically installed on all nodes in a deployment. The Qlik Notifier Service distributes the notifications outside the Qlik Sense Enterprise environment. If a firewall blocks outbound traffic, notifications are not distributed.

System notifications are defined by system notification policies.
See: *Managing system notification policies (page 368)*.

> *System notifications and System notification policies features are available only on Qlik Sense Enterprise on Windows installations licensed with a signed key. For more information on licenses, see: Qlik Sense licenses documentation.*

Creating a system notification

You can create a system notification from the system notification overview page.

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **System notifications** in the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Click ⊕**Create new** in the action bar.
   The **Edit system notification** page is displayed.

4. In the **Identification** section, edit the following properties:

Identification properties

Property	Description
Title	The name of the system notification.

Property	Description
Message	The message the system notification will display on the mobile devices once distributed.
Application link	The link to the Qlik Sense application in the following format: *qliksenselink://<link to the sense application>*.

5. Edit the **User** section to select the users that will receive the system notification:

    a. Select ✚**Add users** to add a user.

    A dedicated 👤 **Users** window is displayed.

    b. Select a user from the list or search for a user by clicking the 🔍 search icon.

    c. Select **Add** to confirm the addition of the selected user.

    > 💡 *To remove all listed users, select* ✚ ***Remove all users***.

6. Edit the **User groups** section to select the user groups that will receive the system notification, or to create a new user group.

    a. Select ✚**Add group** to add a user group.

    b. In the empty field, type the name of the user group you want to add.

    c.
    > 💡 *To remove a user group, select the* ✚ *remove icon.*

    The **Custom properties** section displays custom properties available for this resource. If no custom properties are available, this property group is empty. You must make a custom property available for this resource type before it will be displayed here.

7. Click **Apply** in the action bar to create and save the system notification.

Editing a system notification

You can edit a system notification from the system notification overview page.

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **System notifications** in the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the system notification you want to edit.

4. Click **Edit** in the action bar.
   The **Edit system notification** page is displayed.

5. In the **Identification** section, edit the following properties:

Identification properties

Property	Description
Title	The name of the system notification.
Message	The message the system notification will display on the mobile devices once distributed.
Application link	The link to the Qlik Sense application in the following format: *qliksenselink://<link to the sense application>*.

6. Edit the **User** section to select the users that will receive the system notification:

   a. Select ➕**Add users** to add a user.

      A dedicated 👤 **Users** window is displayed.

   b. Select a user from the list or search for a user by clicking the 🔍 search icon.

   c. Select **Add** to confirm the addition of the selected user.

   > 💡 *To remove all listed users, select ❌ Remove all users.*

7. Edit the **User groups** section to select the user groups that will receive the system notification, or to create a new user group.

   a. Select ➕ **Add group** to add a user group.

   b. In the empty field, type the name of the user group you want to add.

   c.

   > 💡 *To remove a user group, select the ❌ remove icon.*

8. The **Custom properties** section display custom properties available for this resource. If no custom properties are available, this property group is empty. You must make a custom property available for this resource type before it will be displayed here.

9. Click **Apply** in the action bar to create and save the system notification.

Deleting a system notification

You can delete a system notification from the system notification overview page.

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **System notifications** in the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the system notification you want to delete.

4. Click **Delete** in the action bar.

   > ℹ️ *A **Delete** dialog is displayed.*

5. Select **OK** to delete the system notification.

Managing system notification policies

You create system notification policies to determine to which users a system notification is distributed. By creating a system notification policy, you can customize the pool of users or groups of users that receive the notification on their mobile devices.

By default, a system notification policy establishes the recipients of the notification according to the **User** and **User groups** fields in the system notification setting. You can further customize the list of recipients by using custom properties.

System notifications and System notification policies features are available only on Qlik Sense Enterprise on Windows installations licensed with a signed key. For more information on licenses, see: Qlik Sense licenses documentation.

Customizing system notification policies using custom properties

You can create custom properties and use them to customize system notification policies.

To use a custom property with a system notification policy, you must:

1. Create a custom property and apply it to the following resources: **Users**, **System notifications**.
2. Assign the custom property to the users you want to distribute the notification to.
3. Assign the custom property to the system notification.
4. Create a new system notification policy and set it to distribute the notification according the custom property.

The following example describes how to use custom properties to create system notification distribution groups.

Example: Create a distribution group by using a custom property

As an administrator you need to send notifications to a 'Quality improvement virtual team' that is not part of the user groups list. The Users groups list is defined by the company's directory and imported in Qlik Sense. Instead of requesting the creation of a new Quality improvement virtual team group in the company's directory, you can create a new custom property and use it in combination with system notification policies to define the users part of the Quality improvement virtual team.

Creating a custom property

Do the following:

1. In the QMC, navigate to **Custom properties**.
2. Select ⊕**Create new**.
3. Name the custom property *virtual_team*.
4. Under **Resource types**, select **System notifications** and **Users**.
5. Under **Values**, select ⊕**Create new**.

6. Enter the value: *quality_improvement*.

7. Select **Apply**.

Assigning the custom property to selected users

Do the following:

1. In the QMC, navigate to **Users**.

2. Select the users part of the Quality improvement virtual team from the list or search for users by clicking the 🔍 search icon.

3. Click **Edit** to edit the selected users.

4. Under **Custom properties**, assign the *virtual_team* property and set the value *quality_improvement*.

5. Select **Apply**.

Assigning the custom property to a system notification

Do the following:

1. In the QMC, navigate to **System notifications**.

2. Select the system notification you want to assign the custom property to. Alternatively, create a new system notification.

3. Click **Edit** to edit the selected user.

4. Under **Custom properties**, assign the *virtual_team* property and set the value *quality_improvement*.

5. Select **Apply**.

Set the custom property as distribution rule for a system notification policy

Do the following:

1. In the QMC, navigate to **System notification policies**.

2. Select ➕**Create new**.

3. In the **Conditions** box, the **Advance** section is automatically filled with the following syntax:
   `((subject.targetGroups=resource.group))`
   Where:
     - `subject` is a system notification.
     - `targetGroups` is the property on system notifications that defines which group of users receives the notification.
     - `resource` is defined by the resource filter which in system notification policies is: User_*
       `resource.group` therefore defines the groups the user belongs to.

4. Replace the auto-filled syntax with the string that specifies the required custom property:
   `((subject.@virtual_team=resource.@virtual_team))`

5. Click **Validate rule**. The rule syntax is checked, and, if valid, a confirmation is displayed.

6. Select **Apply**.

Creating a system notification policy

You can create a system notification policy from the system notification policies overview page.

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **System notification policies** in the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Click ✚**Create new** in the action bar.
   The **Edit system notification policies** page is displayed.

4. Edit the properties:

Identification

Identification properties

Property	Description	Default value
Create rule from template	Select a template for your system notification policy.	**Unspecified**
Disable	Select to disable the rule if you do not want it to be active.	Unselected
Name	Name of the policy	Blank
Description	Description of the policy	Blank

Basic

Basic properties

Property	Description	Default value
Resource filter	In the list, select the resource that the rule will apply to.	**User_***
Action	Select the actions for the rule.	**Notify**

Advanced

Advanced properties

Property	Description	Default value
Conditions	The text box reflects changes made in the policy editor above. You can define conditions by typing in the text box.	((subject.targetGroups=resource.group))

Tags

Tags properties

Property	Description
Tags	If no tags are available, this property group is empty.
	Connected tags are displayed under the text box.

5. Click **Apply** in the action bar to save your changes.
   Successfully added is displayed at the bottom of the page.

Editing a system notification policy

You can edit a system notification policy from the system notification policies overview page.

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **System notification policies** in the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the system notification policy you want to edit.

4. Click **Edit** in the action bar.
   The **Edit system notification policies** page is displayed.

5. Edit the properties:

Identification

Identification properties

Property	Description	Default value
Create rule from template	Select a template for your system notification policy.	**Unspecified**
Disable	Select to disable the rule if you do not want it to be active.	Unselected
Name	Name of the policy	Blank
Description	Description of the policy	Blank

Basic

Basic properties

Property	Description	Default value
Resource filter	In the list, select the resource that the rule will apply to.	**User_***
Action	Select the actions for the rule.	**Notify**

Advanced

Advanced properties

Property	Description	Default value
Conditions	The text box reflects changes made in the policy editor above. You can define conditions by typing in the text box.	((subject.targetGroups=resource.group))

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

6. Click **Apply** in the action bar to save your changes.

Successfully updated is displayed at the bottom of the page.

Deleting a system notification policy

You can delete a system notification policy from the system notification policies overview page.

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **System notification policies** in the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select the system notification policy you want to delete.
4. Click **Delete** in the action bar.

A **Delete** dialog is displayed.

5. Select **OK** to delete the system notification.

Managing nodes and services

Even if you have a multi-node, geographically distributed Qlik Sense installation, the QMC enables you to manage the nodes and services from one location.

Checking the status of Qlik Sense services

You can check the status of the Engine, Repository, Proxy and Scheduler services on the nodes in your Qlik Sense system.

The QMC looks for status changes every 20 seconds.

> *If one or more services have stopped, the number of stopped services is displayed on the start page.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Nodes** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
    The **Status** column in the overview displays the status of the services on each node, see *Status (page 373)* for information on status texts.

    > *You can also click the type of node you want to check service status on, for example Engines, to display the overview.*

3. Click 🛈 on a service to get detailed information on the status, for example the time stamp.
    The **Service status** window opens.

4. Click **Manage node** in the **Service status** window to edit the node that the service is running on or click **Cancel** to return to the overview.

You have now checked the status of a service.

Status

The **Status** attributes list shows the status of the service.

Attributes

Attribute states

Attribute name	Explanation
Running	The service is running as per normal.
Stopped	The service has stopped.
Disabled	The service has been disabled. Go to **Start** > **Nodes** > [node name] > **Edit** to enable the service.

Attribute name	Explanation
(x) of (y) services are running	Shows the number of services (x) that are running compared to the number of enabled services (y).
(x) of (y) services are stopped	Shows the number of services (x) that are stopped compared to the number of enabled services (y).
(z) has stopped	The name of the service (z) that has stopped (if only one service has stopped).

Managing Qlik Sense ports

This section is only applicable for multi-node sites.

Before adding additional nodes to your site, you must manage the ports to allow communication.

Refer to the Plan and deploy Qlik Sense for more information regarding ports.

Do the following:

1. Ensure that the Windows firewall on the central node is either turned off or configured to allow connections on the required Qlik Sense ports from the other servers (nodes) you are going to add.
2. Ensure that the Windows firewall on the new node is either turned off or configured to allow connections on the required Qlik Sense ports from the central node and other servers (nodes) you are going to add.

See also:

Ports in a default Qlik Sense installation in the Install and upgrade Qlik Sense

Configuring the node

This section is only applicable to multi-node sites.

After you have installed Qlik Sense on the new node, you need to add the node in the QMC on the central node.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc* on the central node.
2. Select **Nodes** from the **Start** page to display the overview.
3. Click ⊕ **Create new** in the action bar.
   The **Node edit** page is displayed.

4. In the **Identification** section, type the **Name** of the node and enter the **Host name** (address) of the
   server that you are adding. You cannot change the host name after it has been saved. To change the
   host name, you must create a new node.

   > ⓘ   *The server address must either be in the fully qualified domain name format:*
   > `node2.domain.com` *or the machine name format:* `node2`. *We recommend that you use the*
   > *fully qualified domain name (FQDN). If you only use the machine name as the host name, the*
   > *FQDN must be added manually to the virtual proxy* **Host allow list**.

5. In the **Node purpose** section, use the drop down list to select which environment the node is intended
   for: **Production**, **Development**, or **Both**.

6. In the **Services activation** section, select all the services you installed on the node that you are
   adding.
   The repository service is always included. If a service is not installed when trying to activate, the
   properties will be applied when the installation is complete.

   > ⓘ   *You can display or hide property groups using the panel to the far right. When you edit a*
   > *property, an arrow (↰) is displayed next to the property name, to indicate that the property*
   > *value will be changed. Clicking ↰ resets that specific property value.*

7. Click **Apply** to create and save the node.
   The node adding process starts. The secure certificates from the central node are packaged and
   password protected and then shipped to the new node.
   Once completed, **Successfully added** is displayed at the bottom of the page and a dialog with your
   authorization password appears.

   > ⓘ   *If you typed the* **Host name** *incorrectly the error message* **Node registration failed** *appears.*
   > *Because the host name cannot be changed after it has been saved, you must create a new*
   > *node with the correct host name.*

   > ⓘ   *Clicking* **Apply** *is not possible if a mandatory field is empty. A dialog for unsaved changes is*
   > *displayed if you leave the edited page without clicking* **Apply**. *Clicking* **Cancel** *allows you to*
   > *continue editing. If the communication with the QRS fails, an error message is displayed and*
   > *then you can continue editing or click* **Apply** *again.*

8. Take note of the URL and the authorization password.

Authorizing the certificate on the node

> ⓘ   *This section is only applicable to multi-node sites.*

After you have configured the new node on the central node and received the certificate authorization URL
and password, you need to authorize the certificate on the host name machine.

> *You need to perform this procedure on every node you have installed.*

Do the following:

1. Connect to the new node through remote desktop.

   > *If the new node has not been configured on the central node, the **Certificate setup** dialog is displayed stating that the service is locked and that the machine needs to be added in the QMC.*

2. On the new node, open a web browser and enter the URL retrieved on the central node when configuring the node.
   Configuring the node (page 374)
   You are prompted for the password.

3. Enter the authorization password and click **Submit**.
   The new node is now connected to the central node and the **Certificate setup** dialog displays that the service was successfully unlocked.

   > *If the certificate setup dialog displays that it failed to install the Qlik Sense certificate package, use the QMC to redistribute the node. If problem persists, check the log files for details.*

The node is now added and operational.

Editing repositories

You can edit repositories that you have update rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Repositories** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the repositories that you want to edit.

4. Click **Edit** in the action bar.
   If several schedulers are selected and they have different values for a specific field, **Multiple values** is displayed in the field name.

5. Edit the properties.
   Identification
   All fields are mandatory and must not be empty.

Identification properties

Property	Description	Default value
Node	The repository name.	Inherits the node name.

Logging

The **Logging** property group contains the logging and tracing properties for the Qlik Sense Repository Service (QRS) in the Qlik Sense system.

Repository logging properties

Property	Description	Default value
Audit activity log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Basic**: a limited set of entries	Basic
Audit security log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Basic**: a limited set of entries	Basic
Service log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Error**: only error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries	Info

Tracing

Tracing settings information

Setting	Description	Value
Application log level	All the application messages for the repository service are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

Audit log level	Detailed, user-based messages are saved to this logger, for example, security rules information. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
License log level	All the license messages are saved to this logger. For example, token usage and user access allocation. Use the drop-down to set the verbosity of the logger: • **Info**: fatal, error, warning, and information entries • **Debug**: same as info, but including also debug entries	Info
Qlik Management Console (QMC) log level	All the QMC messages are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
Performance log level	All the performance messages for the repository service are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

Security log level	All the certificates messages are saved to this logger. Use the drop-down to set the verbosity of the logger: **Off**: no entries **Fatal**: only fatal entries **Error**: same as fatal, but also including error entries **Warning**: same as error, but also including warning entries **Info**: same as warning, but also including information entries **Debug**: same as info, but also including debug entries	Info
Synchronization log level	All the synchronization information in a multi-node environment is saved to this logger. Use the drop-down to set the verbosity of the logger: **Off**: no entries **Fatal**: only fatal entries **Error**: same as fatal, but also including error entries **Warning**: same as error, but also including warning entries **Info**: same as warning, but also including information entries **Debug**: same as info, but also including debug entries	Info
System log level	All the standard repository messages are saved to this logger. Use the drop-down to set the verbosity of the logger: **Off**: no entries **Fatal**: only fatal entries **Error**: same as fatal, but also including error entries **Warning**: same as error, but also including warning entries **Info**: same as warning, but also including information entries **Debug**: same as info, but also including debug entries	Info

User management log level	All user sync messages are saved to this logger. **Example:** Error: User import failure or why a user directory connector setting is incorrect. Warning: Potential error in data source, for example a circular dependence in Active Directory groups. Info: Engine start and progress or user import start and user import results, for example number of users and user groups. Debug: User request string to Active Director/LDAP server or SQL user query to ODBC source. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

> ℹ *The default path to the Qlik Sense log folder is %ProgramData%\Qlik\Sense\Log\<Service>.*

Tags

Tags properties

Property	Description
Tags	💡 *If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

Custom properties

> ℹ *If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

6. Click **Apply** to save your changes.

Successfully updated is displayed at the bottom of the page.

Creating a node

You can create one or more nodes and use them in a multi-node site. Give each node a specific role within the deployment to support planning of resources. For example, specify if a node is to run scheduled reloads or serve content to users.

When you create a node its associated services are also created and they inherit the node name: repository, engine, printing, proxy, and scheduler.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Nodes** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Click ⊕ **Create new** in the action bar.
4. Fill out the properties.

Identification

All fields are mandatory and must not be empty.

Identification property descriptions

Property	Description
Name	The node name.
Host name	The host name. You cannot edit the host name after the creation of the node. The server address must either be in the fully qualified domain name format: `node2.domain.com` or the machine name format: `node2`. ⓘ *We recommend that you use the fully qualified domain name (FQDN). If you only use the machine name as the host name, the FQDN must be added manually to the virtual proxy **Host allow list**.* ⓘ *There is support for using an IPv6 address as host name.*

Node purpose

Use the drop-down to select which environment the node is intended for: **Production**, **Development**, or **Both**.
This setting is defined in the QMC on each node that is added. Depending on what node purpose you choose, different properties are applied to the node. These properties can then be used by load balancing rules and security rules for controlling access.
The effects of choosing the different options are as follows:

- **Production**: this server is intended to support users to access apps but not create them. This means that when a user connects to this node, the **Create new app** button in the hub is not displayed to the user. To hide the **Work** section in the hub, you need to disable the security rule

that grants the application owner access. This means that when a user connects to this node, the buttons in the hub to create apps and the **Work** section are not displayed to the user. You cannot edit an app on a production node.

- **Development**: this server is intended to allow users to create apps but not serve the normal user traffic for users consuming published apps. Create and edit capabilities are enabled.
- **Both**: this setting allows both activities to occur on the node. This means that both normal user traffic is handled and users can create apps.

Node configuration

> *This section is only available when you have a Shared Persistence installation.*

In a multi-node environment, you can select one or more nodes to be **Failover candidates**. In a failover scenario, where the central node stops working, one **Failover candidate** assumes the role of central node. This solution eliminates the risks associated with the central node as a single point of failure.
A requirement for a **Failover candidate** is that the services Repository, Engine, Proxy, and Scheduler are active. A node that does not have all these services active cannot be a failover candidate.

> *It is only when creating a new node that you can make it a **Failover candidate**. Once a node has been created you can neither make it a **Failover candidate** nor clear any **Failover candidate** selection.*

Node roles
These are the roles that by default are assigned to the failover node.

Node roles

Role	Description
Scheduler master	Responsible for the scheduled reload tasks and user synchronization tasks within a Qlik Sense site.
License maintainer	Responsible for the maintenance of licenses and tokens within a Qlik Sense site.
User synchronizer	Responsible for the user synchronization within a Qlik Sense site.
Node registrator	Responsible for the registration and removal of nodes within a Qlik Sense site.
App manager	Responsible for the management of apps within a Qlik Sense site.
Database cleaner	Responsible for the cleaning of the database within a Qlik Sense site.

Services activation

Select which services to include. If a service is not installed when trying to activate, the properties will be applied when the installation is complete.

Service descriptions

Property	Description
Repository	The Qlik Sense Repository Service (QRS) is always included.
Engine	The Qlik Sense Engine Service (QES).
Printing	The Qlik Sense Printing Service (QPR).
Proxy	The Qlik Sense Proxy Service (QPS).
Scheduler	The Qlik Sense Scheduler Service (QSS).

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

Custom properties

*If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

5. Click **Apply** in the action bar to create and save the node.
   Successfully added is displayed at the bottom of the page and a dialog with **your authorization password** appears.
   If you typed the **Host name** incorrectly the message **Node registration failed** appears.

   You cannot edit the host name after the node has been created. Create a new node and type the correct host name.

6. Copy the authorization password and follow the instruction in the dialog to authorize the certificate on the host name machine.
   If successful, the **Certificate setup** dialog displays **The service was successfully unlocked**.

7. Restart the services that you installed on the new node.

You have now created a new node and authorized the certificate to make the node operational.

Load balancing

You can use load balancing to get a more even distribution of the work load between different nodes. On the central node, load balancing is automatically added to the virtual proxy, but on all other nodes you need to configure the virtual proxy with load balancing. If you create a new virtual proxy, you must configure it by adding load balancing and selecting which nodes that the virtual proxy can forward work to.

Editing a node

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Nodes** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
3. Select the node that you want to edit.
4. Click **Edit** in the action bar.
5. Edit the properties.

Identification

All fields are mandatory and must not be empty.

Identification property descriptions

Property	Description
Name	The node name.

Host name	The host name. You cannot edit the host name after the creation of the node. The server address must either be in the fully qualified domain name format: node2.domain.com or the machine name format: node2.
	
	     *We recommend that you use the fully qualified domain name (FQDN). If you only use the machine name as the host name, the FQDN must be added manually to the virtual proxy **Host allow list**.*
	
	     There is support for using an IPv6 address as host name.

Node purpose

Use the drop-down to select which environment the node is intended for: **Production**, **Development**, or **Both**.
This setting is defined in the QMC on each node that is added. Depending on what node purpose you choose, different properties are applied to the node. These properties can then be used by load balancing rules and security rules for controlling access.
The effects of choosing the different options are as follows:

- **Production**: this server is intended to support users to access apps but not create them. This means that when a user connects to this node, the **Create new app** button in the hub is not displayed to the user. To hide the **Work** section in the hub, you need to disable the security rule

that grants the application owner access. This means that when a user connects to this node, the buttons in the hub to create apps and the **Work** section are not displayed to the user. You cannot edit an app on a production node.

- **Development**: this server is intended to allow users to create apps but not serve the normal user traffic for users consuming published apps. Create and edit capabilities are enabled.
- **Both**: this setting allows both activities to occur on the node. This means that both normal user traffic is handled and users can create apps.

Node configuration

> ⓘ *This section is only available when you have a Shared Persistence installation.*

In a multi-node environment, you can select one or more nodes to be **Failover candidates**. In a failover scenario, where the central node stops working, one **Failover candidate** assumes the role of central node. This solution eliminates the risks associated with the central node as a single point of failure.
A requirement for a **Failover candidate** is that the services Repository, Engine, Proxy, and Scheduler are active. A node that does not have all these services active cannot be a failover candidate.

> ⓘ *It is only when creating a new node that you can make it a **Failover candidate**. Once a node has been created you can neither make it a **Failover candidate** nor clear any **Failover candidate** selection.*

Node roles
These are the roles that by default are assigned to the failover node.

Node roles

Role	Description
Scheduler master	Responsible for the scheduled reload tasks and user synchronization tasks within a Qlik Sense site.
License maintainer	Responsible for the maintenance of licenses and tokens within a Qlik Sense site.
User synchronizer	Responsible for the user synchronization within a Qlik Sense site.
Node registrator	Responsible for the registration and removal of nodes within a Qlik Sense site.
App manager	Responsible for the management of apps within a Qlik Sense site.
Database cleaner	Responsible for the cleaning of the database within a Qlik Sense site.

Services activation

Select which services to include. If a service is not installed when trying to activate, the properties will be applied when the installation is complete.

Service descriptions

Property	Description
Repository	The Qlik Sense Repository Service (QRS) is always included.
Engine	The Qlik Sense Engine Service (QES).
Printing	The Qlik Sense Printing Service (QPR).
Proxy	The Qlik Sense Proxy Service (QPS).
Scheduler	The Qlik Sense Scheduler Service (QSS).

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

Custom properties

*If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

6. Click **Apply** in the action bar.

Successfully updated is displayed at the bottom of the page.

Redistributing a certificate

A node that has not received the certificate correctly must be re-registered.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Nodes** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
3. Select the node you want to redistribute, displayed with **Certificate not installed** in the **Status** column.
   The **Redistribute** button in the action bar goes active.
4. Click **Redistribute**.
   A dialog with **your authorization password** appears when finished.
5. Copy the authorization password and follow the instruction in the dialog to authorize the certificate on the host name machine.
   If successful, the **Certificate setup** dialog displays **The service was successfully unlocked**.

You have now redistributed and authorized the certificate to make the node operational.

Deleting nodes

You can delete nodes that you have delete rights to.

> When you delete a node, its services are also deleted: proxy, engine, and scheduler. The deletion of a node may take some time depending on the entities related to it in the central database. A deleted node may therefore still be visible in the system a while after its deletion. Central nodes cannot be deleted.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Nodes** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the nodes that you want to delete.

4. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.

5. Click **OK**.

> To be able to add a deleted node to a cluster, you must first remove the certificates from the node and reinstall Qlik Sense. When you uninstall Qlik Sense, select the option **Remove Qlik Sense certificates and data folders**. You can also manually delete the C:\ProgramData\Qlik folder.

Editing proxies

You can edit a proxy that you have update rights to.

> For security reasons, some settings in the default virtual proxy are not editable.

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Proxies** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the proxies that you want to edit.

4. Click **Edit** in the action bar.

5. Edit the properties.
   Identification
   All fields are mandatory and must not be empty.

Identification properties

Property	Description	Default value
Node	The proxy name.	Inherits the node name.

Ports

Ports properties

Property	Description	Default value
Service listen port HTTPS (default)	The secure listen port for the proxy, which by default manages all Qlik Sense communication.	443
	Make sure that port 443 is available for the Qlik Sense Proxy Service (QPS) to use because the port is sometimes used by other software, for example, web servers.	
	If you change the default listening port 443 or 80 in the QMC, you must use the new port number in the URL to be able to go to the QMC or Hub. Then the QMC address is https://<QPS server name>:Service listen port HTTP/qmc.	
Authentication listen port	The listen port for the internal authentication module.	4244
	When editing this port as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.	
Kerberos authentication	Select to enable Kerberos authentication.	Not selected
	If the Kerberos authentication setup is incorrectly configured, you risk locking yourself out from the QMC.	
REST API listen port	The listen port for the proxy API.	4243
	When editing this port as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.	

Property	Description	Default value
Allow HTTP	Unencrypted communication is allowed if the proxy property **Allow HTTP** is selected. This means that both https (secure communication) and http (unencrypted communication) are allowed. Then the QMC address is *https://<QPS server name>:Service listen port HTTP/qmc* (where *https* can be replaced by *http*). By default, the QMC address is *https://<QPS server name>/qmc*. ⚠️ *If you change the property **Allow HTTP**, note that all web browser bookmarks (that Qlik Sense users or QMC admin users have created) will be invalid.* ℹ️ *The **Service listen port HTTP** needs to be set when **Allow HTTP** is checked.* ℹ️ *A user cannot have multiple engine sessions using different protocols.*	False (not allowed)
Service listen port HTTP	The unencrypted listen port, used when HTTP connection is allowed.	80

Advanced

Advanced properties

Property	Description	Default value
Max header lines	The maximum number of lines in the header.	100
Max header size (bytes)	The maximum total header size.	16384 bytes
Keep-alive timeout (seconds)	The maximum timeout period for a single HTTP/HTTPS request before closing the connection. Protection against denial-of-service attacks. This means that if an ongoing request exceeds this period, Qlik Sense proxy will close the connection. Increase this value if your users work over slow connections and experience closed connections.	10 seconds

Logging

The **Logging** property group contains the proxy logging and tracing properties in the Qlik Sense system.

Logging properties

Property	Description	Default value
Audit activity log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Basic**: a limited set of entries	Basic
Audit security log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Basic**: a limited set of entries	Basic
Service log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Error**: only error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries	Info

TRACING

Tracing settings information

Setting	Description	Value
Performance log interval (minutes)	The interval of performance logging.	5 minutes
Audit log level	More detailed, user-based messages are saved to this logger, for example, proxy calls. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

Performance log level	All the performance messages are saved to this logger. For example, performance counters and number of connections, streams, sessions, tickets, web sockets and load balancing information. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
Security log level	All the certificates messages are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
System log level	All the standard proxy messages are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

The default path to the Qlik Sense log folder is %ProgramData%\Qlik\Sense\Log\<Service>.

Security

Security properties

Property	Description
SSL browser certificate thumbprint	The thumbprint of the Secure Sockets Layer (SSL) certificate that handles the encryption of traffic from the browser to the proxy. When editing a proxy certificate and the Qlik Sense services run with an account without administrator privileges, you need to configure the private key permissions for the certificate.
	To be valid, the certificate must contain a private key. The certificate should be installed to the Local Computer / Computer Account > Personal portion of MMC for the user account that is used to run the Qlik Sense Proxy Service.
	When using a third-party certificate, it is required that the certificate is trusted in Windows, and that the private key is stored with the certificate in the Windows certificate store. The certificate should be installed to the Local Computer / Computer Account > Personal portion of MMC for the user account that is used to run the Qlik Sense Proxy Service.
	Qlik Sense supports certificates that are made to use signing algorithms based on SHA-1 or SHA-256.

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.*
	Connected tags are displayed under the text box.

Custom properties

*If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

6. Edit the fields under **Associated items**.

Virtual proxies

Virtual proxy properties

Property	Description
Description	The description of the virtual proxy.
Prefix	The path name in the proxy's URI that defines each additional path.
Session cookie header name	The name of the HTTP header used for the session cookie.
Is default virtual proxy	Status values: **Yes** or **No**.

7. Click **Apply** in the action bar to save your changes.

> *In most cases, the proxy must be restarted when you apply changes. Sessions handled by this proxy are ended and the users are logged out. Changes to the following resources will not generate an automatic restart of the proxy: Tags, Custom properties, Logging (Audit activity log level, Audit security log level, and Service log level), Tracing (Audit log level, Performance log level, Security log level, and System log level).*

Successfully updated is displayed at the bottom of the page.

Adding load balancing

When you install multiple engines and virtual proxies, you must add load balancing to the new nodes and virtual proxies. It is only on the central node that load balancing is automatically added. If you create a node without configuring the virtual proxy, the node will never actually be used. If you create a new virtual proxy, you must configure it by adding load balancing and selecting which nodes that the virtual proxy can forward work to.

The default algorithm used for load balancing is round-robin, where the load is evenly distributed between the available nodes on the multi-node site. However, any subsequent sessions from the same user/client will open on the current engine node, instead of following the round-robin.

> *Same user/client session is determined by the information contained in the following request headers:*
>
> - X-Qlik-ProxySession header
> - X-Qlik-Security header
> - X-Qlik-User header

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Virtual proxies** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the virtual proxy that you want to add load balancing to.

4. Click **Edit**.
   The virtual proxy properties are shown.

5. In the **Load balancing** property, click ⊕ **Add new server node** to select which server nodes to add load balancing to.
   A dialog opens.

6. Select nodes from the list.

7. Click **Add**.
   The dialog closes and the nodes are added in the list of **Load balancing nodes** on the virtual proxy edit page.
   A confirmation dialog is displayed.

8. Click **OK**.
   Successfully updated is displayed at the bottom of the page.

Configuring load balancing to isolate development nodes

When you install multiple engines and virtual proxies, you must add load balancing to the new nodes and virtual proxies. It is only on the central node that load balancing is automatically added. You can configure a proxy so that it only talks to its local engine or to a subset of the engines, which caters for a number of deployment options to support various scenarios.

It is recommended that you use separate development nodes when performing selective load balancing of apps.

Development activities such as writing scripts and running reloads often require a lot of system resources. It can therefore be beneficial to isolate the development activities to a specific node away from the normal user activities.

In this deployment example, the Qlik Sense site consists of the following nodes:

- Production node A
- Production node B
- Production node C
- Development node 1
- Development node 2
- A proxy node with 3 virtual proxies. This node can reside on any of the nodes above.
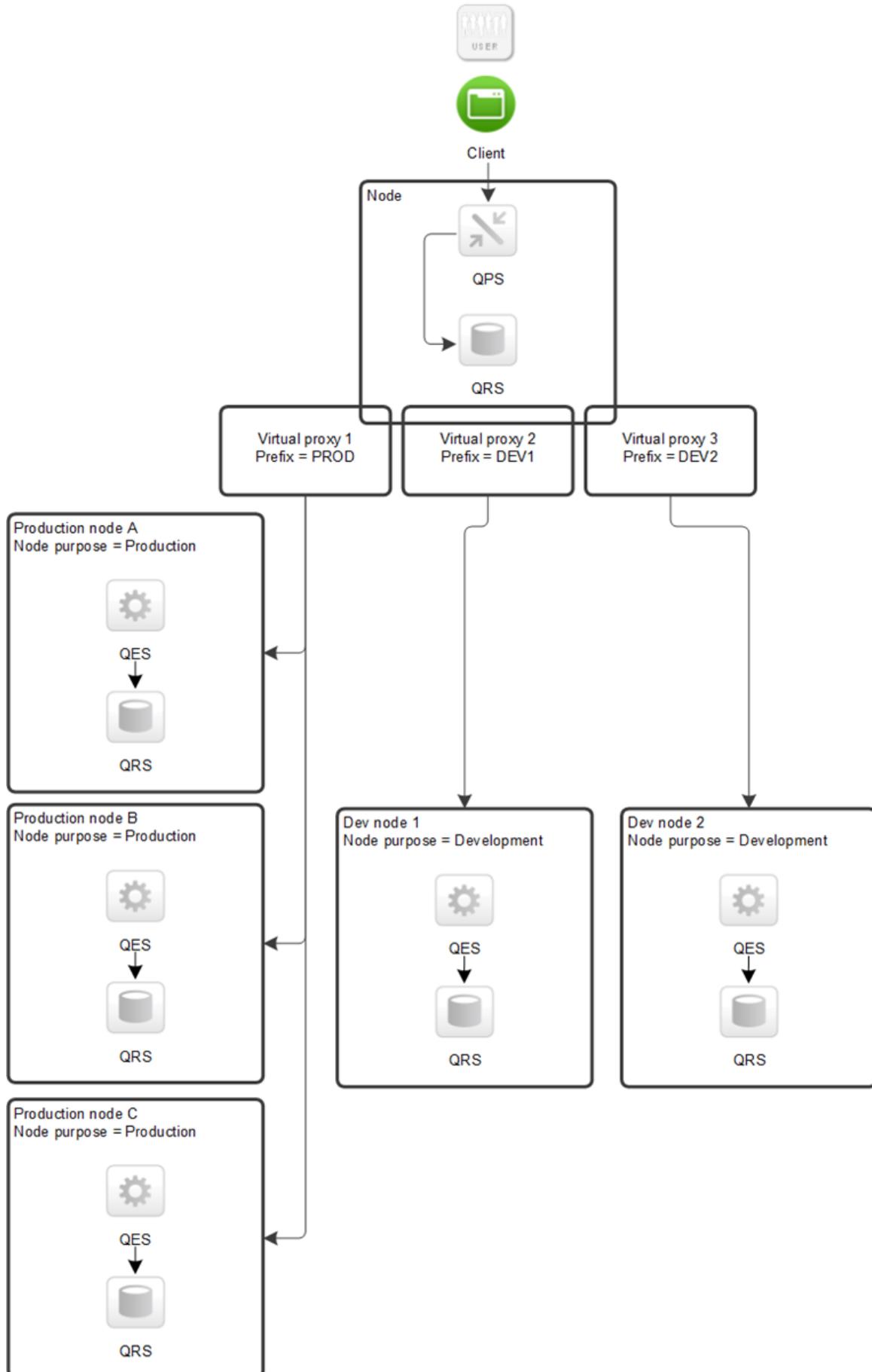
Multi-node site with separate production and development nodes

For more information about how to configure load balancing, refer to Qlik Community.

Deleting load balancing

You can delete load balancing for virtual proxies.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Virtual proxies** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the virtual proxies that you want to edit.
4. Click **Edit**.
    The virtual proxy properties are shown.
5. In the **Load balancing** property, click ✖ next to the node you want to delete load balancing from.
6. Click **Apply** in the action bar to save your changes.
    A confirmation dialog is displayed..
7. Click **OK**.

Creating a virtual proxy

A virtual proxy can be used to handle several different settings for authentication, session handling, and load balancing on the same physical server. Instead of having one server for each configuration, you can reduce the number of servers needed, by using virtual proxies.

> ℹ️ *A virtual proxy must be linked to a proxy service before the virtual proxy is available for use. You can create a virtual proxy without linking it, but it is not until it has been linked that it can be used. See: Linking a virtual proxy to a proxy (page 419)*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Virtual proxies** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Click **Create new**. You cannot add a virtual proxy to more than one proxy at a time.
4. Edit the properties in the **Virtual proxy edit** window.

    Identification
    All fields are mandatory and must not be empty.

Identification properties

Property	Description	Default value
Description	The description of the virtual proxy.	Blank
Prefix	The path name in the proxy's URI that defines each additional path. Example: *https://[node]/[prefix]/* Note the following: • You can only use lowercase letters in the prefix. After upgrade to Qlik Sense 3.0, any uppercase letters in existing virtual proxies will automatically be replaced by lowercase letters. • You can only use the following unreserved characters: (a-z, 0-9, "-", ".", "_" , "~"). For more information, see the Unreserved Characters section in the following document: [→ Uniform Resource Identifier (URI): Generic Syntax](#)	Blank
Session inactivity timeout (minutes)	The maximum period of time with inactivity before timeout. After this, the session is invalid and the user is logged out from the system.	30 minutes
Session cookie header name	The name of the HTTP header used for the session cookie. This value is blank by default and you must enter a value. *From the February 2019 release, a suffix (-HTTP) is added to the session cookie header name when a user accesses the system over http.* *It can be useful to include the value of the **Prefix** property above as a suffix in the cookie name.*	Blank

Authentication

Authentication properties

Property	Description	Default value
Anonymous access mode	• **No anonymous user**: Users must supply user identity and credentials. • **Allow anonymous user**: Users enter as anonymous but can switch and log in with a user account. • **Always anonymous user**: Users are always anonymous.	No anonymous user

Property	Description	Default value
Authentication method	• **Ticket**: a ticket is used for authentication. • **Header authentication static user directory**: allows static header authentication, where the user directory is set in the QMC. • **Header authentication dynamic user directory**: allows dynamic header authentication, where the user directory is fetched from the header. • SAML: SAML2 is used for authentication. • JWT: JSON Web Token is used for authentication. • OIDC: OpenID Connect is used for authentication.	Ticket
Header authentication header name	The name of the HTTP header that identifies users, when header authentication is allowed. Mandatory if you allow header authentication (by selecting either **Header authentication static user directory** or **Header authentication dynamic user directory** for the **Authentication method** property). *Header authentication only supports US-ASCII (UTF-8 is not supported).*	Blank
Header authentication static user directory	The name of the user directory where additional information can be fetched for header authenticated users. Mandatory if you allow static header authentication (by selecting **Header authentication static user directory** for the **Authentication method** property).	Blank
Header authentication dynamic user directory	Mandatory if you allow dynamic header authentication (by selecting **Header authentication dynamic user directory** for the **Authentication method** property). The pattern you supply must contain '$ud', '$id' and a way to separate them. **Example setting and matching header:** $ud\\$id – matches USERDIRECTORY\userid (backslashes must be escaped with an additional \) $id@$ud – matches userid@USERDIRECTORY ($id and $ud can be in any order) $ud:::$id – matches USERDIRECTORY:::userid	Blank
Windows authentication pattern	The chosen authentication pattern for logging in. If the User-Agent header contains the Windows authentication pattern string, Windows authentication is used. If there is no matching string, form authentication is used.	Windows

Property	Description	Default value
Authentication module redirect URI	When using an external authentication module, the clients are redirected to this URI for authentication.	Blank (default module, that is Windows authentication Kerberos/NTLM)
SAML single logout	Select the checkbox to enable a service provider initiated flow for SAML single logout. When selected, the metadata file generated for this virtual proxy will include single logout locations for POST and Redirect bindings.	Blank
SAML host URI	The server name that is exposed to the client. This name is used by the client for accessing Qlik services, such as the QMC. The server name does not have to be the same as the machine name, but in most cases it is. You can use either http:// or https:// in the URI. To be able to use http://, you must select **Allow HTTP** on the edit page of the proxy that the virtual proxy is linked to. Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property).	Blank
SAML entity ID	ID to identify the service provider. The ID must be unique. Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property).	Blank
SAML IdP metadata	The metadata from the IdP is used to configure the service provider, and is essential for the SAML authentication to work. A common way of obtaining the metadata is to download it from the IdP website. Click the browse button and open the IdP metadata .xml file for upload. To avoid errors, you can click **View content** and verify that the file has the correct content and format. The configuration is incomplete without metadata.	-
SAML attribute for user ID	The SAML attribute name for the attribute describing the user ID.Name or friendly name can be used to identify the attribute. *I do not know the name of a mandatory SAML attribute (page 635)*	Blank
SAML attribute for user directory	The SAML attribute name for the attribute describing the user directory. Name or friendly name can be used to identify the attribute.If the name value is enclosed in brackets, that value is used as a constant attribute value: [example] gives the constant attribute value 'example'. *I do not know the name of a mandatory SAML attribute (page 635)*	Blank

Property	Description	Default value
SAML signing algorithm	The hash algorithm used for signing SAML requests. In order to use SHA-256, a third-party certificate is required, where the associated private key has the provider "Microsoft Enhanced RSA and AES Cryptographic Provider".	-
SAML attribute mapping	Click **Add new attribute** to map SAML attributes to Qlik Sense attributes, and define if these are to be required by selecting **Mandatory**. Name or friendly name can be used to identify the attribute.If the name value is enclosed in brackets, that value is used as a constant attribute value: [example] gives the constant attribute value 'example'. ⓘ *SAML response based attributes are not taken into account when running product audit.*	-

Property	Description	Default value

JWT certificate	Add the JWT .X509 public key certificate in PEM format. The following is an example of a public key certificate.
	`-----BEGIN CERTIFICATE-----`
	`MIIDYTCCAkmgAwIBAgIJAM/oG48ciCGeMA0GCSqGSIb3DQEBCwUAMEc`
	`xEDAOBgNV`
	`BAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubmUxHjAcBgkqhki`
	`G9w0BCQEW`
	`D2pkZUBjb21wYW55LmNvbTAeFw0xNzAzMjAxMjMxNDhaFw0yNzAzMTg`
	`xMjMxNDha`
	`MEcxEDAOBgNVBAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubmU`
	`xHjAcBgkq`
	`hkiG9w0BCQEWD2pkZUBjb21wYW55LmNvbTCCASIwDQYJKoZIhvcNAQE`
	`BBQADggEP`
	`ADCCAQoCggEBALIaab/y0u/kVIZnUsRVJ9vaZ2coiB3dVl/PCa40fyZ`
	`dOIK5CvbA`
	`d0mJhuM7m/L4PldKmWh7nsPVC6SHAwgVwXASPHZQ6qha9ENChI2Nfvq`
	`Y4hXTH//Y`
	`FYaGLuKHD7pE7Jqt7Bhdh1zbBjrzsr1eU4Owwv9W9DxM4tVx3Xx8AUC`
	`NRoEWgObz`
	`Oqw9CfYY7/AWB8Hnr8G22X/l0/i4uJhiIKDVEisZ55hiNTEyqww/ew0`
	`ilI7EAngw`
	`L80D7WXpC2tCCe2V3fgUjQM4Q+0jEZGiARhzRhtaceuTBnnKq3+DnHm`
	`W4HzBuhZB`
	`CLMuWaJowkKaSfCQMel6u0/Evxc8i8FkPeMCAwEAAaNQME4wHQYDVR0`
	`OBBYEFNQ9`
	`M2Y5WlRCyftHlD2oIk12YHyBMB8GA1UdIwQYMBaAFNQ9M2Y5WlRCyft`
	`HlD2oIk12`
	`YHyBMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAHO46YL`
	`xtcMcanol`
	`PUC5nGdyYchZVHkd4F5MIe82mypwFszXGvpxKQXyAIPMkTIGb1wnE/w`
	`bCfB7moxX`
	`oFo+NoASER6wtt6FPHNcCiCXHm3B+2at16nOeMLfDefhQq03Q7qjfoa`
	`+7woAYole`
	`C9fTHGAl4TMIPThGSluiVLOLgHFUHpZryI6DdiEutXiH4afXaw0mScG`
	`36Z1uvHIq`
	`dPtjb/vDm1b9jvLITe8mZ8c2is1aBCLOdFvNupARxK7U3UD6HzGIh4x`
	`7eqo6Q9CK`
	`mKIz25FHrKTkyi1n/0+SAlOGp8PSnWrRZKmHkHbpfY5lpCuIBY9Cu2l`
	`1Xeq4QW5E`
	`AqFLKKE=`
	`-----END CERTIFICATE-----`
		Blank

JWT attribute for user ID	The JWT attribute name for the attribute describing the user ID.	Blank
JWT attribute for user directory	The JWT attribute name for the attribute describing the user directory. If the name value is enclosed in brackets, that value is used as a constant attribute value: [example] gives the constant attribute value 'example'.	-

Property	Description	Default value
JWT attribute mapping	Click **Add new attribute** to map JWT attributes to Qlik Sense attributes. If the name value is enclosed in brackets, that value is used as a constant attribute value: [example] gives the constant attribute value 'example'.	Blank
Disable optional OIDC attributes	Only to be used when syncing users through a user directory connector. When selected, the attributes **name**, **groups**, **email**, and **picture** coming from user directory connector sync are protected from being overwritten by the attributes from the OIDC.	
OpenID Connect metadata URI	The URL to the endpoint that provides configuration information for the OAuth clients to interface with the identity provider using the OpenID Connect protocol.	
Client ID	ID of the configured client at the identity provider for user authentication.	
Client secret	Secret for the client configured at the identity provider.	
Realm	Name to associate with the identity provider, used for naming consistency in multi-cloud. If the subject attribute value format is *domainname\username*, **realm** is optional. If not, **realm** is mandatory.	
sub	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values. Mandatory.	
name	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values. Mandatory.	
groups	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values.	
email	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values. Mandatory.	
client_id	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values.	

Property	Description	Default value
picture	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values.	
scope	Used in the OAuth 2.0 specification to specify the access privileges when issuing an access token. For example, use this option to add a groups scope in case the identity provider requires that to support a user groups feature.	
OIDC attribute mapping	Click **Add new attribute** to map OIDC attributes to Qlik Sense attributes, and define if these are to be required by selecting **Mandatory**. Name or friendly name can be used to identify the attribute.	

Load balancing

Load balancing properties

Property	Description	Default value
Load balancing nodes	Click **Add new server node** to add load balancing to that node.	Blank

Advanced

Advanced properties

Property	Description	Default value
Extended security environment	Enabling this setting will send the following information about the client environment in the security header: OS, device, browser, and IP. If not selected, the user can run the same engine session simultaneously on multiple devices.	Blank
Session cookie domain	By default the session cookie is valid only for the machine that the proxy is installed on. This (optional) property allows you to increase its validity to a larger domain. Example: `company.com`	Blank (default machine)
Has secure attribute (https)	Option for session cookie that has the Secure attribute and uses https.	Selected

Property	Description	Default value
SameSite attribute (https)	SameSite attribute values for https: **No attribute**, **None**, **Lax**, **Strict** For more information, see *SameSite cookie attribute (page 167)*	Lax
Has secure attribute (http)	Option for session cookie that has the Secure attribute and uses http.	Blank
SameSite attribute (http)	SameSite attribute values for http: **No attribute**, **None**, **Lax**, **Strict** For more information, see *SameSite cookie attribute (page 167)*	No attribute

Additional response headers	Headers added to all HTTP responses back to the client. Example:
	 `Header1: value1`
	 `Header2: value2`
		Blank

Host allow list	A list of host names following the RFC standards. Put literal IPv6 addresses within brackets. All values added here are validated starting from the bottom level. If, for example, *domain.com* is added, this means that all values ending with *domain.com* will be approved. If *subdomain.domain.com* is added, this means that all values ending with *subdomain.domain.com* will be approved. To support switching schema when using cross-origin resource sharing (CORS), the host allow list must include the schema to avoid requests being blocked by the CORS policy. **Example:** If you have a mashup loaded from an unsecure web site (*http://subdomain.domain.com*) and Qlik Sense running secure (*https:/qlik.sense…*), the schema, (*http://subdomain.domain.com*), must be present in the host allow list. *Even if the allow list is empty, the name of the machine where Qlik Sense is installed is still considered part of the allow list, although not visible.*	Blank

Integration

Integration properties

Property	Description	Default value
Session module base URI	The address to an external session module, if any.	Blank (default module, that is in memory)
Load balancing module base URI	The address to an external load balancing module that selects which Qlik Sense engine to use for the user's session, if any.	Blank (default module, that is round robin)

Client authentication link

The client authentication link is used to authenticate the client against the Qlik Sense server.

> *The **Client authentication link** can be generated on any virtual proxy in the QMC. However, if the client authentication link will be retrieved from the hub, you must generate the link from the default virtual proxy on the central node.*

Client authentication link properties

Property	Description	Default value
Client authentication link host URI	The Qlik Sense URI that will be a part of the client authentication link.	Blank
Client authentication link friendly name	A name that helps the user to identify the host. The friendly name will be a part of the client authentication link.	Blank
Generate client authentication link	Click the button to generate a link that can be copied and distributed to users.	-

Configuring client authentication (page 497)

Tags

> *If no QMC tags are available, this property group is empty.*

Click the text box to display a list of the available tags. Start typing to reduce the list. Connected tags are displayed under the text box.

Custom properties

> *If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

5. Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

6. Click **Apply** in the action bar to save your changes.

Successfully updated is displayed at the bottom of the page.

Editing a virtual proxy

You can edit an existing virtual proxy.

> *A virtual proxy must be linked to a proxy service before the virtual proxy is available for use. You can create a virtual proxy without linking it, but it is not until it has been linked that it can be used. See: Linking a virtual proxy to a proxy (page 419)*

> *For security reasons, some settings in the default virtual proxy are not editable. Incorrect settings could make the system inoperable.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Virtual proxies** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the virtual proxy that you want to edit and click **Edit** in the action bar. You can only edit virtual proxies for one proxy at a time.

4. Edit the properties in the **Virtual proxy edit** window:
   Identification
   All fields are mandatory and must not be empty.

Identification properties

Property	Description	Default value
Description	The description of the virtual proxy.	Blank

Property	Description	Default value
Prefix	The path name in the proxy's URI that defines each additional path. Example: *https://[node]/[prefix]/* Note the following: • You can only use lowercase letters in the prefix. After upgrade to Qlik Sense 3.0, any uppercase letters in existing virtual proxies will automatically be replaced by lowercase letters. • You can only use the following unreserved characters: (a-z, 0-9, "-", ".", "_" , "~"). For more information, see the Unreserved Characters section in the following document: ⤷ Uniform Resource Identifier (URI): Generic Syntax	Blank
Session inactivity timeout (minutes)	The maximum period of time with inactivity before timeout. After this, the session is invalid and the user is logged out from the system.	30 minutes
Session cookie header name	The name of the HTTP header used for the session cookie. This value is blank by default and you must enter a value. *From the February 2019 release, a suffix (-HTTP) is added to the session cookie header name when a user accesses the system over http.* *It can be useful to include the value of the **Prefix** property above as a suffix in the cookie name.*	Blank

Authentication

Authentication properties

Property	Description	Default value
Anonymous access mode	• **No anonymous user**: Users must supply user identity and credentials. • **Allow anonymous user**: Users enter as anonymous but can switch and log in with a user account. • **Always anonymous user**: Users are always anonymous.	No anonymous user

Property	Description	Default value
Authentication method	• **Ticket**: a ticket is used for authentication. • **Header authentication static user directory**: allows static header authentication, where the user directory is set in the QMC. • **Header authentication dynamic user directory**: allows dynamic header authentication, where the user directory is fetched from the header. • SAML: SAML2 is used for authentication. • JWT: JSON Web Token is used for authentication. • OIDC: OpenID Connect is used for authentication.	Ticket
Header authentication header name	The name of the HTTP header that identifies users, when header authentication is allowed. Mandatory if you allow header authentication (by selecting either **Header authentication static user directory** or **Header authentication dynamic user directory** for the **Authentication method** property). *Header authentication only supports US-ASCII (UTF-8 is not supported).*	Blank
Header authentication static user directory	The name of the user directory where additional information can be fetched for header authenticated users. Mandatory if you allow static header authentication (by selecting **Header authentication static user directory** for the **Authentication method** property).	Blank
Header authentication dynamic user directory	Mandatory if you allow dynamic header authentication (by selecting **Header authentication dynamic user directory** for the **Authentication method** property). The pattern you supply must contain '$ud', '$id' and a way to separate them. **Example setting and matching header:** $ud\\$id – matches USERDIRECTORY\userid (backslashes must be escaped with an additional \) $id@$ud – matches userid@USERDIRECTORY ($id and $ud can be in any order) $ud:::$id – matches USERDIRECTORY:::userid	Blank
Windows authentication pattern	The chosen authentication pattern for logging in. If the User-Agent header contains the Windows authentication pattern string, Windows authentication is used. If there is no matching string, form authentication is used.	Windows

Property	Description	Default value
Authentication module redirect URI	When using an external authentication module, the clients are redirected to this URI for authentication.	Blank (default module, that is Windows authentication Kerberos/NTLM)
SAML single logout	Select the checkbox to enable a service provider initiated flow for SAML single logout. When selected, the metadata file generated for this virtual proxy will include single logout locations for POST and Redirect bindings.	Blank
SAML host URI	The server name that is exposed to the client. This name is used by the client for accessing Qlik services, such as the QMC. The server name does not have to be the same as the machine name, but in most cases it is. You can use either http:// or https:// in the URI. To be able to use http://, you must select **Allow HTTP** on the edit page of the proxy that the virtual proxy is linked to. Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property).	Blank
SAML entity ID	ID to identify the service provider. The ID must be unique. Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property).	Blank
SAML IdP metadata	The metadata from the IdP is used to configure the service provider, and is essential for the SAML authentication to work. A common way of obtaining the metadata is to download it from the IdP website. Click the browse button and open the IdP metadata .xml file for upload. To avoid errors, you can click **View content** and verify that the file has the correct content and format. The configuration is incomplete without metadata.	-
SAML attribute for user ID	The SAML attribute name for the attribute describing the user ID.Name or friendly name can be used to identify the attribute. *I do not know the name of a mandatory SAML attribute (page 635)*	Blank
SAML attribute for user directory	The SAML attribute name for the attribute describing the user directory. Name or friendly name can be used to identify the attribute.If the name value is enclosed in brackets, that value is used as a constant attribute value: [example] gives the constant attribute value 'example'. *I do not know the name of a mandatory SAML attribute (page 635)*	Blank

Property	Description	Default value
SAML signing algorithm	The hash algorithm used for signing SAML requests. In order to use SHA-256, a third-party certificate is required, where the associated private key has the provider "Microsoft Enhanced RSA and AES Cryptographic Provider".	-
SAML attribute mapping	Click **Add new attribute** to map SAML attributes to Qlik Sense attributes, and define if these are to be required by selecting **Mandatory**. Name or friendly name can be used to identify the attribute.If the name value is enclosed in brackets, that value is used as a constant attribute value: [example] gives the constant attribute value 'example'. *SAML response based attributes are not taken into account when running product audit.*	-

Property	Description	Default value
JWT certificate	Add the JWT .X509 public key certificate in PEM format. The following is an example of a public key certificate. -----BEGIN CERTIFICATE----- MIIDYTCCAkmgAwIBAgIJAM/oG48ciCGeMA0GCSqGSIb3DQEBCwUAMEc xEDAOBgNV BAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4grRG9ubmUxHjAcBgkqhki G9w0BCQEW D2pkZUBjb21wYW55LmNvbTAeFw0xNzAzMjAxMjMxNDhaFw0yNzAzMTg xMjMxNDha MEcxEDAOBgNVBAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4grRG9ubmU xHjAcBgkq hkiG9w0BCQEWD2pkZUBjb21wYW55LmNvbTCCASIwDQYJKoZIhvcNAQE BBQADggEP ADCCAQoCggEBALIaab/y0u/kVIZnUsRVJ9vaZ2coiB3dVl/PCa4OfyZ dOIK5CvbA d0mJhuM7m/L4PldKmWh7nsPVC6SHAwgVwXASPHZQ6qha9ENChI2Nfvq Y4hXTH//Y FYaGLuKHD7pE7Jqt7Bhdh1zbBjrzsr1eU4Owwv9W9DxM4tVx3Xx8AUC NRoEWgObz Oqw9CfYY7/AWB8Hnr8G22X/l0/i4uJhiIKDVEisZ55hiNTEyqww/ew0 ilI7EAngw L80D7WXpC2tCCe2V3fgUjQM4Q+0jEZGiARhzRhtaceuTBnnKq3+DnHm W4HzBuhZB CLMuWaJowkKaSfCQMel6u0/Evxc8i8FkPeMCAwEAAaNQME4wHQYDVR0 OBBYEFNQ9 M2Y5WlRCyftHlD2oIk12YHyBMB8GA1UdIwQYMBaAFNQ9M2Y5WlRCyft HlD2oIk12 YHyBMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAHO46YL xtcMcanol PUC5nGdyYchZVHkd4F5MIe82mypwFszXGvpxKQXyAIPMkTIGb1wnE/w bCfB7moxX oFo+NoASER6wtt6FPHNCCiCXHm3B+2at16nOeMLfDefhQq03Q7qjfoa +7woAYole C9fTHGAl4TMIPThGSluiVLOLgHFUHpZryI6DdiEutXiH4afXaw0mScG 36Z1uvHIq dPtjb/vDm1b9jvLITe8mZ8c2is1aBCLOdFvNupARxK7U3UD6HzGIh4x 7eqo6Q9CK mKIz25FHrKTkyi1n/0+SAlOGp8PSnWrRZKmHkHbpfY5lpCuIBY9Cu2l 1Xeq4QW5E AqFLKKE= -----END CERTIFICATE-----	Blank
JWT attribute for user ID	The JWT attribute name for the attribute describing the user ID.	Blank
JWT attribute for user directory	The JWT attribute name for the attribute describing the user directory. If the name value is enclosed in brackets, that value is used as a constant attribute value: [example] gives the constant attribute value 'example'.	-

Property	Description	Default value
JWT attribute mapping	Click **Add new attribute** to map JWT attributes to Qlik Sense attributes. If the name value is enclosed in brackets, that value is used as a constant attribute value: [example] gives the constant attribute value 'example'.	Blank
Disable optional OIDC attributes	Only to be used when syncing users through a user directory connector. When selected, the attributes **name**, **groups**, **email**, and **picture** coming from user directory connector sync are protected from being overwritten by the attributes from the OIDC.	
OpenID Connect metadata URI	The URL to the endpoint that provides configuration information for the OAuth clients to interface with the identity provider using the OpenID Connect protocol.	
Client ID	ID of the configured client at the identity provider for user authentication.	
Client secret	Secret for the client configured at the identity provider.	
Realm	Name to associate with the identity provider, used for naming consistency in multi-cloud. If the subject attribute value format is *domainname\username*, **realm** is optional. If not, **realm** is mandatory.	
sub	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values. Mandatory.	
name	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values. Mandatory.	
groups	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values.	
email	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values. Mandatory.	
client_id	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values.	

Property	Description	Default value
picture	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values.	
scope	Used in the OAuth 2.0 specification to specify the access privileges when issuing an access token. For example, use this option to add a groups scope in case the identity provider requires that to support a user groups feature.	
OIDC attribute mapping	Click **Add new attribute** to map OIDC attributes to Qlik Sense attributes, and define if these are to be required by selecting **Mandatory**. Name or friendly name can be used to identify the attribute.	

Load balancing

Load balancing properties

Property	Description	Default value
Load balancing nodes	Click **Add new server node** to add load balancing to that node.	Blank

Advanced

Advanced properties

Property	Description	Default value
Extended security environment	Enabling this setting will send the following information about the client environment in the security header: OS, device, browser, and IP. If not selected, the user can run the same engine session simultaneously on multiple devices.	Blank
Session cookie domain	By default the session cookie is valid only for the machine that the proxy is installed on. This (optional) property allows you to increase its validity to a larger domain. Example: `company.com`	Blank (default machine)
Has secure attribute (https)	Option for session cookie that has the Secure attribute and uses https.	Selected

Property	Description	Default value
SameSite attribute (https)	SameSite attribute values for https: **No attribute**, **None**, **Lax**, **Strict** For more information, see *SameSite cookie attribute (page 167)*	Lax
Has secure attribute (http)	Option for session cookie that has the Secure attribute and uses http.	Blank
SameSite attribute (http)	SameSite attribute values for http: **No attribute**, **None**, **Lax**, **Strict** For more information, see *SameSite cookie attribute (page 167)*	No attribute

Additional response headers	Headers added to all HTTP responses back to the client. Example:
	`Header1: value1`
	`Header2: value2`
		Blank

Host allow list	A list of host names following the RFC standards. Put literal IPv6 addresses within brackets. All values added here are validated starting from the bottom level. If, for example, *domain.com* is added, this means that all values ending with *domain.com* will be approved. If *subdomain.domain.com* is added, this means that all values ending with *subdomain.domain.com* will be approved. To support switching schema when using cross-origin resource sharing (CORS), the host allow list must include the schema to avoid requests being blocked by the CORS policy. **Example:** If you have a mashup loaded from an unsecure web site (*http://subdomain.domain.com*) and Qlik Sense running secure (*https://qlik.sense…*), the schema, (*http://subdomain.domain.com*), must be present in the host allow list. *Even if the allow list is empty, the name of the machine where Qlik Sense is installed is still considered part of the allow list, although not visible.*	Blank

Integration

Integration properties

Property	Description	Default value
Session module base URI	The address to an external session module, if any.	Blank (default module, that is in memory)
Load balancing module base URI	The address to an external load balancing module that selects which Qlik Sense engine to use for the user's session, if any.	Blank (default module, that is round robin)

Client authentication link

The client authentication link is used to authenticate the client against the Qlik Sense server.

> *The **Client authentication link** can be generated on any virtual proxy in the QMC. However, if the client authentication link will be retrieved from the hub, you must generate the link from the default virtual proxy on the central node.*

Client authentication link properties

Property	Description	Default value
Client authentication link host URI	The Qlik Sense URI that will be a part of the client authentication link.	Blank
Client authentication link friendly name	A name that helps the user to identify the host. The friendly name will be a part of the client authentication link.	Blank
Generate client authentication link	Click the button to generate a link that can be copied and distributed to users.	-

Configuring client authentication (page 497)

Tags

> *If no QMC tags are available, this property group is empty.*

Click the text box to be display a list of the available tags. Start typing to reduce the list. Connected tags are displayed under the text box.

Custom properties

> ℹ️ *If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

5. Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.
6. Edit the fields under **Associated items**.

Proxies

Proxy properties

Property	Description
Node	The proxy name.

Status	One of the following statuses is displayed:
	
	• **Running**
	  The service is running as per normal.
	
	• **Stopped**
	  The service has stopped.
	
	• **Disabled**
	  The service has been disabled.
	
	> 💡 *Click ℹ️ in the **Status** column for more detailed information on the status.*
	
	Checking the status of Qlik Sense services (page 373).

Service listen port HTTPS (default)	The secure listen port for the proxy, which by default manages all Qlik Sense communication. > ℹ️ *Make sure that port 443 is available for the Qlik Sense Proxy Service (QPS) to use because the port is sometimes used by other software, for example, web servers.*
Allow HTTP	Status values: **Yes** or **No**. **Yes**: Unencrypted communication is allowed. This means that both https (secure communication) and (http) unencrypted communication is allowed. > ℹ️ *From the February 2019 release, a suffix (-HTTP) is added to the session cookie header name when a user accesses the system over http.*

Property	Description
Service listen port HTTP	The unencrypted listen port, used when HTTP connection is allowed.
Authentication listen port	The listen port for the internal authentication module.
	When editing this port as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.
Kerberos authentication	Status values: **Yes** or **No**. **Yes**: Kerberos authentication is enabled.
REST API listen port	The listen port for the proxy API.
	When editing this port as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.
SSL browser certificate thumbprint	The thumbprint of the Secure Sockets Layer (SSL) certificate that handles the encryption of traffic from the browser to the proxy. When editing a proxy certificate and the Qlik Sense services run with an account without administrator privileges, you need to configure the private key permissions for the certificate.
Keep-alive timeout (seconds)	The maximum timeout period for a single HTTP/HTTPS request before closing the connection. Protection against denial-of-service attacks. This means that if an ongoing request exceeds this period, Qlik Sense proxy will close the connection. Increase this value if your users work over slow connections and experience closed connections.
Max header size (bytes)	The maximum total header size.
Max header lines	The maximum number of lines in the header.
Audit activity log level	Levels: **Off** or **Basic** (a limited set of entries)
Audit security log level	Levels: **Off** or **Basic** (a limited set of entries)
Service log level	Each level from **Error** to **Info** includes more information than the previous level.

Property	Description
Audit log level	More detailed, user-based messages are saved to this logger, for example, proxy calls. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log level	All the performance messages are saved to this logger. For example, performance counters and number of connections, streams, sessions, tickets, web sockets and load balancing information. Each level from **Fatal** to **Debug** includes more information than the previous level.
Security log level	All the certificates messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
System log level	All the standard proxy messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log interval (minutes)	The interval of performance logging.
ID	The ID of the proxy.
Created	The date and time when the proxy was created.
Last modified	The date and time when the proxy was last modified.
Modified by	By whom the proxy was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼▲	Sort the list ascending or descending. Some columns do not support sorting.
⌄▼	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⌄▼ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. *Searching and filtering in the QMC (page 25)*
Edit	Edit the selected proxy.

Property	Description
Unlink	Unlink a proxy service from the selected proxy. *A virtual proxy must be linked to a proxy service in order to work.*
⊕ **Link**	Link a proxy service to the selected proxy.
Show more items	The overview shows a set number of items by default. To show more items, scroll to the end of the list and click **Show more items**. Sorting and filtering of items is always done on the full database list of items, not only the items that are displayed.

7. Click **Apply** in the action bar to save your changes.

> *In most cases, the proxy must be restarted when you apply changes to the virtual proxy. Sessions handled by the proxy, to which the virtual proxy is linked, are ended and the users are logged out. Changes to the following resources in the virtual proxy will not generate an automatic restart of the proxy: Tags, Custom properties, and Load balancing nodes.*

Successfully updated is displayed at the bottom of the page.

Linking a virtual proxy to a proxy

A virtual proxy must be linked to a proxy service before the virtual proxy is available for use.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Virtual proxies** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the virtual proxy that you want to link to a proxy.
4. Click **Edit** in the action bar.
5. To the right on the **Virtual proxy edit** page, under **Associated items**, click **Proxies**.
   The **Associated proxies** page is opened.
6. In the action bar, click ⊕**Link**.
   The **Select proxy services** page is opened.
7. Select the node to link to and click **Link**.
   The linked node is presented in the list **Associated proxies**. Your session is ended because the proxy has been restarted.
8. Restart the QMC.

You have linked the virtual proxy to a proxy, and now the virtual proxy is available for use.

Deleting virtual proxies

You can delete virtual proxies that you have delete rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Virtual proxies** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the virtual proxy you want to delete. You cannot delete virtual proxies for more than one proxy at a time.

4. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.

5. Click **OK**.

Editing schedulers

You can edit schedulers that you have update rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Schedulers** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

3. Select the schedulers that you want to edit.

4. Click **Edit** in the action bar.
   If several schedulers are selected and they have different values for a specific field, **Multiple values** is displayed in the field name.

5. Edit the properties.

   > *You can display or hide property groups using the panel to the far right.*

   Identification

   All fields are mandatory and must not be empty.

   Identification properties

Property	Description	Default value
Node	The scheduler name.	Inherits the node name.

   Logging

   The **Logging** property group contains the scheduler logging and tracing properties in the Qlik Sense system.

Logging properties

Property	Description	Default value
Audit activity log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Basic**: a limited set of entries	Basic
Service log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Error**: only error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries	Info

Tracing

Tracing settings information

Setting	Description	Value
Application log level	All the application messages for the scheduler service are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
Audit log level	More detailed, user based, messages are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

Performance log level	All the performance messages are saved to this logger. Use the drop-down to set the verbosity of the logger: **Off**: no entries **Fatal**: only fatal entries **Error**: same as fatal, but also including error entries **Warning**: same as error, but also including warning entries **Info**: same as warning, but also including information entries **Debug**: same as info, but also including debug entries	Info
Security log level	All the certificates messages are saved to this logger. Use the drop-down to set the verbosity of the logger: **Off**: no entries **Fatal**: only fatal entries **Error**: same as fatal, but also including error entries **Warning**: same as error, but also including warning entries **Info**: same as warning, but also including information entries **Debug**: same as info, but also including debug entries	Info
System log level	All the standard scheduler messages are saved to this logger. Use the drop-down to set the verbosity of the logger: **Off**: no entries **Fatal**: only fatal entries **Error**: same as fatal, but also including error entries **Warning**: same as error, but also including warning entries **Info**: same as warning, but also including information entries **Debug**: same as info, but also including debug entries	Info
Task execution log level	All the task execution messages are saved to this logger. Use the drop-down to set the verbosity of the logger: **Off**: no entries **Fatal**: only fatal entries **Error**: same as fatal, but also including error entries **Warning**: same as error, but also including warning entries **Info**: same as warning, but also including information entries **Debug**: same as info, but also including debug entries	Info

> ℹ️ *The default path to the Qlik Sense log folder is %ProgramData%\Qlik\Sense\Log\<Service>.*

Advanced

Advanced properties

Property	Description	Default value
Type	If enabled by the property above, the QSS type is set to: • Manager: sends the task to a worker QSS within the site. • Worker: receives the task from the manager QSS and executes the task. • Manager and worker: when the manager QSS also acts a worker QSS, on a single node site.	Worker (except for on a central node; Manager)
Max concurrent reloads	The maximum number of reloads that the scheduler can perform at the same time.	4
Engine timeout (minutes)	If the number for **Max concurrent reloads** is reached (a separate property), the request to start a new engine process is queued, waiting for the number of running reload processes to go below **Max concurrent reloads**. If this does not happen within the given time period, the request to start a new engine process is removed from the queue.	30

Tags

Tags properties

Property	Description
Tags	💡 *If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

Custom properties

> ℹ️ *If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

6. Click **Apply** to save your changes.

Successfully updated is displayed at the bottom of the page.

Editing an engine

You can edit engines that you have update rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Engines** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select the engine that you want to edit.
4. Click **Edit** in the action bar.
5. Edit the properties.

   Identification

   Identification properties

Property	Description	Default value
Node	The engine name.	Inherits the node name.

   Apps

   Apps properties

Property	Description	Default value
App autosave interval (seconds)	The number of seconds between autosaving of the apps. Autosave is always performed when a session ends.	30
App cache time (seconds)	The number of seconds that a Qlik Sense app is allowed to remain in memory, after the last session that used the app has ended.	28800
Table files root directory	A scheduled reload will search for files in this directory when relative paths are used to define file location. *This setting is used to support legacy features in QlikView scripts for relative paths to files during reload. You cannot use this setting to change the directory where the apps are stored.*	%ProgramData%\Qlik\Sense\Apps
Max number of undos	The maximum number of undos when editing app content, such as sheets, objects, bookmarks, and stories: min = 0, max = 999.	100

Advanced

Advanced properties

Property	Description	Default value
Listen ports	The listen port used by the Qlik Sense Engine Service (QES) for communication with the Qlik Sense web clients. Click ➕ to add more ports. Click ➕ to remove a port.	4747
Allow data lineage	Save the data lineage (that is, the origin of the data) when executing a load script that loads data into Qlik Sense. This setting allows information about the **LOAD** statement that was used to load the table to be stored in the QVD file.	Selected
Min memory usage (%)	The minimum memory capacity used by Qlik Sense. The cache is not cleared below this limit. For a detailed description of this setting and the role it plays in memory management of the engine, see ➡ Associative Engine memory management and CPU usage.	70
Max memory usage (%)	The maximum memory capacity used by Qlik Sense. For a detailed description of this setting and the role it plays in memory management of the engine, see ➡ Associative Engine memory management and CPU usage.	90

Property	Description	Default value
Memory usage mode	Influences how the Operating System (Windows) manages memory for the Engine process. Use the drop-down to select one of the following methods: • **Hard max limit**: never use more memory than defined by the **Max memory usage (%)** setting. This setting requires that the Operating System is configured to support this, as described in the ⬗ SetProcessWorkingSetSizeEx documentation (QUOTA_ LIMITS_HARDWS_MAX_ENABLE parameter). • **Ignore max limit**: use as much memory as necessary, regardless of the **Max memory usage (%)** setting. • **Soft max limit**: use more memory than defined by the **Max memory usage (%)** setting, if necessary and available.	Hard max limit

Property	Description	Default value
CPU throttle (%)	The amount of CPU capacity used by Qlik Sense. Range: 0 – 100 %. You can increase or decrease the priority of the Qlik Sense Engine Service process, depending on how much CPU capacity the process is using. In this way, some of the CPU capacity can be released and used by other applications, improving the overall performance of the server. *If the CPU usage for the Qlik Sense Engine Service process exceeds the throttle level, it is most likely because the operating system has determined that more resources are available.*	0 (that is, no throttling)
Standard mode	When selected, standard mode is used. If cleared, legacy mode is used. Standard mode is the default mode that prevents actions that are potentially harmful. Standard mode is to be used unless there are special reasons not to. Legacy mode can be used for running QlikView load scripts unchanged, when loading data into Qlik Sense. For security reasons, Qlik Sense in standard mode does not support absolute or relative paths in the data load script or functions and variables that expose the file system. *Disabling standard mode can create a security risk by exposing the file system.*	Selected

Property	Description	Default value
HTTP callback port	The callback port used by the Qlik Sense Repository Service for sending HTTP events to engine.	4748
Hypercube memory limit (bytes)	Limit for how much memory a hypercube evaluation can allocate during a request. If multiple hypercubes are calculated during the request, the limit is applied to each hypercube calculation separately . Note that the limit is not enforced on every allocation. If the setting has the value 0, the engine applies a global heuristic to limit the amount of simultaneously executing requests that allocate a lot of memory to calculations. A negative value disables the limit. For performance reasons, memory usage and limits are checked periodically rather than on every allocation, therefore it is possible to briefly exceed the limit in some cases.	0
Reload memory limit (bytes)	Limit for how much memory a reload request can allocate. A negative value or 0 disables the limit. For performance reasons, memory usage and limits are checked periodically rather than on every allocation, therefore it is possible to briefly exceed the limit in some cases.	-1

Property	Description	Default value
Export memory limit (bytes)	Limit for how much memory the export part of an export data request can allocate. Allocations made due to calculations are not counted against this limit. A negative value or 0 disables the limit. For performance reasons, memory usage and limits are checked periodically rather than on every allocation, therefore it is possible to briefly exceed the limit in some cases.	-1
Hypercube time limit (seconds)	Limits the single core CPU time equivalent that a hypercube calculation can use. The single core CPU time equivalent is a heuristic that approximates the CPU time spent, divided by the number of cores used during the calculation. This is not a hard limit and it is dependent on the complexity of processed calculation. A negative value or 0 disables the limit. For performance reasons, the CPU time is not tracked exactly.	60
Reload time limit (seconds)	Limits the CPU time that a reload request can use. A negative value or 0 disables the limit.	-1
Export time limit (seconds)	Limits the CPU time that the export part of an export data request can use. A negative value or 0 disables the limit.	-1
Create search index during reload	When selected, all apps on the server are indexed during reload so that performance during the first search session is improved.	Selected

Logging

The **Logging** property group contains the engine logging and tracing properties in the Qlik Sense system.

Logging properties

Property	Description	Default value
Audit activity log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Basic**: a limited set of entries	Basic
Service log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Error**: only error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries	Info

TRACING

Tracing descriptions

Setting	Description	Value
Performance log interval (minutes)	The number of minutes in-between performance logging entries.	5
System log level	All the standard engine messages are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

Performance log level	All the performance messages are saved to this logger (by default updated default every five minutes). The log contains, for example, the number of active users, the number of open sessions, and the CPU load. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
QIX performance log level	All the QIX protocol performance messages are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Off
Audit log level	More detailed, user based, messages are saved to this logger, for example, when the user makes a selection in an app. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Off
Session log level	All the session messages are saved to this logger when a client session is terminated, for example, user information, machine ID, IP address and port number. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

Traffic log level	All the traffic messages are saved to this logger, for example, all JSON-messages to and from the engine. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Off
Analytic connections log level	All the analytic connections messages are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

> *The default path to the Qlik Sense log folder is %ProgramData%\Qlik\Sense\Log\<Service>.*

Tags

1. Click the text box to display the available **tags**.
2. Start typing to filter the list.

> *Connected **tags** are listed under the text box.*

Custom properties

> *If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

> *If you are running the Qlik Analytics Platform, additional settings are available, see* Qlik Analytics Platform.

6. Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

Successfully updated engine properties is displayed at the bottom of the page.

> *Changes to engine service settings require a manual restart of the engine service in order to take effect. A restart can only be performed by an administrator who has access to the server for a manual restart.*

Editing printing

You can edit a printing service that you have update rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Printing** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select the printing services that you want to edit.
4. Click **Edit** in the action bar.
5. Edit the properties.

> *You can display or hide property groups using the panel to the far right.*

Identification

The **Identification** property group contains the basic printing properties in the Qlik Sense system. All fields are mandatory and must not be empty.
The **Node** property is the name of the printing service. The **Node**'s default value inherits the node name.

Logging

Logging properties

Property	Description	Default value
Audit activity log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

Property	Description	Default value
Service log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Error**: only error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries	Info

> *The default path to the Qlik Sense log folder is %ProgramData%\Qlik\Sense\Log\<Service>.*

Tags

Tags properties

Property	Description
Tags	*If no tags are available, this property group is empty.* Connected tags are displayed under the text box.

Custom properties

> *If no **custom properties** are available, this property group is not displayed at all (or displayed but empty) and you must make a **custom property** available for this resource type before it will be displayed here.*

Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

6. Click **Apply** in the action bar to save your changes.

Successfully updated is displayed at the bottom of the page.

Using custom properties

You create a custom property to be able to use your own values in the security rules. You define one or more values for the custom property, and use these in the security rule for a resource.

> *You might, for example, want to add a custom property named Country and assign two values (USA and UK) to be able to create different security rules for the two regions.*

To use custom properties

1. Log into QMC
2. Select **Custom Properties**.
3. Create or edit custom property.
4. Select resource types.
5. Create values.
6. Select resource and apply value.
7. Create security rule using custom property.

    Access right based on custom property is implemented.

Creating a custom property

You can create a custom property.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Custom properties** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Click ⊕ **Create new** in the action bar.
4. Edit the properties.

    ### Identification

    Identification properties

Property	Description
Name	The custom property name is mandatory and must not be empty. The value must only use characters and numbers (A-Z and 0-9) and must begin with a character (A-Z).
Description	Optional. Add a description of the custom property.

Resource types

Resource properties

Property	Description
Resource types	Select the resources that you want to make the custom property available for. Custom properties can be applied to the following resources: • **Analytic connections** • **Apps** • **Content libraries** • **Data connections** • **Engines** • **Extensions** • **External program task** • **Nodes** • **Printing** • **Proxies** • **Reload tasks** • **Repositories** • **Schedulers** • **Streams** • **System notifications** • **User synchronization tasks** • **Users** • **Virtual proxies**

Values

The values that you create can be used in security rules
Do the following:

1. Click ⊕ **Create new** in the **Values** heading. Type the value and click **OK** to add the value.

   > *The value must be applied to a resource before it can be used in security rules.*

2. Click ⊗ to delete a value from the **Values** list.

3. Click **OK** to confirm the deletion.

5. Click **Apply** in the action bar to create and save the custom property.
   Successfully added is displayed at the bottom of the page.

You can use the new custom property and its values on resources and in security rules.

Editing a custom property

You can edit a custom property that you have update rights to.

> ℹ️ *You cannot edit properties for several custom properties at the same time.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Custom properties** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select one custom property and click **Edit** in the action bar at the bottom of the page.
4. Edit the properties.

Identification

Identification properties

Property	Description
Name	The custom property name is mandatory and must not be empty. The value must only use characters and numbers (A-Z and 0-9) and must begin with a character (A-Z).
Description	Optional. Add a description of the custom property.

Resource types

Resource properties

Property	Description
Resource types	Select the resources that you want to make the custom property available for. Custom properties can be applied to the following resources: • **Analytic connections** • **Apps** • **Content libraries** • **Data connections** • **Engines** • **Extensions** • **External program task** • **Nodes** • **Printing** • **Proxies** • **Reload tasks** • **Repositories** • **Schedulers** • **Streams** • **System notifications** • **User synchronization tasks** • **Users** • **Virtual proxies**

Values

The **Values** that you create can be used in security rules.

Click ⊕ **Create new** in the **Values** heading; type the value and click **OK** to add the value.

> ℹ️ *The value must be applied to a resource before it can be used in security rules.*

Click ⊗ to delete a value from the **Values** list and click **OK** to confirm.

5. Click **Apply** in the action bar.

Successfully updated is displayed at the bottom of the page.

Deleting a custom property

You can delete custom properties that you have delete rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Custom properties** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the custom properties that you want to delete.

4. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.

5. Click **OK**.

Applying custom property values

To be able to use custom property values in the security rules, you must first apply the custom property values to a resource.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select a resource on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select one or more resources and click **Edit**.

4. Select **Custom properties** from the **Properties** panel.

   > *If **Custom properties** is not available in the properties panel, you must first make a custom property available for the resource. You do this when you create (or edit) a custom property.*

5. Click the text box next to the custom property to display a list of available values.

6. Select the values that you want to use.
   The values are displayed under the text box.

7. Click **Apply** in the action bar.
   Successfully added is displayed at the bottom of the page.

You have now applied custom property values, and you can use them when creating security rules for the resource.

Custom properties – read-only access to all resources

You create a custom property to be able to use your own values in the security rules. You define one or more values for the custom property, and use these in the security rule for a resource.

For example, you may want to set up read-only access to all resources for some users, who will only be reviewing work. To do this, you create a custom property with one value, apply it to a security rule, and apply the rule to users who need it.

Creating custom properties

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Open **Custom properties**.

3. Click ⊕ **Create new**.

4. Name the customer property *AccessAllResources*.

5. Optional. Add a description.

6. Under **Resource types**, select **Users**.

7. Under **Values**, click ⊕ **Create new** and name the value *ReaderOnly*.

8. Click **Apply**.

You have now created a custom property with one value that can be used to give users read access to all resources. You can easily create additional values according to your needs, for example, a value that gives users rights to create, update, and publish.

> *You can create custom properties for more than one resource type, if needed. In this example, it is sufficient to select **Users**. When you create the security rule, the resource filter will be used to grant access to all resources.*

Creating security rules

Do the following:

1. In the QMC, open **Security rules**.

2. Click ⊕ **Create new**.

3. Name the security rule *ReaderAccess*.

4. Add a description: This rule grants *ReaderOnly* members of the custom properties group *AccessAllResources* read access to all resources.

   > *By default, the **Resource filter** field has an asterisk, indicating that all resources are selected. Click ▼ next to the text box to view the resources.*

5. Under **Basic**, ensure that the action **Read** is selected.

6. In the rule creation box, click the **name** list and select @AccessAllResources.

7. Click the empty text box next to **value** and select ReaderOnly.

8. The **Conditions** box in the **Advanced** section should now contain the following string: ((user.@AccessAllResources="ReaderOnly"))

   > *In the **Context** list, you can select if the rule is to be applicable in the hub, QMC, or both.*

9. Click **Apply**.

> *If you are connected to a user directory, the directory may contain properties that can be used in security rules.*

Applying custom properties to users

Do the following:

1. In the QMC, open **Users**.

2. Select one or more users.

> *Use Ctrl+Click to select multiple users.*

3. Click **Edit**.

4. On the **Edit user** page, ensure that the **Custom properties** section is displayed.

5. Click the text box for the custom property AccessAllResources and select ReaderOnly.

6. Click **Apply**.

The selected users now have read access to all the resources in the QMC and can view apps, streams, content libraries, and so on.

Using tags

You create tags and apply them to resources to be able to search and manage the environment efficiently from the resource overview pages in the QMC.

Creating tags

You can create a tag. Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Tags** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Click ➕ **Create new** in the action bar.

4. Type a tag name.

Identification

Identification properties

Property	Description
Name	The name of the tag. The name must be unique.

View tag associated items

The property group **View tag associated items** displays which resources that are using the tag. The connections are made from the **Tags** property group when editing a resource.
The property group **View tag associated items** contains the following resources:

- **Apps**
- **App objects**
- **Security rules**
- **Extensions**

- **Content libraries**
- **Data connections**
- **Nodes**
- **Engines**
- **Proxies**
- **Virtual proxies**
- **Repositories**
- **Schedulers**
- **Streams**
- **Users**
- **User directory connectors**
- **Reload tasks**
- **User synchronization tasks**
- **Custom banner messages**

5. Click **Apply** in the action bar to create and save the tag.
   Successfully added new tag is displayed at the bottom of the page.

Connecting tags

You can connect a tag to a resource.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select a resource type (for example, **Apps**) on the QMC start page, or from the **Start**▼ drop-down menu, to display the overview.

   > *You can filter a column by using the filtering option:* ▾

3. Select the items that you want a tag to connect to.

4. Click **Edit** in the action bar.

5. Ensure **Tags** is selected in the **Properties** section.

6. Click the **Tags** text box to see a list of available tags.

   > *If the tag is not available, you must first create the tag. You can neither create nor delete tags when you are editing a resource. You create tags in the **Tags** section, which is available on the start page.*

7. To filter the list, start typing the tag name.

8. Select a tag.
   The tag will added in blue under the text box.

9. Click **Apply** at the bottom of the page to save your changes.

(x) is added to the label of the tag, where x denotes how many of the resources being edited that use the tag.

You have now connected a tag to the resource.

Disconnecting tags

You can remove the connection between a tag and a resource.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select a resource type (for example, **Apps**) on the QMC start page, or from the **Start**▼ drop-down menu, to display the overview.

   > *You can filter a column by using the filtering option:* ⌐▼

3. Select the items you want to remove a tag from and click **Edit** in the action bar.
4. Ensure that **Tags** is selected in the **Properties** section.
5. Under the **Tags** text box, click ✖ to remove the tag.
6. Click **Apply** at the bottom of the page to save your changes.

Editing tags

You can edit tags that you have update rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Tags** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select the tags that you want to edit.
4. Click **Edit** in the action bar.
5. Edit the properties.

   ### Identification

   Identification properties

Property	Description
Name	The name of the tag. The name must be unique.

   ### View tags associations

   The property group **View tag associated items** displays which resources that are using the tag. The connections are made from the **Tags** property group when editing a resource.
   The property group **View tag associated items** contains the following resources:
   - **Apps**
   - **App objects**

- **Security rules**
- **Extensions**
- **Content libraries**
- **Data connections**
- **Nodes**
- **Engines**
- **Proxies**
- **Virtual proxies**
- **Repositories**
- **Schedulers**
- **Streams**
- **Users**
- **User directory connectors**
- **Reload tasks**
- **User synchronization tasks**
- **Custom banner messages**

6. Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

Successfully updated tag is displayed at the bottom of the page.

Deleting tags

You can delete tags that you have delete rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Tags** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

3. Select the tags that you want to delete.

> *You can filter a column by using the filtering option:* �

4. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.

5. Click **OK**.

1.7   QMC performance – best practices

To maintain optimal performance in the Qlik Management Console (QMC), it is important that you know about some of the key factors affecting QMC performance. By following the advice in this topic, you reduce the risk of experiencing slow response times and other issues originating from inappropriate use of the QMC.

Suggestions for improved performance

When planning, setting up, and maintaining the QMC, consider the following options for improved performance. Some of them involve minor sacrifices that may be worthwhile.

- Number of admins: The QMC is not designed to be a self-service tool, it is intended for a limited number of administrators. Keeping the number of admins down benefits performance.
- Number and size of apps: Housekeeping is recommended. Check for unused or rarely used apps and remove them, if possible. Very large apps might be split into smaller ones.
- Design of the security rules: Properly designed security rules can improve performance, see *Security rules (page 445)*.
- Security rules caching, see *Security rules caching (page 445)*.
- Counters: Queries for showing numbers in the QMC can be removed to improve performance.
- Custom filters: Use custom filters to quickly access the data you want to work with. Data connected to custom filters is cached in the browser. When you switch between custom filtered views, only changes to the data are loaded. This is faster than a full table reload. See *Managing custom filters in table views (page 27)*.

Security rules

Security rules grant users access to resources where they can perform certain actions, such as create, read, update, and delete, given that certain conditions are fulfilled.

Security rules are always inclusive, that is, they are always used to grant a user access. A security rule never actively excludes a user, but if a user is not included in any security rule granting access, the user is, in effect, denied access. The main point, though, is that it is sufficient that there is one rule for granting a user access to a resource for the user to be able to access the resource. That many rules, indirectly, exclude the user is irrelevant.

When a security rule grants access to a resource rule evaluation stops. The worst-case scenario for rule evaluation is when a user has no privileges at all, in which case all security rules are evaluated.

Security rules caching

The Qlik Sense security rule mechanism includes two different cache layers that have been implemented to increase rule evaluation performance:

- Security rule cache (rule engine)
- Security filter result cache (Qlik Sense Repository Service)

Security rule cache

The rule engine is a component used for parsing rules to evaluate access to resources. The security rule cache exists in the rule engine and consists of parsed system rules. The cache is not stored in the database and is deleted when Qlik Sense Repository Service is restarted. If there are no changes to the security rules, the cache will not be reset, which benefits performance. Security rule evaluation is not cached for static content.

When the rule engine filters out what rules to use, depending on the resource filter, context, and actions, the rules are sorted with the ones granting access most frequently first.

Security filter result cache

This cache exists in Qlik Sense Repository Service. Using this cache avoids using the rule engine. The cache is not stored in the database and is deleted when Qlik Sense Repository Service is restarted. There are three cache categories that are invalidated (deleted) in different ways:

• Global cache: Any change to security rules, load balancing rules, license rules, or custom properties, will trigger complete invalidation of the cache. As a consequence, any optimizations gained since the session started are lost.

• User cache: Changes to user attributes or custom properties will trigger user-based invalidation, that is, the cache related to that specific user is deleted.

• Entity cache: Any change to a single entity (for example, changing app name or owner) will trigger entity-based invalidation, that is, the cache related to that specific entity is deleted.

Related logs

The following logs are related to cache invalidation of security filter results. You can use them for troubleshooting and monitoring purposes. The logs are found here:
C:\ProgramData\Qlik\Sense\Log\Repository\Trace\HOST_NAME_Audit_Repository.txt.

Global cache invalidation

```
Invalidating entire security filter result cache due to {reason} (Logged at Info level)
```

User cache invalidation

```
Invalidating security filter result cache for user with id: {userId} (Logged at Debug level)
```

Entity cache invalidation

```
Invalidating security filter result cache for entity (type_id): {entity.Type.Name}_{entity.Id}
```
(Logged at Debug level)

Guidelines for writing performance efficient security rules

The following guidelines represent general best practices when writing security rules. In addition to these common guidelines, your specific environment may have more potential improvements that are not presented here.

Use specific resource filter

Before access to a resource is evaluated, the rules that apply to that resource are filtered out with the resource filter. Therefore, it is important that the resource filter is as specific as possible. The more specific the filter, the fewer the rules that must be processed by the rule engine.

The following table shows an example of resource filters of different efficiency.

Resource filters

Resource filter	Evaluation target	Efficiency

*	All resources	Least efficient
app*	All resources that start with "app" (for example, *app*, *app.object*)	More efficient than the above
app_*	App resources	More efficient than the above
app_644d2485-d318-45b0-996e-29f5d379cac2	App resource with id 644d2485-d318-45b0-996e-29f5d379cac2	Most efficient

Even if the last example is the most efficient, it also has very limited reusability. The general recommendation is to specify resource type to a level where any test on resource type in the rule is unnecessary.

Use correct context and target specific actions

Before access to a resource is evaluated, rules that apply to that resource are filtered with the correct context and actions.

Only in hub, **Only in QMC**, or **Both in hub and QMC** are the three context alternatives. Again, be as specific as possible. The first two are more efficient because only one case is evaluated. Furthermore, you should specify the actions that the rule should allow rather than using full CRUD access (create, read, update, delete).

Avoid traversing several object reference boundaries

In many cases it improves efficiency to be as specific as possible, but not always. The following two examples show rules that are designed to give a user read access to a reload task.

Example 1:

`user@property=resource.app.stream@property`

Outcome: The user can read a reload task if the user has a custom property that matches a custom property on the stream of the app of the task.

Inefficient, object reference boundaries (`app` and `stream`) are traversed, which is expensive.

Example 2:

`user.@property=resource.@property`

Outcome: The user can read a task if the user has a custom property that matches a custom property directly on the task.

More efficient, avoids traversing boundaries.

Minimize the number of custom properties

Less is sometimes more efficient. Keeping the number of custom properties to a minimum is advantageous.

Example 3:

`user.@CustomProperty=resource.@CustomProp2`
Not recommended because two custom properties must be fetched from the repository.

Example 4:

```
user.@customProperty=“ReaderOnly”
```
Recommended because only one custom property must be fetched from the repository.

Order of execution in rule syntax matters

When writing rules, you should have the more expensive operation last. In the following examples, it is enough that one of the conditions is true. If the less expensive operation comes first and is `true`, the more expensive operation never needs to be evaluated.

Example 5:

```
resource.app.stream.owner.@a = “b” or user.name = “user1”
```

Less efficient because the more expensive operation is evaluated first.

Example 6:

```
user.name = “user1” or resource.app.stream.owner.@a = “b”
```
More efficient, the more expensive operation comes last, and will only be evaluated if the first operation is false.

Avoid hard coded values – use attributes instead

It is preferable to use a rule like `resource.@property == user.name`, instead of several rules with hard coded strings `resource.@property == "user1"`, `resource.@property == "user2"`.

HasPrivilege is less efficient

If possible, avoid `HasPrivilege("action")` as it triggers a second rule evaluation.

Example 7:

```
App.Stream.HasPrivilege("read")
```

The function creates a new instance of the rule engine that triggers a second evaluation of the rules.

Like operator is less efficient

If possible, avoid `(EXPRESSION) like (EXPRESSION)` as it can have negative impact on rule evaluation performance.

Example 8:

```
resource.name like unit*"
```

The like operator compares by each character of the string, in contrast to the equal (=) operator, which compares the entire string.

See also:

1.8   Configuring Qlik Sense Enterprise on Windows

When Qlik Sense Enterprise on Windows is installed, the site must be prepared for the Qlik Sense users to be able to access the hub and start using Qlik Sense. This is the recommended workflow when you configure Qlik Sense Enterprise on Windows after installation:

Do the following:

1. If not performed during the installation, activate the license. This will:
   - Make you the root admin for the site.
   - Provide analyzer and professional access for a defined number of users. (user-based license)
   - Provide tokens that can be used on access types (token-based license).
2. If not performed during the installation, allocate user access to yourself.
3. Add a user directory connector in the QMC to prepare for import of users.
4. Synchronize with user directories to retrieve users from the directory service configured by the user directory connector.
5. Add additional admin users, if more administrators than the root admin are to be given access to the QMC.
6. Provide the users with an access type: **Professional access** or **Analyzer access** (user-based license), or **User access** or **Login access**, (token-based license), so that they can access streams and apps in the hub.
7. Create new streams.
8. Create the security rules for the streams to enable the users to read from and/or publish to the streams. Analyzer access does not grant publishing rights.

The Qlik Sense Enterprise on Windows environment is now available for the Qlik Sense users.

> *By default all Qlik Sense users have read and publish rights to the default stream called **Everyone**.*

Default configuration

A Qlik Sense installation includes the streams **Everyone** and **Monitoring apps**, and six administrator roles: **RootAdmin**, **AuditAdmin**, **ContentAdmin**, **DeploymentAdmin**, **HubAdmin**, and **SecurityAdmin**.

The default configuration of a Qlik Sense installation is as follows:

- All authenticated users have read and publish rights to the **Everyone** stream.
- Anonymous users have read rights to the **Everyone** stream.
- The administrator roles **RootAdmin**, **ContentAdmin**, and **SecurityAdmin** have read and publish rights to the **Monitoring apps** stream.

- The **RootAdmin** has full access rights to all Qlik Sense resources.
- The other administrators can access subsets of the Qlik Sense resources.
- Proxy load balances to local engine.
- An anonymous user is not allowed to create content.
- There can only be one owner of an owned object.
- Only the owner of an unpublished app can see it.
- A published app is locked for editing.
- Authenticated users (not anonymous) can:
  - Publish apps they own.
  - Create new private app objects for unpublished apps.
  - Create new private app objects for published apps (sheets, bookmarks, snapshots and stories).
  - Export the app data they are allowed to see.
- Everyone can manage data connections from Qlik Sense, but only **RootAdmin**, **ContentAdmin**, and **SecurityAdmin** can manage data connections of the type Folder directory.
- Everyone can view extensions.
- Everyone with update rights for a content library can manage its corresponding files.

Configuring security

You manage the following Qlik Sense security settings from the QMC:

- Admin roles to grant users QMC administrator access of various extent.
- Authentication for different user authentication methods.
- Proxy certificate for communication between the web browser and the proxy.
- Virtual proxies to allow different modules based on the URI to be used to access Qlik Sense.
- Custom properties to allow using your own values in security rules.
- Access control and security rules to grant user access to Qlik Sense resources.

> *For some useful tips regarding how to work with the QMC, see QMC performance – best practices (page 444).*

Adding root admin and admin users

The first user that accesses the QMC and adds the server license, obtains the role root administrator (RootAdmin) for the Qlik Sense system. This user has full access rights to all resources in the site: security rules, streams, nodes, and so on. Additional users can be assigned as RootAdmin or other admin roles with different administrative rights.

This workflow illustrates adding QMC administrators:
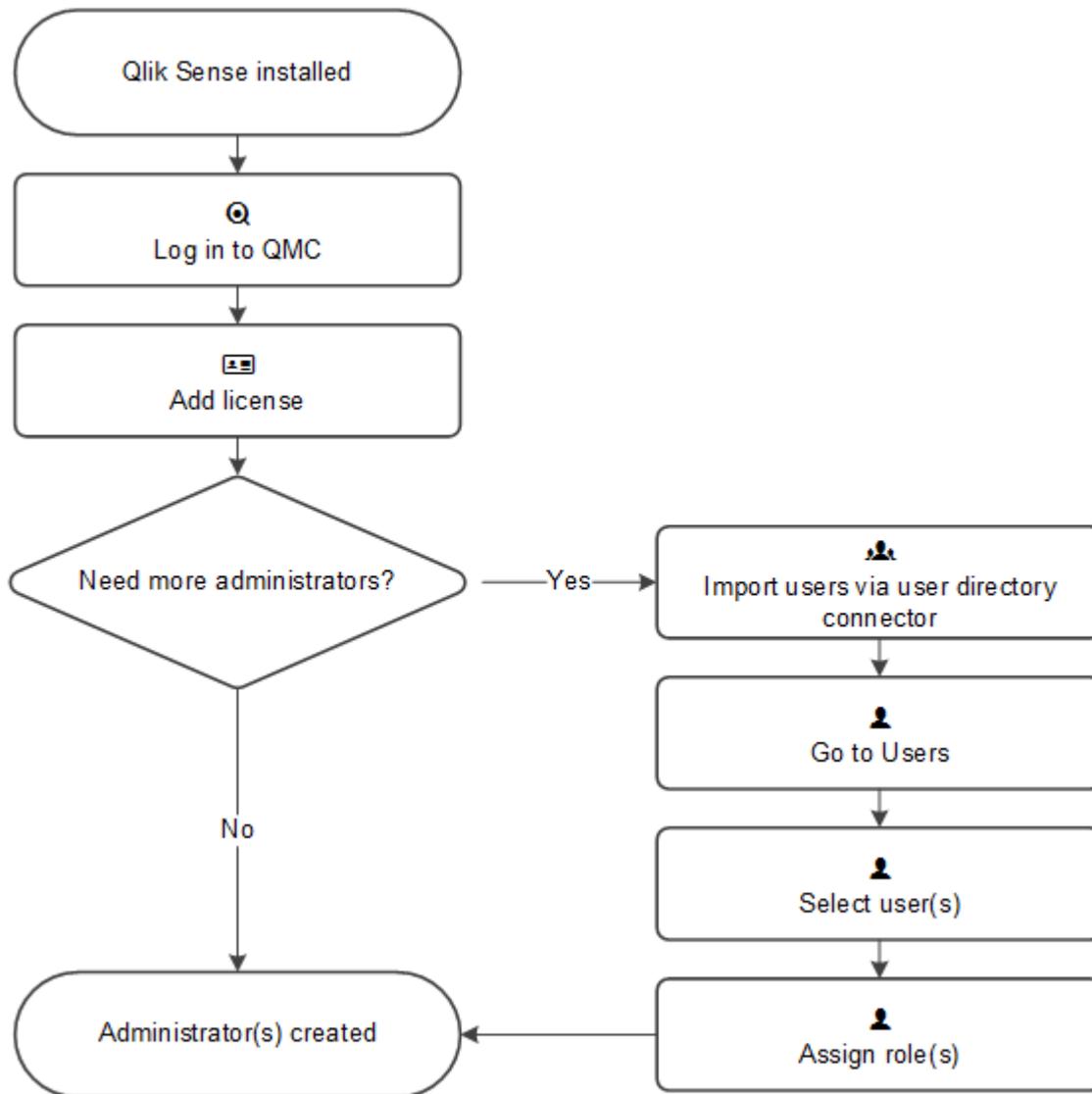
Setup workflow for a root administrator (RootAdmin)

Do the following:

1. Verify that Qlik Sense is installed.
2. Log in to the (QMC) using the Windows account that you want to use as root administrator (RootAdmin).
3. Add the LEF license to the QMC.

> *Adding the LEF makes you the root administrator for the Qlik Sense site.*

4. To add more administrators, see *Setup workflow for an admin user (page 451)*.

The root administrator role is now created.

Setup workflow for an admin user

Do the following:

1. Log in as root administrator (RootAdmin).

2. Import users via the user directory connector.

3. Select **Users** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.

4. Select the users that are to have administrative rights and click **Edit**.

5. Click ➕**Add role** and select one of the roles in the drop-down list. You can also type the name of a new role, but this role will not be valid until it has been properly defined.

> 💡 *You can assign several administration roles to a user.*

> ℹ️ *You cannot remove the root administrator role from yourself. This is to prevent you from accidentally blocking the RootAdmin from using the QMC.*

Administrators roles are now created.

> ℹ️ *Like in Qlik Sense, if a user does not have access to a resource in the QMC, the user cannot access it in the QMC interface. For example, if you change a user's role from RootAdmin to DeploymentAdmin, the user can no longer access the apps, sheets, streams, or data connection pages in the QMC.*

> ℹ️ *The root administrator cannot change or delete the security rules that are delivered with the Qlik Sense system. These security rules are listed in the **Security rules** overview page with **Type** set to **Default**.*

Default administration roles

The QMC is delivered with a set of predefined administration roles. Each role is associated with security rules tailored for specific purposes. The RootAdmin is created on installation. This role is automatically assigned to the user who provided the first valid license key to the QMC. The RootAdmin has full access rights to all Qlik Sense resources.

The *Administration rights (page 452)* table displays an overview of the default QMC administrator roles, which parts of the QMC they can manage, and what administration rights they have. A HubAdmin cannot manage any areas of the QMC. This role has administration rights only in the hub. For more information see *HubAdmin (page 546)*.

> 💡 *As RootAdmin or SecurityAdmin you have the possibility to create new roles to suit your purposes.*

> ℹ️ *For some useful tips regarding how to work with the QMC, see QMC performance – best practices (page 444).*

Administration rights

The *Legend (page 454)* describes the actions presented in this table.

Administration rights

QMC resource	AuditAdmin	ContentAdmin	DeploymentAdmin	HubAdmin	SecurityAdmin
Stream_*	R	CRUDPO	R (Monitoring apps stream)	-	CRUDPO
App*	RA	CRUDEPAO	RUA	-	CRUDEPAO
App.Object*	R	CRUDPO	R (Monitoring apps)	-	CRUDPO
DataConnection_*	R	CRUDO	-	-	CRUDO
Extension_*	R	CRUDO	R	-	R
ContentLibrary_*	R	CRUDO	R	-	CRUDO
ContentCacheControl_*	-	R	-	-	R
UserDirectoryConnector*	R	CRUD	CRUD	-	CRUD
ServerNodeConfiguration_*	R	-	CRUD	-	R
Engine*	R	-	CRUD	-	-
Proxy*	R	-	CRUD	-	CRUD
VirtualProxy*	R	-	CRUD	-	CRUD
Repository*	R	-	CRUD	-	-
Scheduler*	R	-	CRUD	-	-
ReloadTask_*	R	CRUD	CRUD	CRU	-
UserSyncTask_*	R	CRUD	CRUD	-	CRUD
SchemaEvent_*	R	CRUD	CRUD	CRU	-
CompositeEvent_*	R	CRUD	CRUD	-	-
User*	R	CRUD	CRUD	-	CRUD
SystemRule_*	R	CRUD	CRUD	-	CRUD
CustomProperty*	R	CRUD	CRUD	-	CRUD
License_*	R	R	CRUD	-	R
Tag_*	R	CRUD	CRUD	-	CRUD
FileExtension	R	CRD	-	-	CRD
FileExtensionWhiteList	R	RU	-	-	RU
AnalyticConnection_*	R	CRUD	R	-	CRUD

QMC resource	AuditAdmin	ContentAdmin	DeploymentAdmin	HubAdmin	SecurityAdmin
TermsAcceptance_*	R	R	CRUD	-	R
ServiceStatus_*	R	-	CRUD	-	R
ServiceCluster	R	-	CRUD	-	-
LoadBalancingSelectList	R	-	R	-	-
CustomBannerMessage_*	-	R	CRUD	-	CRUDEPOLM
*(All in Audit view)	R	-	-	-	-

Legend

The following table presents the actions that are available for administrators.

[caption]

Action	Description
C: **Create**	Create resource
R: **Read**	Read resource
U: **Update**	Update resource
D: **Delete**	Delete resource
E: **Export**	Export an app
A: **Export data**	Export app data
P: **Publish**	Publish a resource to a stream
O: **Change owner**	Change the owner of a resource
L: **Change role**	Change the role of a user
B: **Load balancing**	Balance load for nodes and virtual proxies
M: **Access offline**	Access apps offline

QMC section access for default admin roles

The QMC is delivered with a set of predefined administration roles. Each role is associated with QMC section access rules that grant administrators read access to sections in the QMC according to their needs. The RootAdmin has access to all QMC sections.

> The QMC section access rules only grant read access to a QMC section. For a presentation of the other rights, such as create, edit, update, and so on, see: Legend (page 454). The HubAdmin can only access the hub and does not have access to QMC.

Read access rights for default administrators

An "R" indicates that an admin has read access to that QMC section.

Access rights for default administrators

QMC	AuditAdmin	ContentAdmin	DeploymentAdmin	SecurityAdmin
QmcSection_Audit	R	R	R	R
QmcSection_Tag	R	R	R	R
QmcSection_Stream	-	R	-	R
QmcSection_App	-	R	R	R
QmcSection_App.Object	-	R	-	R
QmcSection_DataConnection	-	R	-	R
QmcSection_AnalyticConnection	-	R	-	R
QmcSection_User	-	R	R	R
QmcSection_CustomPropertyDefinition	-	R	R	R
QmcSection_Task	-	R	R	-
QmcSection_Event	-	R	R	-
QmcSection_SchemaEvent	-	R	-	-
QmcSection_CompositeEvent	-	R	-	-
QmcSection_Extension	-	R	-	-
QmcSection_ReloadTask	-	R	R	-
QmcSection_UserSyncTask	-	R	R	-
QmcSection_ContentLibrary	-	R	-	R
QmcSection_Templates	-	-	R	R
QmcSection_ServerNodeConfiguration	-	-	R	-
QmcSection_ServiceCluster	-	-	R	-
QmcSection_EngineService	-	-	R	-
QmcSection_ProxyService	-	-	R	R

QMC	AuditAdmin	ContentAdmin	DeploymentAdmin	SecurityAdmin
QmcSection_ VirtualProxyConfiguration	-	-	R	R
QmcSection_ RepositoryService	-	-	R	-
QmcSection_SchedulerService	-	-	R	-
QmcSection_PrintingService	-	-	R	-
QmcSection_Licenses	-	-	R	-
QmcSection_ License.LoginAccessType	-	-	R	-
QmcSection_ License.UserAccessType	-	-	R	-
QmcSection_ License.UserAccessRule	-	-	R	-
QmcSection_ License.ApplicationAccessTyp e	-	-	R	-
QmcSection_Token	-	-	R	-
QmcSection_UserDirectory	-	-	R	-
QmcSection_Certificates	-	-	R	R
QmcSection_ Certificates.Export	-	-	R	R
QmcSection_SyncRule	-	-	R	-
QmcSection_ LoadBalancingRules	-	-	R	-
QmcSection_ CustomBannerMessage	-	R	R	R
QmcSection_SystemRule	-	-	-	R

Authentication

After a standard Qlik Sense installation, the Qlik Sense Proxy Service (QPS) includes a module that handles authentication of Microsoft Windows users.

You can use other authentication methods, and it is also possible to implement customized solutions for authentication.

Mutual authentication (also known as two-way authentication) is not supported in Qlik Sense.

Anonymous authentication

You can allow users to access Qlik Sense without supplying the user identity and credentials. This is done by editing the virtual proxy property **Anonymous access mode**. There are various levels of anonymous use, see the descriptions in the procedure below.

> *User-based licenses, with professional access and analyzer access, do not support anonymous authentication. Capacity-based licenses will allow anonymous authentication using an Analyzer Capacity license (signed key) or a Token license.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Virtual proxies** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the virtual proxy that handles the authentication and click **Edit**.
4. Edit **Anonymous access mode** in the **Authentication** property group:
   - Select **Allow anonymous user** in the drop-down list if you want a user to enter as anonymous and then be able to switch to a user account.
   - Select **Always anonymous user** if all users always are to be anonymous.

   The default value is **No anonymous user** and the Qlik Sense users must supply the user identity and credentials.
5. Click **Apply** in the action bar to apply and save your changes.
   Successfully updated is displayed at the bottom of the page.

For the anonymous authentication method to be operational, you need to create a license rule that allows anonymous users for either an Analyzer Capacity license (requires a signed license key) or a Login Access Token.

Analyzer Capacity license

Do the following:

1. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
2. Select **Analyzer capacity rules**.
3. Click ⊕**Create new** in the action bar.
4. Edit the Identification properties.

Identification properties

Property	Description
Name	Enter a name for the rule (mandatory).
Description	Provide a brief explanation of the rule (optional).

5. Create either a basic or an advanced rule:

    a. Under **Basic** properties, do the following:

        • Select **user**: `userDirectory =`

        • Select **value**: `NONE`

    b. Under Advanced properties, do the following:

        • In the Conditions field, add `user.IsAnonymous()`

6. Click **Apply** in the action bar.

Anonymous use of Qlik Sense is now allowed.

Login Access Token

Do the following:

1. Select **License management** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
2. Click **Login access rules**.
3. Select a rule to edit and click **Edit** in the action bar.
4. Click **License rules** under **Associated items**.
5. Select the license rule that you want to edit and click **Edit** in the action bar.
6. In the **Advanced** section, add *user.isAnonymous()* in the **Conditions** text field.

Anonymous use of Qlik Sense is now allowed.

> 𝐆→   *Anonymous users can use the default Everyone stream in the hub, which has already been set up for anonymous access. You can also create a stream dedicated to anonymous users. For more information about creating a stream for anonymous users, see* How to allow Anonymous Hub access in *Qlik Sense Enterprise Client-Managed.*

Authentication methods

Authentication is often used in conjunction with a single sign-on (SSO) system that supplies a reverse proxy or filter for authentication of the user.

> *Header and SAML authentication cannot be used for a default virtual proxy. If you only have a default virtual proxy you need to create a new virtual proxy for header or SAML authentication.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Virtual proxies** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
3. Select the virtual proxy that handles the authentication and click **Edit**.
4. In the **Authentication** property group, make the necessary selections.
   Depending on what authentication method you select, there are different additional fields.

Authentication properties

Property	Description	Default value
Anonymous access mode	• **No anonymous user**: Users must supply user identity and credentials. • **Allow anonymous user**: Users enter as anonymous but can switch and log in with a user account. • **Always anonymous user**: Users are always anonymous.	No anonymous user
Authenticati on method	• **Ticket**: a ticket is used for authentication. • **Header authentication static user directory**: allows static header authentication, where the user directory is set in the QMC. • **Header authentication dynamic user directory**: allows dynamic header authentication, where the user directory is fetched from the header. • SAML: SAML2 is used for authentication. • JWT: JSON Web Token is used for authentication. • OIDC: OpenID Connect is used for authentication.	Ticket
Header authenticati on header name	The name of the HTTP header that identifies users, when header authentication is allowed. Mandatory if you allow header authentication (by selecting either **Header authentication static user directory** or **Header authentication dynamic user directory** for the **Authentication method** property). ⓘ *Header authentication only supports US-ASCII (UTF-8 is not supported).*	Blank
Header authenticati on static user directory	The name of the user directory where additional information can be fetched for header authenticated users. Mandatory if you allow static header authentication (by selecting **Header authentication static user directory** for the **Authentication method** property).	Blank

Property	Description	Default value
Header authentication dynamic user directory	Mandatory if you allow dynamic header authentication (by selecting **Header authentication dynamic user directory** for the **Authentication method** property). The pattern you supply must contain '$ud', '$id' and a way to separate them. **Example setting and matching header:** $ud\\$id – matches USERDIRECTORY\userid (backslashes must be escaped with an additional \) $id@$ud – matches userid@USERDIRECTORY ($id and $ud can be in any order) $ud:::$id – matches USERDIRECTORY:::userid	Blank
Windows authentication pattern	The chosen authentication pattern for logging in. If the User-Agent header contains the Windows authentication pattern string, Windows authentication is used. If there is no matching string, form authentication is used.	Windows
Authentication module redirect URI	When using an external authentication module, the clients are redirected to this URI for authentication.	Blank (default module, that is Windows authentication Kerberos/NTLM)
SAML single logout	Select the checkbox to enable a service provider initiated flow for SAML single logout. When selected, the metadata file generated for this virtual proxy will include single logout locations for POST and Redirect bindings.	Blank

Property	Description	Default value
SAML host URI	The server name that is exposed to the client. This name is used by the client for accessing Qlik services, such as the QMC. The server name does not have to be the same as the machine name, but in most cases it is. You can use either http:// or https:// in the URI. To be able to use http://, you must select **Allow HTTP** on the edit page of the proxy that the virtual proxy is linked to. Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property).	Blank
SAML entity ID	ID to identify the service provider. The ID must be unique. Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property).	Blank
SAML IdP metadata	The metadata from the IdP is used to configure the service provider, and is essential for the SAML authentication to work. A common way of obtaining the metadata is to download it from the IdP website. Click the browse button and open the IdP metadata .xml file for upload. To avoid errors, you can click **View content** and verify that the file has the correct content and format. The configuration is incomplete without metadata.	-
SAML attribute for user ID	The SAML attribute name for the attribute describing the user ID.Name or friendly name can be used to identify the attribute. *I do not know the name of a mandatory SAML attribute (page 635)*	Blank
SAML attribute for user directory	The SAML attribute name for the attribute describing the user directory. Name or friendly name can be used to identify the attribute.If the name value is enclosed in brackets, that value is used as a constant attribute value: [example] gives the constant attribute value 'example'. *I do not know the name of a mandatory SAML attribute (page 635)*	Blank

Property	Description	Default value
SAML signing algorithm	The hash algorithm used for signing SAML requests. In order to use SHA-256, a third-party certificate is required, where the associated private key has the provider "Microsoft Enhanced RSA and AES Cryptographic Provider".	-
SAML attribute mapping	Click **Add new attribute** to map SAML attributes to Qlik Sense attributes, and define if these are to be required by selecting **Mandatory**. Name or friendly name can be used to identify the attribute.If the name value is enclosed in brackets, that value is used as a constant attribute value: [example] gives the constant attribute value 'example'. *SAML response based attributes are not taken into account when running product audit.*	-

Property	Description	Default value

JWT certificate	Add the JWT .X509 public key certificate in PEM format. The following is an example of a public key certificate.
	
	`-----BEGIN CERTIFICATE-----`
	`MIIDYTCCAkmgAwIBAgIJAM/oG48ciCGeMA0GCSqGSIb3DQEBCwU`
	`AMEcxEDAOBgNV`
	`BAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubUxHjAcBgk`
	`qhkiG9w0BCQEW`
	`D2pkZUBjb21wYW55LmNvbTAeFw0xNzAzMjAxMjMxNDhaFw0yNzA`
	`zMTgxMjMxNDha`
	`MEcxEDAOBgNVBAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9`
	`ubmUxHjAcBgkq`
	`hkiG9w0BCQEWD2pkZUBjb21wYW55LmNvbTCCASIwDQYJKoZIhvc`
	`NAQEBBQADggEP`
	`ADCCAQoCggEBALIaab/y0u/kVIZnUsRVJ9vaZ2coiB3dVl/PCa4`
	`0fyZdOIK5CvbA`
	`d0mJhuM7m/L4PldKmwh7nsPVC6SHAwgVwXASPHZQ6qha9ENChI2`
	`NfvqY4hXTH//Y`
	`FYaGLuKHD7pE7Jqt7Bhdh1zbBjrzsr1eU4Owwv9W9DxM4tVx3Xx`
	`8AUCNRoEWgObz`
	`Oqw9CfYY7/AWB8Hnr8G22X/l0/i4uJhiIKDVEisZ55hiNTEyqwW`
	`/ew0ilI7EAngw`
	`L80D7WXpC2tCCe2V3fgUjQM4Q+0jEZGiARhzRhtaceuTBnnKq3+`
	`DnHmW4HzBuhZB`
	`CLMuWaJowkKaSfCQMel6u0/Evxc8i8FkPeMCAwEAAaNQME4wHQY`
	`DVR0OBBYEFNQ9`
	`M2Y5WlRCyftHlD2oIk12YHyBMB8GA1UdIwQYMBaAFNQ9M2Y5WlR`
	`CyftHlD2oIk12`
	`YHyBMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAHO`
	`46YLxtcMcanol`
	`PUC5nGdyYchZVHkd4F5MIe82mypwFszXGvpxKQXyAIPMkTIGb1w`
	`nE/wbCfB7moxX`
	`oFo+NoASER6wtt6FPHNcCiCXHm3B+2at16nOeMLfDefhQq03Q7q`
	`jfoa+7woAYole`
	`C9fTHGAl4TMIPThGSluiVLOLgHFUHpZryI6DdiEutXiH4afXaw0`
	`mScG36Z1uvHIq`
	`dPtjb/vDm1b9jvLITe8mZ8c2is1aBCLOdFvNupARxK7U3UD6HzG`
	`Ih4x7eqo6Q9CK`
	`mKIz25FHrKTkyi1n/0+SAlOGp8PSnwrRZKmHkHbpfY5lpCuIBY9`
	`Cu2l1Xeq4QW5E`
	`AqFLKKE=`
	`-----END CERTIFICATE-----`
		Blank

JWT attribute for user ID	The JWT attribute name for the attribute describing the user ID.	Blank

Property	Description	Default value
JWT attribute for user directory	The JWT attribute name for the attribute describing the user directory. If the name value is enclosed in brackets, that value is used as a constant attribute value: [example] gives the constant attribute value 'example'.	-
JWT attribute mapping	Click **Add new attribute** to map JWT attributes to Qlik Sense attributes. If the name value is enclosed in brackets, that value is used as a constant attribute value: [example] gives the constant attribute value 'example'.	Blank
Disable optional OIDC attributes	Only to be used when syncing users through a user directory connector. When selected, the attributes **name**, **groups**, **email**, and **picture** coming from user directory connector sync are protected from being overwritten by the attributes from the OIDC.	
OpenID Connect metadata URI	The URL to the endpoint that provides configuration information for the OAuth clients to interface with the identity provider using the OpenID Connect protocol.	
Client ID	ID of the configured client at the identity provider for user authentication.	
Client secret	Secret for the client configured at the identity provider.	
Realm	Name to associate with the identity provider, used for naming consistency in multi-cloud. If the subject attribute value format is *domainname\username*, **realm** is optional. If not, **realm** is mandatory.	
sub	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values. Mandatory.	
name	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values. Mandatory.	
groups	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values.	

Property	Description	Default value
email	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values. Mandatory.	
client_id	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values.	
picture	Statements (name/value pairs) about the entity/user and metadata about the OpenID Connect service. You can use multiple, comma-separated values.	
scope	Used in the OAuth 2.0 specification to specify the access privileges when issuing an access token. For example, use this option to add a groups scope in case the identity provider requires that to support a user groups feature.	
OIDC attribute mapping	Click **Add new attribute** to map OIDC attributes to Qlik Sense attributes, and define if these are to be required by selecting **Mandatory**. Name or friendly name can be used to identify the attribute.	

5. Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.
    Successfully updated is displayed at the bottom of the page.

SAML authentication

The Security Assertion Markup Language (SAML) is a data format for authentication and authorization. One of the key benefits of SAML is that it enables single sign-on (SSO), and thereby minimizes the number of times a user has to log on to cloud applications and websites.

Three entities are involved in the authentication process:

- the user
- the identity provider (IdP)
- the service provider (SP)

The identity provider authenticates the user. When the identity provider has asserted the user identity, the service provider can give the user access to their services. Because the identity provider has enabled SSO, the user can access several service provider sites and applications without having to log in at each site.

Identity provider initiated SSO

With identity provider initiated SSO, the user logs in directly to the identity provider, which performs the SSO authentication.

We recommend that you always set RelayState to *https://<machine_name>/<vp_prefix>/hub*, because if RelayState is empty, some identity providers will send a `get` request instead of a `post` request, which will cause a failure.

> ℹ️ *If RelayState is empty, misspelled, or not part of the host allow list, the user will automatically be redirected to the hub.*

> ℹ️ *For the IdP initiated SSO to work the assertions must be signed.*

Service provider initiated SSO

With service provider initiated SSO, the user starts at the service provider site, but instead of logging in at the SP site, SSO authentication is initiated with the identity provider. In the authentication process, Qlik Sense plays the role of a service provider. When a user logs in to Qlik Sense, the login is transferred to the identity provider that handles the actual SSO authentication.

Metadata

The service provider (Qlik Sense) needs configuration information from an identity provider. This information is available as an IdP metadata file that users can download and deliver to the service provider for easy configuration. The IdP metadata is uploaded from the QMC.

> ℹ️ *Not all IdPs support download of metadata files. If download is not supported, the metadata file can be created manually.*

Qlik Sense as a service provider is to provide the identity provider with SP metadata, which is downloaded from the QMC. The metadata includes the following information:

- Assertion consumer service (ACS) URL
- Entity ID
- Security certificate

> ℹ️ *If the virtual proxy is set up with a metadata file that does not include certificates, the IdP initiated workflow will not work.*

➦   [Wikipedia: SAML 2.0](#)

Configuring SAML

With a SAML configuration, you can enable a single sign-on (SSO) solution that minimizes the number of times a user has to log on to cloud applications and websites. The SAML configuration involves the following steps:

1. Configuring the virtual proxy.
   This step includes upload of the identity provider metadata.
2. Linking the virtual proxy to a proxy.

3. Uploading the service provider metadata to the identity provider.
4. Accessing Qlik Sense by using the virtual proxy prefix.

Configuring the virtual proxy

Do the following:

1. Create a virtual proxy and select SAML as authentication method.
   Creating a virtual proxy (page 396)

   > The virtual proxy must be linked to a proxy service in order to work. However, SAML
   > authentication cannot be used for a default virtual proxy. If you only have a default virtual
   > proxy you need to create a new virtual proxy for SAML authentication.

2. (If you have already uploaded the identity provider metadata file, you can skip to the next step.) For
   the configuration to be complete, you need to upload the metadata file from the identity provider
   (**SAML IdP metadata**). Contact the identity provider if you cannot obtain the metadata from identity
   provider's website.

   Do the following:

   i. On the virtual proxy edit page, under **Authentication**, click the button for selecting the
      metadata file for **SAML IdP metadata**.
   ii. Navigate to the file and click **Open**.
   iii. Click **View content** to preview the file before you upload it.
       Invalid file format or content will generate an error when you click **Apply**.

   > If the link **View content** is displayed, a metadata file has already been uploaded. If you
   > attempt to upload a file with exactly the same content as the already uploaded file, **Apply**
   > will be disabled.

3. Stay on the virtual proxy edit page.

Linking the virtual proxy to a proxy

Do the following:

1. To the right on the **Virtual proxy edit** page, under **Associated items**, click **Proxies**.
   The **Associated proxies** page is opened.

2. In the action bar, click ⊕ **Link**.
   The **Select proxy services** page is opened.

3. Select the node to link to and click **Link**.
   The linked node is presented in the list **Associated proxies**. Your session is ended because the proxy
   has been restarted.

4. Restart the QMC.

Uploading the service provider metadata to the identity provider

Do the following:

1. Open the virtual proxy overview page and select the proxy whose metadata that you want to download.
2. Click **Download metadata**.
3. Deliver the SP metadata, either through a web interface, or physically to the identity provider.

Accessing Qlik Sense by using the virtual proxy prefix

You can access your new virtual proxy by using the virtual proxy prefix in the URI.

Do the following:

- Enter the following URI: *https://[node]/[prefix]/*.
  You access Qlik Sense through your new virtual proxy with the SAML configuration that you have designed.

> *You can create several virtual proxies, one for each SAML configuration that you need.*

SAML single logout

The Security Assertion Markup Language (SAML) has a single logout option to ensure that all identity provider (IdP) sessions for a user are properly closed.

With SAML single sign-on (SSO), you only need to log in once, and can then access several web sites without additional login prompts. This is convenient, but potentially also risky. If one or more sessions are not properly closed, they are vulnerable to attack. By using SAML single logout you can eliminate that risk.

Two alternatives exist for SAML single logout:

- Logout initiated by the IdP.
- Logout initiated by the service provider.

> *Qlik Sense only supports logout initiated by the service provider.*

Single logout initiated by the service provider

There are two use cases for single logout initiated by the service provider: one where you actively log out from the sessions, and one where the session times out.

User logout

In the user logout use case, you actively log out, for example, by clicking logout. The session is destroyed and the SAML single logout request is sent to the IdP. Then the IdP deletes the IdP session for the user and sends a logout response to the service provider (Qlik Sense). Qlik Sense then redirects to the logout page.

Session timeout

In the session timeout use case, the session times out, the web client is notified, and the SAML single logout request is sent to the IdP. Then the IdP deletes the IdP session for the user and sends a logout response to the service provider (Qlik Sense). Qlik Sense then redirects to the logout page.

Enabling SAML single logout

Before you enable SAML single logout for Qlik Sense, you need to ensure your identity provider supports it, and that it is configured correctly. For example, some identity providers require that you upload a certificate. If a certificate is required, we recommend that you use the *server.pem* certificate that is available in the following folder: *%ProgramData%\Qlik\Sense\Repository\Exported Certificates\.Local Certificates*, or a third-party certificate, if you have configured the proxy to such a certificate.

Upgrading

If you are upgrading from an earlier version of Qlik Sense, you must set up the IdP for SAML single logout.

Do the following:

1. Make sure that your IdP is set up to support SAML single logout. The metadata file should include the logout locations where Qlik Sense will send the logout requests.
2. Download new metadata from the IdP (usually available from the identity provider's web page).
3. In the **Authentication** section, on the virtual proxy edit page, add the SAML IdP metadata file with settings for SAML single logout.
4. On the same page, select **SAML single logout**.
5. Download the new metadata file from the service provider (Qlik Sense).
6. Upload the service provider metadata file to the IdP.
7. Make sure that your IdP sends the NameID during SSO. For example, Active Directory Federation Services (ADFS) require additional settings to send NameID.
8. Extract the certificate from the service provider metadata file downloaded from the **QMC** > **Virtual proxies**. Click **Download SP metadata** for the related virtual proxy.
9. Copy the certificate located between the tags *<X509Certificate>* and *</X509Certificate>* in the file.
10. In the new file, add *-----BEGIN CERTIFICATE-----* at the beginning and *-----END CERTIFICATE-----* at the end of the file.
11. Save the file with a *.pem* or a *.crt* extension.

Limitations
- If the proxy service is restarted, or the proxy settings are changed, the web client will lose the session. In the case where the proxy is restarting, there is no way of sending logout requests to the IdP. As a consequence, the web client is automatically logged in, because the IdP session is still valid, unless it has expired.
- Logout requests going from the proxy to the IdP will only support SAML HTTP Redirect binding. Incoming logout responses from the IdP to the proxy will support both SAML HTTP Redirect and SAML HTTP POST binding.

SAML configuration with Okta

The Security Assertion Markup Language (SAML) is a data format for authentication and authorization. SAML enables single sign-on (SSO), to reduce the number of times a user has to log on to access websites and applications.

SAML can be configured for authentication with third-party products. With Okta, authentication is initiated either by the identity provider (IdP) or by the service provider (SP).

Single sign-on initiated by the identity provider

The identity provider authenticates the user. When the identity provider has asserted the user identity, the service provider can give the user access to their services. Because the identity provider has enabled SSO, the user can access several service provider sites and applications without having to log in at each site.

Single sign-on initiated by the service provider

The service provider redirects the user to the identity provider, where the authentication takes place. In the authentication process, Qlik Sense plays the role of a service provider. After a successful authentication, the user can access several service provider sites and applications without additional logins.

Setting up SAML SSO with Okta requires configuration of a virtual proxy in Qlik Sense and also of the identity provider, Okta.

Creating and configuring the virtual proxy

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. In the QMC, open **Virtual proxies**.
3. Click ⊕ **Create new**.
4. In **Properties**, to the right, ensure that the sections **Identification**, **Authentication**, **Load balancing**, and **Advanced** are selected.
5. Under **Identification**, enter *okta* for **Description** and **Prefix**.
6. For **Session cookie header name**, add *-okta* at the end of the existing name so that it reads *X-Qlik-Session-okta*.
7. For **Authentication method**, select **SAML**.
8. Select **SAML single logout**. SAML single logout is a security measure to ensure that all SSO sessions are properly closed.
9. For **SAML host URI**, enter the URL users will use to access Qlik Sense, that is, the name of your server, in the following format: *https://myhost.company.com*.
10. For **SAML entity ID**, enter *okta*.
    This is a unique identifier for your Okta configuration.

    > ⓘ **SAML IdP metadata** *will be added at a later stage.*

11. For **SAML attribute for user ID**, enter *email*.

This is the user's email address, stored in Okta. You can choose a different standard or custom field within the Okta configuration to act as the user ID.

12. For **SAML attribute for user directory**, enter *[okta]*.
    This is a static attribute that requires brackets.

13. For **SAML signing algorithm**, select **SHA-1**.

14. Under **SAML attribute mapping**, click ➕ **Add new attribute**.

15. Enter *groups* as **SAML attribute** and *group* as **Qlik Sense attribute**. Clear the selection in **Mandatory**. The name *groups* is the attribute name in the SAML assertion. The attribute name *group* is the name Qlik Sense will respond to when using this attribute in security rules.

16. Under **Load balancing nodes**, click ➕ **Add new server node**.

17. Select the engine nodes this virtual proxy will load balance connections to.

18. Under **Advanced**, in the **Host allow list** section, click ➕ **Add new value**.

19. Add the host name of the Qlik Sense server, that is, the same server that you entered for **SAML host URI**.

20. Click **Apply** and then **OK** to restart the services.

21. In the **Associated items** menu to the right, select **Proxies**.

22. Click **Link** and link the virtual proxy to the proxy or proxies that will use this configuration.
    The proxy service is restarted.

23. Navigate back to the **Virtual proxies** overview page.

24. Select the *okta* configuration that you created and click **Download SP metadata** in the action bar.

25. Open the metadata that Qlik Sense generated. Check the following:

    ○ *entityID*: You need this value to enable Okta to communicate with the Qlik Sense server.

    ○ *SingleLogoutService*URL (*Location*). This is the URL Qlik Sense generates when you enter the SAML host URI and add the virtual proxy path to the end. Notice that *samlauthn* and *slo* have been added to the end. This is the URL Okta will use to communicate SAML single logout to the identity provider.

    ○ *AssertionConsumerService* URL (*Location*). This is the URL Qlik Sense generates when you enter the SAML host URI and add the virtual proxy path to the end. Notice that *samlauthn* has been added to the end. This is the URL Okta will use to communicate SAML assertions to Qlik Sense.

    ○ *NameIDFormat*: By default, the *transient* name format is specified in the metadata. It is not always required to be set this way in SAML configurations, but to ensure proper operability, you should make note of this value and set it appropriately in the configuration.

This completes the virtual proxy settings for now. You will return to this page to upload the IdP metadata file, which you retrieve from the identity provider's web page. The next step is to configure Okta.

Configuring Okta

Okta will be the identity provider in your configuration, and before you can begin configuring Okta, you need to register an account. See https://www.okta.com/ for details.

> ℹ️ *If you are installing Qlik Sense Enterprise on Windows, with Multi-Cloud, you must use a developer account for Okta.*

> ℹ️ *Because this configuration involves a third-party product, we cannot guarantee that the configuration is exactly as described here. Changes may occur in the third-party product, without our knowledge.*

Do the following:

1. In Okta, hover over **Developer Console** in the top menu and select **Classic UI**.

2. In the top menu, select **Applications**.

3. Click **Add Application**.

4. Click **Create New App**.

5. For **Platform**, select **Web**.

6. For **Sign on method**, select **SAML 2.0**.

7. Click **Create**.
   The configuration screen appears.

8. Name this app *Qlik Sense SAML configuration*.

9. Optional: Add a logo.

10. Click **Next**.
    The **SAML Settings** page appears.

11. For **Single sign on URL**, enter the *AssertionConsumerService* URL from your SP metadata file into the field. Make sure to include the trailing slash after *samlauthn*, or Qlik Sense will not accept the SAML assertion.

12. For **Audience URI (SP Entity ID)**: Enter the *entityID* value from the SP metadata you opened earlier (*okta*).

13. For **Name ID format**, select **Transient**.

14. Click **Show Advanced Settings**.

15. For **Enable Single Logout**, select **Allow application to initiate Single Logout**.

16. For **Single Logout URL**, use the following format: *https://<machine_name>/<vp_prefix>/samlauthn/slo/*

17. For **SP issuer**, use the SAML entity ID from the virtual proxy (*okta*).

18. Extract the certificate from the service provider metadata file downloaded from the **QMC** > **Virtual proxies**. Click **Download SP metadata** for the related virtual proxy.

19. Copy the certificate located between the tags *<X509Certificate>* and *</X509Certificate>* in the file.

20. In the new file, add *-----BEGIN CERTIFICATE-----* at the beginning and *-----END CERTIFICATE-----* at the end of the file.

21. Save the file with a *.pem* or a *.crt* extension.

22. Click **Upload Certificate**.

23. In the **ATTRIBUTE STATEMENTS** section, for **Name**, enter *email* and for **Value**, select *user.email*.

24. In the **GROUP ATTRIBUTE STATEMENTS** section, for **Name**, enter *groups* and for **Filter**, select **Regex** and add the following string: *^[A-Za-z0-9_.]+$*

> *You use a regular expression to define a search pattern. Only strings that match the search pattern criteria will be found. With the following search pattern: `^[A-Za-z0-9_.]+$`, a group name is found if it only contains any of the following characters: letters `A-Z`, `a-z`, numbers `0-9`,underscore (`_`), period (`.`). Note that if a name includes a dash (`-`), it does not match the search pattern, and will not be found. For more information, see* [→   Wikipedia: Regular expressions](#)*.*

25. Click **Next**.
    A feedback section is opened.
26. For the question **Are you a customer or partner?** select **I'm an Okta customer adding an internal app**.
27. Optional: Select **This is an internal app that we have created**.
28. Click **Finish**.
    The **Sign On** page is displayed. From this page you can download the IdP metadata.
29. Scroll down and click the link **Identity Provider metadata**. Qlik Sense requires that the metadata file has an xml extension, so make sure to save the file as *metadata.xml*.
30. Scroll up and select **People** in the top menu.
31. You must assign users to the app, so that they can use the connection that you have created. Click **Assign to People** and add users. (Users must have an Okta account.)

This completes the Okta configuration. A final step is needed before you can test the connection: uploading the IdP metadata to the virtual proxy.

Uploading the IdP metadata file

Do the following:

1. Navigate back to the QMC and open the *okta* virtual proxy for editing.
2. Under **Authentication**, **SAML IdP metadata**, click **Choose File**.
3. Select the metadata file downloaded from Okta.
4. Click **View content** to review the metadata.
5. Click **Apply**.
6. Click **OK** to accept the changes to the virtual proxy.
7. Click **Refresh QMC**.

You are now set to test the configuration.

Testing the Okta SAML configuration

As mentioned earlier, you can either initiate single sign-on (SSO) through a service provider or an identity provider.

Single sign-on initiated by the service provider

Do the following:

1. Open a new browsers window and navigate to the Qlik Sense server URL, including the virtual proxy path. Example: *https://myhost.company.com/okta/*
   The browser is redirected to Okta to authenticate the login request.
2. Type your user credentials.
   Okta redirects you back to the Qlik Sense hub.

Single sign-on initiated by the identity provider

1. Open a browser and navigate to www.okta.com.
2. Log in with your user credentials.
3. In the menu at the top, click **My Applications**.
   The available applications are displayed.
4. Click the Qlik Sense SAML application.
   The Qlik Sense hub is opened in a new tab.

> *We recommend that you always set RelayState to https://<machine_name>/<vp_prefix>/hub, because if RelayState is empty, some identity providers will send a `get` request instead of a `post` request, which will cause a failure. If RelayState is empty, misspelled, or not part of the host allow list, the user will automatically be redirected to the hub.*

> *For the IdP initiated SSO to work the assertions must be signed.*

SAML configuration with OneLogin

The Security Assertion Markup Language (SAML) is a data format for authentication and authorization. SAML enables single sign-on (SSO), to reduce the number of times a user has to log on to access websites and applications.

SAML can be configured for authentication with third-party products. With OneLogin, authentication is initiated either by the identity provider (IdP) or by the service provider (SP).

Single sign-on initiated by the identity provider

The identity provider authenticates the user. When the identity provider has asserted the user identity, the service provider can give the user access to their services. Because the identity provider has enabled SSO, the user can access several service provider sites and applications without having to log in at each site.

Single sign-on initiated by the service provider

The service provider redirects the user to the identity provider, where the authentication takes place. In the authentication process, Qlik Sense plays the role of a service provider. After a successful authentication, the user can access several service provider sites and applications without additional logins.

Setting up SAML SSO with OneLogin requires configuration of a virtual proxy in Qlik Sense and also of the identity provider, OneLogin.

Creating and configuring the virtual proxy

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. In the QMC, open **Virtual proxies**.
3. Click ⊕ **Create new**.
4. In **Properties**, to the right, ensure that the sections **Identification**, **Authentication**, **Load balancing**, and **Advanced** are selected.
5. Under **Identification**, enter *onelogin* for **Description** and **Prefix**.
6. For **Session cookie header name**, add *-onelogin* at the end of the existing name so that it reads *X-Qlik-Session-onelogin*.
7. For **Authentication method**, select **SAML**.
8. Select **SAML single logout**. SAML single logout is a way to make sure that all SSO sessions are properly closed.
9. For **SAML host URI**, enter the URL users will use to access Qlik Sense, that is, the name of your server, in the following format: *https://myhost.company.com*.
10. For **SAML entity ID**, enter *onelogin*.
    This is a unique identifier for your OneLogin configuration.

    > ⓘ *SAML IdP metadata will be added at a later stage.*

11. For **SAML attribute for user ID**, enter *userid*.
    This is the user's email address, stored in OneLogin. You can choose a different standard or custom field within the OneLogin configuration to act as the user ID.
12. For **SAML attribute for user directory**, enter *[onelogin]*.
    This is a static attribute that requires brackets.
13. For **SAML signing algorithm**, select **SHA-1**.
14. Under **SAML attribute mapping**, click ⊕ **Add new attribute**.
15. Enter *Email* as **SAML attribute** and *email* as **Qlik Sense attribute**. Clear the selection in **Mandatory**. (If a mandatory attribute is missing from the SAML response, Qlik Sense will reject the authentication request.)
16. Click ⊕ **Add new attribute** again, to add another attribute.
17. Enter *userid* as **SAML attribute** and *name* as **Qlik Sense attribute**. Clear the selection in **Mandatory**.
18. Under **Load balancing nodes**, click ⊕ **Add new server node**.
19. Select the engine nodes this virtual proxy will load balance connections to.
20. Under **Advanced**, in the **Host allow list** section, click ⊕ **Add new value**.
21. Add the host name of the Qlik Sense server, that is, the same server that you entered for **SAML host URI**.

22. Click **Apply** and then **OK** to restart the services.

23. In the **Associated items** menu to the right, select **Proxies**.

24. Click **Link** and link the virtual proxy to the proxy or proxies that will use this configuration.
    The proxy service is restarted.

25. Navigate back to the **Virtual proxies** overview page.

26. Select the *onelogin* configuration that you created and click **Download SP metadata** in the action bar.

27. Open the metadata that Qlik Sense generated. Check the following:

    ○ *entityID*: You need this value to enable OneLogin to communicate with the Qlik Sense server.

    ○ *AssertionConsumerService* URL (*Location*). This is the URL Qlik Sense generates when you enter
       the SAML host URI and add the virtual proxy path to the end. Notice that *samlauthn* has been
       added to the end. This is the URL OneLogin will use to communicate SAML assertions to Qlik
       Sense.

This completes the virtual proxy settings for now. You will return to this page to upload the IdP metadata file,
which you retrieve from the identity provider's web page. The next step is to configure OneLogin.

Configuring OneLogin

OneLogin will be the identity provider in your configuration, and before you can begin configuring OneLogin,
you need to register an account. See https://www.onelogin.com/ for details.

> *Because this configuration involves a third-party product, we cannot guarantee that the
> configuration is exactly as described here. Changes may occur in the third-party product, without our
> knowledge.*

Do the following:

1. In the OneLogin top menu, select **Applications**.

2. Click **Add App**.

3. In the search box, type *SAML*.
   A list of SAML templates appears.

4. Select **SAML Custom Connector (Advanced)**.

5. Change **Display Name** to *Qlik Sense SAML configuration*.

6. Click **SAVE**.

7. Click the tab **Configuration**.

8. For **Audience**, enter the entity ID from the SAML virtual proxy: *onelogin*.

9. For **Recipient**, **ACS (Consumer) URL Validator**, and **ACS (Consumer) URL**, enter the
   AssertionConsumerService URL from your SP metadata file into the field. Make sure to include the
   trailing slash after *samlauthn*, or Qlik Sense will not accept the SAML assertion.

10. For **Single Logout URL**, use the following format: *https://<myhost.company.com>/<vp_
    prefix>/samlauthn/slo/*

11. For **SAML signature element**, select the value **Assertion**.

12. Click the tab **Parameters**.

13. By default, OneLogin supplies the *NameID (fka Email)* attribute.
    This is one of the two attributes that you added in the virtual proxy setup.

14. Click **Add parameter** to add the second attribute from the virtual proxy setup.
    A **New Field** window is opened.

15. For **Field name**, type *userid*.

16. Select **Include in SAML assertion** and click **SAVE**.

17. Click the *userid* attribute.
    An **Edit Field Userid** window is opened.

18. In the **Value** list, select **Email name part** and click **SAVE**.

19. Click **SAVE** up to the right.

20. In the top menu, click **Users**, and select **Users**.

21. Click the user for whom you will add the app.

22. Click the **Applications** tab, and click the **+** sign, next to **Applications**.

23. In the **Assign New Login to <user>** window, select the *Qlik Sense SAML configuration* that you created earlier and click **CONTINUE**.

24. In the window **Edit Qlik Sense SAML Configuration Login for <user>**, click **CANCEL**.

25. In the top menu, click **Applications** and select **Applications**.

26. Click the *Qlik Sense SAML Configuration* app.

27. From the **MORE ACTIONS** list, select **SAML Metadata**.

This completes the OneLogin configuration. A final step is needed before you can test the connection: uploading the IdP metadata to the virtual proxy.

Uploading the IdP metadata file

Do the following:

1. Navigate back to the QMC and open the *onelogin* virtual proxy for editing.

2. Under **Authentication**, **SAML IdP metadata**, click **Choose File**.

3. Select the metadata file downloaded from OneLogin.

4. Click **View content** to review the metadata.

5. Click **Apply**.

6. Click **OK** to accept the changes to the virtual proxy.

7. Click **Refresh QMC**.

You are now set to test the configuration.

Testing the OneLogin SAML configuration

As mentioned earlier, you can either initiate single sign-on (SSO) through a service provider or an identity provider.

Single sign-on initiated by the service provider

Do the following:

1. Open a new browsers window and navigate to the Qlik Sense server URL, including the virtual proxy path. Example: *https://myhost.company.com/onelogin/*
   The browser is redirected to OneLogin to authenticate the login request.
2. Type your user credentials.
   OneLogin redirects you back to the Qlik Sense hub.

Single sign-on initiated by the identity provider

1. Open a browser and navigate to www.onelogin.com.
2. Log in with your user credentials.
3. In the menu at the top, click **My Applications**.
   The available applications are displayed.
4. Click the Qlik Sense SAML application.
   The Qlik Sense hub is opened in a new tab.

> *We recommend that you always set RelayState to https://<machine_name>/<vp_prefix>/hub, because if RelayState is empty, some identity providers will send a* `get` *request instead of a* `post` *request, which will cause a failure. If RelayState is empty, misspelled, or not part of the host allow list, the user will automatically be redirected to the hub.*

> *For the IdP initiated SSO to work the assertions must be signed.*

SAML configuration with AD FS

The Security Assertion Markup Language (SAML) is a data format for authentication and authorization. SAML enables single sign-on (SSO), to reduce the number of times a user has to log on to access websites and applications.

SAML can be configured for authentication with third-party products. With Active Directory Federation Services (AD FS), authentication is initiated by the service provider (SP).

Single sign-on initiated by the service provider

The service provider redirects the user to the identity provider, where the authentication takes place. In the authentication process, Qlik Sense plays the role of a service provider. After a successful authentication, the user can access several service provider sites and applications without additional logins.

Setting up SAML SSO with AD FS requires configuration of a virtual proxy in Qlik Sense and also of the identity provider, AD FS. We assume that you have already installed AD FS. This topic does not cover how to install AD FS.

> 💡 *The following video presents how to install AD FS on a Windows server:* [Qlik Sense SAML: ADFS Integration Part One of Three](#)*.*

Creating and configuring the virtual proxy

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. In the QMC, open **Virtual proxies**.
3. Click ➕ **Create new**.
4. In **Properties**, to the right, ensure that the sections **Identification**, **Authentication**, **Load balancing**, and **Advanced** are selected.
5. Under **Identification**, enter *adfs* for **Description** and **Prefix**.
6. For **Session cookie header name**, add *-adfs* at the end of the existing name so that it reads *X-Qlik-Session-adfs*.
7. For **Authentication method**, select **SAML**.
8. Select **SAML single logout**. SAML single logout is a security measure to ensure that all SSO sessions are properly closed.
9. For **SAML host URI**, enter the URL users will use to access Qlik Sense, that is, the name of your server, in the following format: *https://myhost.company.com*.
10. For **SAML entity ID**, enter *adfs*.
    This is a unique identifier for your AD FS configuration.
11. Download the IdP metadata from your AD FS server: *https://<adfs_server>/FederationMetadata/2007-06/FederationMetadata.xml*
12. Under **Authentication**, **SAML IdP metadata**, click **Choose File**.
13. Select the metadata file downloaded from AD FS.
14. Click **View content** to review the metadata.
15. For **SAML attribute for user ID**, enter *http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn*.
    This is the schema definition of the user principal name (UPN). This definition is available in AD FS manager, under **Service > Claim Descriptions**.
16. For **SAML attribute for user directory**, enter *[adfs]*.
    This is a static attribute that requires brackets.
17. For **SAML signing algorithm**, select **SHA-1**.
    This is the signing certificate that the Qlik Sense server adds to the metadata.
18. Under **SAML attribute mapping**, click ➕ **Add new attribute**.
19. Enter *http://schemas.xmlsoap.org/claims/Group* as **SAML attribute** and *Group* as **Qlik Sense attribute**. Clear the selection in **Mandatory**. If you keep the selection, and the attribute is missing from the SAML response, Qlik Sense will reject the authentication request. The SAML attribute description is available in AD FS manager, under **Service > Claim Descriptions**.
20. Under **Load balancing nodes**, click ➕ **Add new server node**.
21. Select the engine nodes this virtual proxy will load balance connections to.

22. Under **Advanced**, in the **Host allow list** section, click ➕ **Add new value**.

23. Add the host name of the Qlik Sense server, that is, the same server that you entered for **SAML host URI**.

24. Click **Apply** and then **OK** to restart the services.

25. In the **Associated items** menu to the right, select **Proxies**.

26. Click **Link** and link the virtual proxy to the proxy or proxies that will use this configuration.
The proxy service is restarted.

27. Navigate back to the **Virtual proxies** overview page.

28. Select the *adfs* configuration that you created and click **Download SP metadata** in the action bar.
You will need this metadata file when you configure the AD FS.

29. Open the metadata that Qlik Sense generated. Check the following:

    ○ *entityID*: You need this value to enable AD FS to communicate with the Qlik Sense server.

    ○ *AssertionConsumerService* URL (*Location*). This is the URL Qlik Sense generates when you enter the SAML host URI and add the virtual proxy path to the end. Notice that *samlauthn* has been added to the end. This is the URL AD FS will use to communicate SAML assertions to Qlik Sense.

    ○ *NameIDFormat*: By default, the *transient* name format is specified in the metadata. It is not always required to be set this way in SAML configurations, but to ensure proper operability, you should make note of this value and set it appropriately in the configuration.

This completes the virtual proxy settings. The next step is to configure AD FS.

Configuring AD FS

This topic describes how you configure AD FS, but not how to install AD FS. AD FS will be the identity provider in your configuration, and before you can begin configuring, you need access to AD FS.

> *Because this configuration involves a third-party product, we cannot guarantee that the configuration is exactly as described here. Changes may occur in the third-party product, without our knowledge.*

Do the following:

1. In AD FS, open the Server Manager.

2. In the menu to the right, select **Tools > AD FS Management**.

3. Click the **Trust Relationships** folder to the left.
A wizard is opened.

4. To the right, under **Actions**, select **Add Relying Party Trust**.

5. Click **Start**.

6. Select the option **Import data about the relying from a file**, navigate to the SP metadata file that you downloaded after configuring the virtual proxy, and click **Next**.

7. Type a display name for the relying party and click **Next**.

8. Select **I do not want to configure multi-factor authentication settings for this relying party trust at this time** and click **Next**.

9. Select **Permit all users access to this relying party** and click **Next**.

10. In the **Ready to Add Trust** window, click **Next**.

11. Click **Close**.
    The **Edit Claim Rules for <display name>** dialog is opened.

12. Click **Add Rule**.
    A rule template page window is opened.

13. Click **Next**.
    The rule configuration window is opened.

14. Type a claim rule name and select **Active Directory** in **Attribute store**.

15. In the **LDAP Attribute** list, select *User-Principal-Name*, and for the **Outgoing Claim Type**, select *UPN*.

16. On the second row of the **LDAP Attribute** list, select *User-Principal-Name* again and for the **Outgoing Claim Type**, select *Name ID*.

17. On the third row of the **LDAP Attribute** list, select *Token-Groups - Unqualified Names* and for the **Outgoing Claim Type**, select *Group*.

18. Click **Finish**.

19. Click **Apply** and **OK**.

20. Double-click your new relying party trust and open the **Advanced** tab.

21. Change the **Secure hash algorithm** to *SHA-1*.

22. Click **Apply** and **OK**.

PowerShell settings for the certificates

Because the certificates are self-signed, you must turn off the revocation checks for the signing certificate and the encryption certificate. You do this in Windows PowerShell.

Do the following:

1. Open **PowerShell**.

2. Enter the following string:
   ```
   Set-ADFSRelyingPartyTrust –targetname "<your target name>" –
   SigningCertificateRevocationCheck "none"
   ```
   On a new line, enter the following string:

3. ```
   Set-ADFSRelyingPartyTrust –targetname "<your target name>" –
   EncryptionCertificateRevocationCheck "none"
   ```

4. Press **Enter**.

This completes the AD FS configuration. You are now set to test the configuration.

Testing the AD FS SAML configuration

You initiate single sign-on (SSO) through the service provider.

Single sign-on initiated by the service provider

Do the following:

1. Open a new browsers window and navigate to the Qlik Sense server URL, including the virtual proxy path. Example: *https://myhost.company.com/adfs/*
   The browser is redirected to AD FS to authenticate the login request.
2. Type your user credentials.
   AD FS redirects you back to the Qlik Sense hub.

JWT authentication

JSON Web Token (JWT) is an open standard for secure transmission of information between two parties as a JavaScript Object Notation (JSON) object. JWT is used for authentication and authorization. Because JWT enables single sign-on (SSO), it minimizes the number of times a user has to log on to cloud applications and websites.

JWT structure

A JWT consists of three parts: a header, a payload, and a signature.

Header

The header usually consists of two parts: type (typ) and algorithm (alg). The algorithm is used to generate the signature.

Example:

```
{
"typ": "JWT",
"alg": "RS256"
}
```
RS256 indicates that RS256 - RSA signature with SHA256 is used to sign this token.

Payload

The payload is a JSON object that consists of the claims that you want to make. Claims are statements about an entity (usually the user) and additional metadata.

Example:

```
{
"userId":"jde",
"name":"John Donne",
"email":"jde@company.com",
"roles":["RootAdmin"],
"exp": 1472034208
}
```

Signature

The signature is used to verify the identity of the JWT sender and to ensure that the message has not been tampered with. The signature is the encoded header and payload, signed with a secret key. In the normal case, X.509 certificates are used to generate and validate the signature. In the virtual proxy in the QMC, the certificate, including the public key, is configured to validate the signatures.

Authentication is performed by verifying the signature. If the signature is valid, access is granted to Qlik Sense.

Supported signature algorithms

The following signatures are supported in Qlik Sense:

- RS256 - RSA signature with SHA256
- RS384 - RSA signature with SHA384
- RS512 - RSA signature with SHA512

Example: Accessing Qlik Sense with a signed JWT

The following example shows the steps involved when gaining access to Qlik Sense by using a signed JWT.
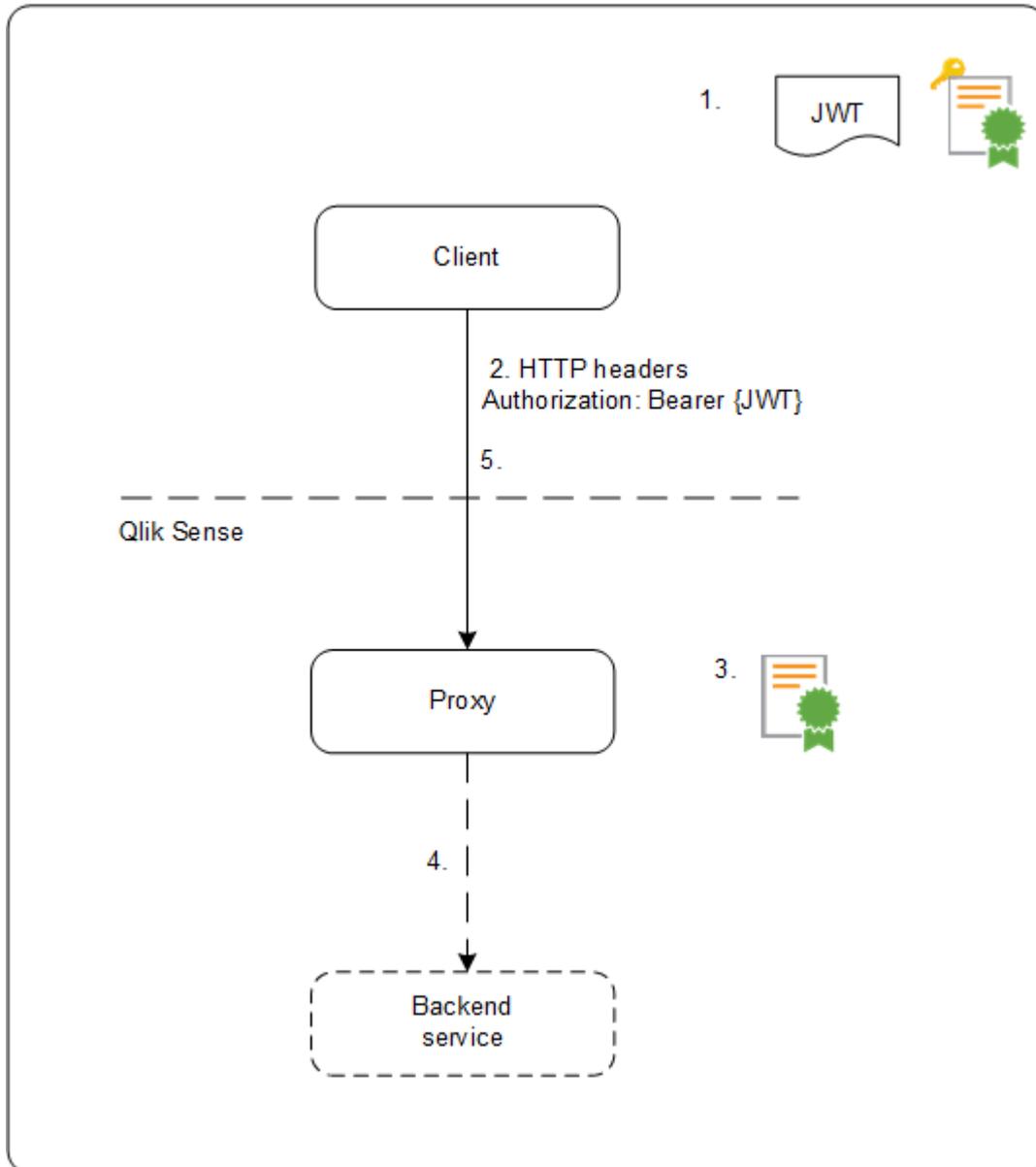
1. A JWT is generated, including a set of claims, and is signed with the private key for the configured certificate.

2. A request is sent to the proxy including the signed JWT in the HTTP Authorization header.

3. The proxy validates the signature of the JWT using the public key from the configured certificate.

4. The proxy injects the Qlik Sense headers including the configured attribute mappings and forwards the call to the backend service.

5. The client will receive a session and subsequent calls are not required to include a JWT.

    a. If the calls do include a JWT it will be validated, and if it is invalid the user will be rejected access.

    b. If the user in the JWT is different from the user stored for the session, the user will obtain a new session.

Standard fields

The following fields can be used inside a JWT claim:

- Issuer (iss): identifies the principal that issued the JWT.
- Subject (sub): identifies the subject of the JWT.
- Audience (aud): identifies the recipients of the JWT.
- Expiration time (exp): identifies the expiration time after which the JWT is not accepted.
- Not before (nbf): identifies the starting time on which the JWT is accepted.
- Issued at (iat): identifies the time at which the JWT was issued.
- JWT ID (jti): identifies the token.

Limitations

The following limitations exist:

- Encrypted JWTs are not supported.

> *When using HTTPS, all traffic, including JWTs, are encrypted during transport.*

- Only the following signing algorithms are supported:
  - RS256 - RSA signature with SHA256
  - RS384 - RSA signature with SHA384
  - RS512 - RSA signature with SHA512

OIDC configuration with AD FS

OpenID Connect (OIDC) is an authentication layer on top of OAuth 2.0, an authorization framework. OIDC enables single sign-on (SSO) to reduce the number of times a user has to log on to access websites and applications. OIDC can be configured for authentication with third-party products.

Configuring AD FS

This topic describes how you configure AD FS, but not how to install AD FS. AD FS will be the identity provider in your configuration, and before you can begin configuring, you need access to AD FS.

> *Because this configuration involves a third-party product, we cannot guarantee that the configuration is exactly as described here. Changes may occur in the third-party product, without our knowledge.*

Do the following:

1. In AD FS, open the Server Manager.
2. In the menu to the right, select **Tools** > **AD FS Management**.
3. In the AD FS management pane, select **Application Groups** > **Actions** > **Add an Application Group**.

4. Select **Server Application**. Enter a name and description. Click **Next**.

5. Under **Server Application**, there is a client ID. Note it down.

6. Enter the Redirect URI: *https://<QSEhostname>/<VirtualProxyPrefix>/oidcauthn* and click the **Add** URI button.

> *Use adfs as the virtual proxy prefix.*

7. Click **Next**.

8. Select **Generate a shared secret**. A secret key is generated. Note it down.
   A summary of your settings is displayed. Click **Next** and complete the steps for adding the application group.

9. Open the created application group.
   The **Properties** window appears.

10. Click **Add application**.
    A new window appears: **Add a new application to <app group name>**.

11. Select **Web API** template. Click **Next**.

12. Optionally, edit the **Web API** name.

13. Under **Identifier**, add the client ID that you noted down when creating the server application in this application group. Click **Next**.

14. Under **Apply Access Control Policy**, select **Permit everyone**. Click **Next**.

15. Under **Configure Application Permissions** > **Client application**, the server application is selected. Keep this unchanged. Under **Permitted scopes**, select **allatclaims**, **email**, **openid**, and **profile**. Click **Next**.

16. A summary of your settings is shown. Click **Next** to complete the steps for adding the Web API.

17. Open **Web API** > **Issuance Transform Rules**.

18. Click **Add Rule**. Enter a name for the rule, select **Active Directory** for **Attribute store** and then add "*E-Mail Addresses*" – "*E-Mail Address*" and "*Token-Groups - Unqualified Names*" - "*Group*" mapping. Save your changes.

19. Navigate to **Relying Party Trusts** in the **ADFS Management** tool.

20. Make sure you have the following relying party trust. **Identifier** should be *https://<ADFShostname>/adfs/services/trust*.

21. If the relying party trust is not available, you need to add a new. Follow the steps described in *https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-relying-party-trust#to-create-a-claims-aware-relying-party-trust-manually*, but skip the steps **Configure certificate** and **Configure URL**.

22. Make sure you add the email address for users who will be using Qlik Sense Enterprise sites through AD FS authentication.

    a. Open **Active Directory Users and Computers** on the AD server.

    b. Navigate to the **Users** folder, right-click the user and select **Properties**.

    c. Under **General**, enter the user's email address in the **E-mail** field.

    d. Click **OK** to save the changes.

Creating and configuring the virtual proxy

Do the following:

1. In the Qlik Management Console (QMC), open **Virtual proxies**.

2. Click ⊕ **Create new**.

3. In **Properties**, to the right, ensure that the sections **Identification**, **Authentication**, **Load balancing**, and **Advanced** are selected.

4. Under **Identification**, enter *adfs* for **Description** and **Prefix**.

5. For **Session cookie header name**, add *-adfs* at the end of the existing name so that it reads *X-Qlik-Session-adfs*.

6. For **Authentication method**, select **OIDC**.

7. Enter the "OpenID Configuration" URL in the **OpenID Connect metadata URI** field. The URL should be in the following format: *https://<ADFShostname>/adfs/.well-known/openid-configuration*.

8. Enter the noted Client ID and Client secret in the corresponding fields.

9. For **Realm**, enter *adfs*. Users added in the repository through OIDC authentication will have user directory name set to "adfs".

   > ℹ️ *If the subject attribute value format is domainname\username, realm is optional. If not, realm is mandatory.*
   > *The attributes sub, name, and email are mandatory. Other attributes are not mandatory, but must have a value. A configuration with empty attributes will generate an error.*

10. In the **name** field, change the value to *unique_name*.

11. In the **groups** field, change the value to *group*.

12. In the **client_id** field, change the value to *appid*.

13. In the **scope** field, enter *openid allatclaims profile email*.

    > ℹ️ *The openid part is mandatory. Other scopes can be added, but must match what is set on the identity provider side.*

14. Under **Load balancing nodes**, click **Add new server node**.

15. Select the engine nodes this virtual proxy will load balance connections to.

16. Under **Advanced**, in the **Host allow list** section, click **Add new value**.

17. Add the host name of the AD FS server.

18. Click **Apply** and then **OK** to restart the services.

19. In the **Associated items** menu to the right, select **Proxies**.

20. Click **Link** and link the virtual proxy to the proxy or proxies that will use this configuration.
    The proxy service is restarted.

Verify that the claims and scopes that you have configured in the IdP server are returned in **claims_supported** and **scopes_supported** tags when you select the **OpenID Connect Metadata URI**, *https://{IdP_ hostname}/.well-known/openid-configuration*.

This completes the AD FS configuration.

> ℹ️ *For an example where a token is used for verification of attributes, see* ⬋ [Qlik Sense: How to request an OIDC token manually and check if correct attributes are included (PowerShell)](#)

OIDC configuration with Auth0

OpenID Connect (OIDC) is an authentication layer on top of OAuth 2.0, an authorization framework. OIDC enables single sign-on (SSO) to reduce the number of times a user has to log on to access websites and applications. OIDC can be configured for authentication with third-party products.

Configuring Auth0

> ℹ️ *Because this configuration involves a third-party product, we cannot guarantee that the configuration is exactly as described here. Changes may occur in the third-party product, without our knowledge.*

Do the following:

1. Log in to *https://auth0.com/* and create an account with your email address.
2. In the left menu in Auth0, open **Applications**.
3. Click **Create application**.
4. Name the application, select **Single Page Web Applications** and click **Create**.
5. Optionally, select your web app technology.
6. Select **Settings**.
7. In the box **Allowed Callback URLs**, add the URL to your host in the format *https://<QSEhostname>/<VirtualProxyPrefix>/oidcauthn*.

   > ℹ️ *Use auth0 as the virtual proxy prefix.*

8. Scroll down and click **Save changes**.
9. Note down the **Client ID** and **Client Secret** values.
10. Scroll to the bottom and select **Advanced Settings**.
11. Select **Endpoints**.
12. Note down the **OpenID configuration** URL.

Creating and configuring the virtual proxy

Do the following:

1. In the Qlik Management Console (QMC), open **Virtual proxies**.
2. Click ➕ **Create new**.

3. In **Properties**, to the right, ensure that the sections **Identification**, **Authentication**, **Load balancing**, and **Advanced** are selected.

4. Under **Identification**, enter *auth0* for **Description** and **Prefix**.

5. For **Session cookie header name**, add *-auth0* at the end of the existing name so that it reads *X-Qlik-Session-auth0*.

6. For **Authentication method**, select **OIDC**.

7. Enter the noted "OpenID Configuration" URL in the **OpenID Connect metadata URI** field. It will be in the following format: *https://<Auth0hostname>/.well-known/openid-configuration*.

8. Enter the noted Client ID and Client secret in the corresponding fields.

9. For **Realm**, enter *auth0*. Users added in the repository through OIDC authentication will have user directory name set to "auth0".

> ⓘ   *If the subject attribute value format is domainname\username, realm is optional. If not, realm is mandatory.*
> *The attributes sub, name, and email are mandatory. Other attributes are not mandatory, but must have a value. A configuration with empty attributes will generate an error.*

10. In the **client_id** field, change the value to *aud*.

11. In the **scope** field, enter *openid profile email*.

> ⓘ   *The openid part is mandatory. Other scopes can be added, but must match what is set on the identity provider side.*

12. Under **Load balancing nodes**, click **Add new server node**.

13. Select the engine nodes this virtual proxy will load balance connections to.

14. Under **Advanced**, in the **Host allow list** section, click **Add new value**.

15. Add the host name of the Auth0 tenant, that is, the same host name that you entered for **OpenID Connect metadata URI**.

16. Click **Apply** and then **OK** to restart the services.

17. In the **Associated items** menu to the right, select **Proxies**.

18. Click **Link** and link the virtual proxy to the proxy or proxies that will use this configuration.
    The proxy service is restarted.

Verify that the claims and scopes that you have configured in the IdP server are returned in **claims_supported** and **scopes_supported** tags when you select the **OpenID Connect Metadata URI**, *https://{IdP_hostname}/.well-known/openid-configuration*.

Example of returned values when accessing https://{IdP_hostname}/.well-known/openid-configuration

This completes the Auth0 configuration.

> *For an example where a token is used for verification of attributes, see* ⎘ [Qlik Sense: How to request an OIDC token manually and check if correct attributes are included (PowerShell)](#)

OIDC configuration with Okta

OpenID Connect (OIDC) is an authentication layer on top of OAuth 2.0, an authorization framework. OIDC enables single sign-on (SSO) to reduce the number of times a user has to log on to access websites and applications. OIDC can be configured for authentication with third-party products.

Configuring Okta

> *Because this configuration involves a third-party product, we cannot guarantee that the configuration is exactly as described here. Changes may occur in the third-party product, without our knowledge.*

Do the following:

1. Log in to *https://www.okta.com/* with an admin account.
2. Go to **Security** > **API**.
3. In the **Authorization Servers** tab, select **Add Authorization Server** and enter the name, audience, and description for the Authorization Server.
   a. After creating the authorization server, go to **Claims** tab.
      i. Click **Add Claim**.
      ii. Enter **Name** of the claim as *groups*.
      iii. For **Include in token type**" dropdown, select **ID Token** and **Always**.

   iv.   Set **Value type** to **Groups**.

   v.   Set **Filter** to **Matches regex .***

   vi.   Click **Create**.

b.   Go to the **Scopes** tab.

   i.   Open the **Scopes** tab.

   ii.   Click **Add scope**.

   iii.   Enter **Name** of the scope as *groups*.

   iv.   Select **Include in public metadata**.

   v.   Click **Create**.

c.   Go to the **Access Policies** tab.

   i.   Click **Add Policy**. Enter name and description for the new policy and keep **Assign to** set to *All clients* option. Click **Create Policy**.

   ii.   After the new policy is created, add a new rule for the policy by clicking **Add Rule**. Enter a rule name. Keep the default values as they are for all fields and click **Create Rule**.

d.   Note the Issuer URI which can be found in **Settings** tab of authorization server. This URI will be in the format: *https://<yourOktaDomain>/oauth2/<authServerId>*

> *Instead of creating a new authorization server, the default authorization server available in Okta can be used by making the above-mentioned changes.*

4.   In the top menu, select **Applications**.

5.   Click **Add Application**.

6.   Click **Create New App**.

7.   For **Platform**, select **Web**.

8.   For **Sign on method**, select **OpenID Connect**.

9.   Click **Create**.
   The configuration window appears.

10.   Name the app *Qlik SenseOIDC configuration*.

11.   Optionally, add a logo.

12.   For **Login Redirect URIs**, enter *https://<QSEhostname>/<VirtualProxyPrefix>/oidcauthn*.

> *Use okta as the virtual proxy prefix.*

13.   Click **Save**.
   The **Application details** page appears.

14.   Note down **Client ID** and **Client secret**, available under **General** > **Client credentials**.

15.   You must assign users to the app, so that they can use the connection that you have created. Click **Assign to People** and add users. Users must have an Okta account.

Creating and configuring the virtual proxy

Do the following:

1. In the Qlik Management Console (QMC), open **Virtual proxies**.
2. Click ⊕ **Create new**.
3. In **Properties**, to the right, ensure that the sections **Identification**, **Authentication**, **Load balancing**, and **Advanced** are selected.
4. Under **Identification**, enter *okta* for **Description** and **Prefix**.
5. For **Session cookie header name**, add *-okta* at the end of the existing name so that it reads *X-Qlik-Session-okta*.
6. For **Authentication method**, select **OIDC**.
7. In the **OpenID Connect metadata URI** field, enter the noted Issuer URI from Okta's Authorization Server Settings in the following format: *https://<yourOktaDomain>/oauth2/<authServerId>/.well-known/openid-configuration*.
8. Enter the noted Client ID and Client secret in the corresponding fields.
9. For **Realm**, enter "okta". Users added in the repository through OIDC authentication will have user directory name set to "okta".

   > *If the subject attribute value format is domainname\username, realm is optional. If not, realm is mandatory.*
   > *The attributes sub, name, and email are mandatory. Other attributes are not mandatory, but must have a value. A configuration with empty attributes will generate an error.*

10. In the **client_id** field, change the value to *aud*.
11. In the **scope** field, enter *openid profile email*.

    > *The openid part is mandatory. Other scopes can be added, but must match what is set on the identity provider side.*

12. Under **Load balancing nodes**, click **Add new server node**.
13. Select the engine nodes this virtual proxy will load balance connections to.
14. Under **Advanced**, in the **Host allow list** section, click **Add new value**.
15. Add the host name of Okta, that is, the same name that you entered for **OpenID Connect metadata URI**.
16. Click **Apply** and then **OK** to restart the services.
17. In the **Associated items** menu to the right, select **Proxies**.
18. Click **Link** and link the virtual proxy to the proxy or proxies that will use this configuration.
    The proxy service is restarted.

Verify that the claims and scopes that you have configured in the IdP server are returned in **claims_supported** and **scopes_supported** tags when you select the **OpenID Connect Metadata URI**, *https://{IdP_hostname}/.well-known/openid-configuration*.

Example of returned values when accessing https://{IdP_hostname}/.well-known/openid-configuration

This completes the Okta configuration.

> ⓘ *For an example where a token is used for verification of attributes, see* ⮕ [Qlik Sense: How to request an OIDC token manually and check if correct attributes are included (PowerShell)](#)

Configuring SAP HANA for SAML single sign-on (SSO) with Qlik Sense

When you have many users who have different access rights in SAP HANA, you can create a single sign-on (SSO) ODBC connector to SAP HANA and use SAP HANA security for authentication instead of creating multiple ODBC connectors with credentials passed.

A user of Qlik Sense should be able to be identified and authenticated from Qlik through to SAP HANA. Therefore someone viewing an application through the hub in Qlik Sense, would only be able to see the values and attributes that they are authorized to see in the SAP HANA system. This will not apply to static data that has already been loaded in to a Qlik application. But will apply where a user is making a new connection, reloading data or using Direct Discovery.

This is useful when you have a number of designers or many users of apps. A key component of this is to allow a user to log in to a Qlik app and pass the userid through to the connection string dynamically allowing each user to effectively connect to source with their own database login. This would enable all of the row/table level security to remain at source.

To set up SSO, do the following:

> ⓘ *Steps 1-4 are performed in your SAP HANA Studio.*

1. Generate a certificate and private key.

2. Install the certificate in SAP HANA.

3. Create an identity provider (IdP) and user mappings in SAP HANA Studio.

4. Validate your SAP HANA configuration.

5. Configure Qlik Sense by distributing the PEM files to all nodes in your Qlik Sense installation. Use the same certificate on all nodes.

   - On each computer, copy the certificate and private key files to the certificate folder. By default, this is *C:\ProgramData\Qlik\Sense\Engine\Certificates*.

   > *Make sure the certificates are named Qlik.pem and Qlik_key.pem*

6. Create an ODBC connection to SAP HANA.

   - Select **Current user**.
     Any use of the data connection will now be executed with the end user credentials from SAP HANA.

   - Select data and verify that available data aligns with the privileges of the mapped database user.

Enable settings in Qlik Sense by navigating to *C:\ProgramData\Qlik\Sense\Engine* and opening *Settings.ini*. The table below defines the SSO settings possible.

SSO settings

Name	Default	Description
SSOCertificateFolder	Default engine folder	Folder where certificates will be created.
SSOCertificate	"qlik.pem"	Certificate file name.
SSOPrivateKey	"qlik_key.pem"	Private key name.
SSOCasing	0	0: Case sensitive >0: Upper case <0: Lower case
SSOExternalId	0	0: (domain\username) 1: UPN (username@domain.com) 2: (username)

Configuring Cloudera Impala for single sign-on

With a single sign-on (SSO) solution, you can minimize the number of times a user has to log on to access apps and websites.

When you set up Cloudera Impala as a data source in Qlik Sense, you can configure Cloudera Impala for SSO. You store the Qlik Sense user credentials and define a trusted relationship so that the system passes the Qlik Sense credentials from Qlik Sense to Cloudera Impala.

Users who create apps using an SSO data connection to Cloudera Impala are authenticated in Cloudera Impala. If the app data is loaded in-memory, access to the data is controlled from within Qlik Sense. To prevent the creation of other Cloudera Impala data source connections, you should set the security rules in the QMC so that ODBC data connections cannot be created.

> ⚠️ *The Cloudera Impala Connector in the Qlik ODBC Connector Package also supports SSO. If you are using the connector in the ODBC Connector Package, use the following configuration instructions:*
> [Configuring SSO for the Cloudera Impala connector.](#)

> ℹ️ *Only the vendor supplied driver works in this configuration, not the driver in the Qlik Connector Package.*

> ℹ️ *This configuration is for Cloudera Impala only, Hive requires a different configuration option.*

Setting up SSO for Cloudera Impala

To set up SSO for Cloudera Impala, you first need to set up a "kerberized" cluster, that is, a cluster that forces Kerberos authentication, and use Sentry for authorization. Then you need to add users who can do impersonation in Cloudera Manager, install the vendor ODBC drivers, create a data source to Cloudera Impala, configure Qlik Sense, and create an ODBC connection to Cloudera Impala.

Do the following:

1. Set up a "kerberized" cluster that forces Kerberos authentication and use Sentry for authorization. See the Cloudera documentation for details: 🔗   [Cloudera](#)
2. Add users who can do impersonation in Cloudera Manager.
   a. In Cloudera Manager, navigate to the Impala cluster and select **Configuration**.
   b. Search for *proxy user*.
   c. In **Proxy User Configuration**, add the service account users who are allowed to impersonate other users.
      In the following example, the service account user svc-bob12 can impersonate users.
      Example: *hue=*;svc-sensecloudera58=*;svc-bob12=*;*
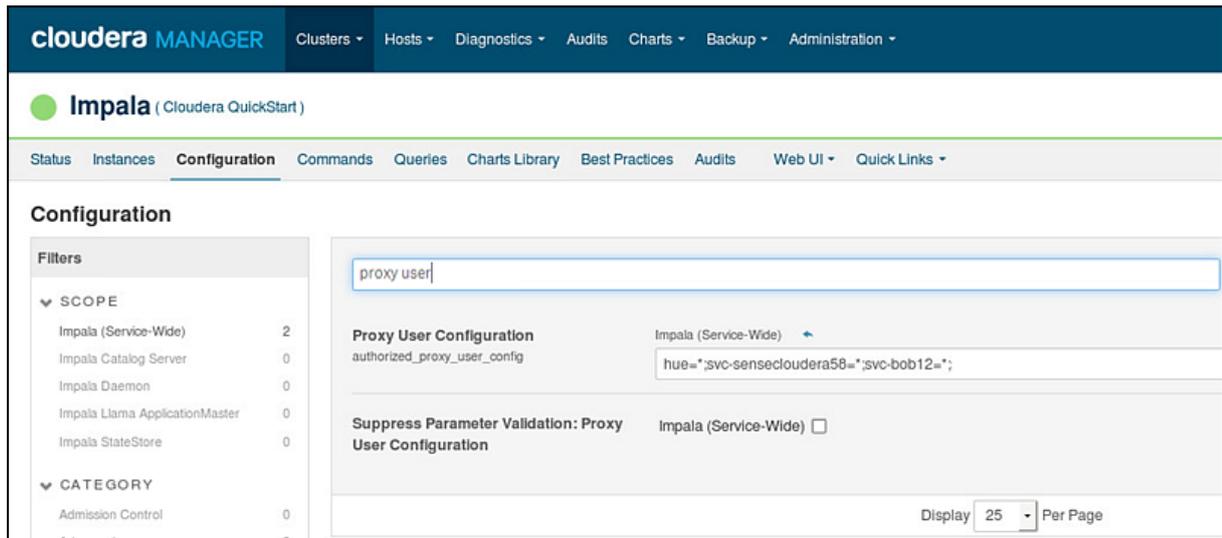
Proxy user configuration for Cloudera Impala only

     d. Restart the Cloudera services.

3. Install the vendor ODBC drivers.

4. Create a data source to Cloudera Impala.

5. Configure Qlik Sense (if needed).

     a. Navigate to *%ProgramData%\Qlik\Sense\Engine* and open *Settings.ini*.

     b. Edit the settings, see *SSO settings in Settings.ini (page 497)*, and save.

     c. Restart the Qlik Sense Engine Service.

6. Create an ODBC connection to Cloudera Impala using Qlik Sense.

     a. Open the data load editor.

     b. Create an ODBC connection and under **Logon credentials**, select **Single Sign-On**.
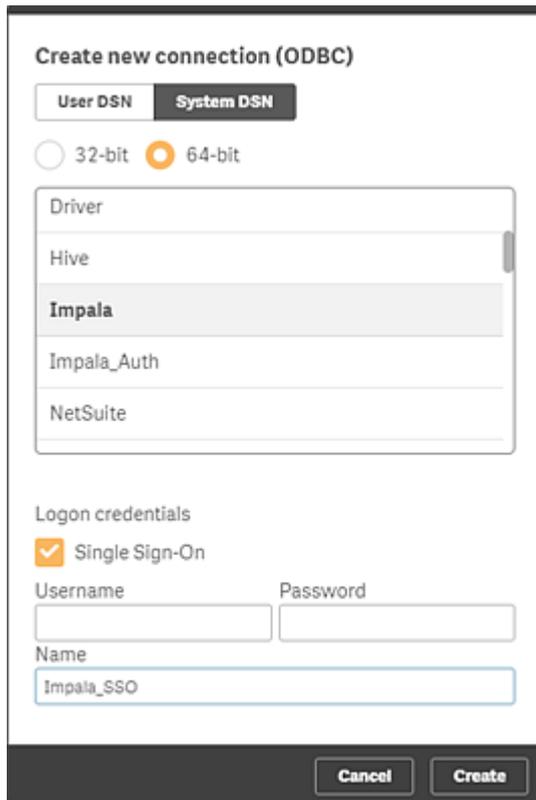
c. In the data model viewer, verify that the available data aligns with the privileges of the mapped database user.

The setup is complete.

SSO settings in *Settings.ini*

SSO settings

Setting	Default value	Possible values
SSODisableLogOn	0	• 0: Enables SSO • 1: Disables SSO
SSOCasing	0	• 0: Case sensitive • >0: Upper case • <0: Lower case
SSOExternalId	0	• 0: (domain\username) • 1: UPN (username@domain.com) • 2: (username)

Configuring client authentication

A Qlik Sense administrator can allow users to authenticate their client against Qlik Sense. To do so, you must generate an authentication link in the Qlik Management Console (QMC), and then distribute the link to client users. The authentication link will not expire.

You can generate an authentication link for any node and distribute the link manually. However, if you are generating a link that will be retrieved from the Qlik Sense hub, you must select the default virtual proxy on the central node.

Make sure user access or professional access is allocated to the users.

For more information about access, see *Managing user access (page 317)* and *Managing professional access (page 307)*.

> *Client authentication is not supported on test servers.*

Generate and distribute an authentication link

1. As a Qlik Sense administrator, open the QMC.
2. Click the **Virtual proxies** tab, select the proxy, and then click **Edit**.
3. In the **Edit virtual proxy** page, click the **Client authentication link** tab.
4. Enter a client authentication link host URI. This is the URL that will take users to the authentication page for the Qlik Sense server.
5. Enter a friendly name for the Qlik Sense host server for client authentication. This name will be used to identify the server to client users when they authenticate.
6. Click **Generate**. An authentication link is generated. Copy the link to a text editor and save the file. If you have to generate the link again later with the same settings, the same link will be generated.
7. Click the **Apply** button. Note that this will restart any proxies associated with the virtual proxy.
8. Distribute the link in one of the following ways:
   a. Inform client users that they can retrieve the link from the Qlik Sense hub. The link will be available to all Qlik Sense users when they select **Client authentication** from ••• in the top toolbar in the Qlik Sense hub. After a user selects the link, the client adds an authentication button to its welcome page. The button is identified by the friendly name that you provided above for the Qlik Sense server. The user can now click the button to log in to the client using their Qlik Sense credentials.
   b. Distribute the authentication link to client users by email or another method. After a user selects the link, the client adds an authentication button to its welcome page. The button is identified by the friendly name that you provided above for the Qlik Sense server. The user can now click the button to log in to the client using their Qlik Sense credentials.
   c. Configure and then distribute the *hubs.ini* file:
      i. Create a file called *hubs.ini* using a text editor.
      ii. Save your changes.
      iii. Add the authentication link on a new line.
      iv. Distribute the file to the client users that you want to allow to authenticate against Qlik Sense.
      v. Instruct the users to paste the file here: *C:\Users\<user name>\Documents\Qlik\Sense\Hubs*.
      The next time the user launches the client, they will be able to authenticate against the Qlik Sense server using their Qlik Sense credentials.

Configuring system function calculations

As an administrator, you can prevent some system functions from returning any value to end users, or API calls. This is an optional setting.

The following functions can be blocked from returning any value:

- ComputerName()
- EngineVersion()
- OSName()
- OSVersion()
- ProductVersion()
- QTProduct()

> *Some current applications may use the functions in conditional calculations.*

1. Navigate to *%ProgramData%\Qlik\Sense\Engine* and open *Settings.ini*.
2. Edit the settings, see *System function calculation settings in Settings.ini (page 499)*, and save.
3. Restart the Qlik Sense Engine Service.

The setup is complete.

System function calculation settings in *Settings.ini*

Setting	Default value	Possible values
BlockSystemInfo	BlockSystemInfo=0	0: Enables system function calculations 1: Disables system function calculations

Changing a proxy certificate

In Qlik Sense, all communication between services and the Qlik Sense web clients is based on web protocols. The web protocols use Secure Sockets Layer (SSL) for the following:

- Encryption and exchange of information and keys
- Certificates for authentication of the communicating parties

After a standard Qlik Sense installation, the Qlik Sense Proxy Service (QPS) includes a module that handles the encryption of traffic from the browser to the proxy. The certificate for communication between the web browser and the proxy can be replaced.

> *Third-party certificates are bound to the Qlik Sense Proxy Service HTTPS port (443). Communication via the API port (4243) always uses the Qlik Sense server certificate.*

> **ℹ** *When editing a proxy certificate and the Qlik Sense services run with an account without administrator privileges, you need to configure the private key permissions for the certificate.*

> **ℹ** *An admin needs to add read access to the certificate's private key for the group 'Qlik Sense service users' when the proxy is running with a user without admin privileges, otherwise the proxy cannot access the certificate.*

This flow describes changing proxy certificate:

```
┌─────────────────────────┐
│  Install server certificate │
└─────────────────────────┘
           │
           ▼
┌─────────────────────────┐
│          ⊙              │
│     Log in to QMC       │
└─────────────────────────┘
           │
           ▼
┌─────────────────────────┐
│          ✕              │
│     Select Proxies      │
└─────────────────────────┘
           │
           ▼
┌─────────────────────────┐
│          ✕              │
│     Find proxy node     │
└─────────────────────────┘
           │
           ▼
┌─────────────────────────┐
│          ✕              │
│     Add thumbprint      │
└─────────────────────────┘
           │
           ▼
┌───────────────────────────────┐
│   Installed certificate used for │
│ communication between browser and │
│             proxy             │
└───────────────────────────────┘
```

Do the following:

1. Install the new server certificate:

    a. Note down the thumbprint for the new certificate.

    b. Install the new server certificate on the proxy node, in the Windows Certificate Store in *Local Machine/Personal*.

> ℹ️ *To be valid, the certificate must contain a private key. The certificate should be installed to the Local Computer / Computer Account > Personal portion of MMC for the user account that is used to run the Qlik Sense Proxy Service.*

> ℹ️ *When using a third-party certificate, it is required that the certificate is trusted in Windows, and that the private key is stored with the certificate in the Windows certificate store. The certificate should be installed to the Local Computer / Computer Account > Personal portion of MMC for the user account that is used to run the Qlik Sense Proxy Service.*

> ℹ️ *Qlik Sense supports certificates that are made to use signing algorithms based on SHA-1 or SHA-256.*

2. Open the QMC: *https://<QPS server name>/qmc*
3. Select **Proxies** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
4. Find the relevant proxy in the overview and select **Edit**.
5. Edit the **SSL browser certificate thumbprint** found in the **Security** property group by adding the thumbprint of the installed server certificate, from step 1 in this procedure.
6. Click **Apply** in the action bar to apply and save your changes.
   Successfully updated is displayed at the bottom of the page.
7. Restart proxy.

The installed certificate is now used for communication between the web browser and the proxy. A green padlock (or similar icon depending on browser) is displayed when entering the address of the QMC in your Internet browser. This means that the browser trusts the certificate and has identified the server machine. By default, the QMC address is *https://<QPS server name>/qmc*.

Changing to a signed server proxy certificate

By default, a self-signed certificate is used to secure communication between the web browser (client) and the Qlik Sense proxy. This results in a warning in the client web browser, such as "The site's security certificate is not trusted" (Chrome) or "This Connection is Untrusted" (Firefox). To resolve this issue, the certificate used for communication between the web browser (client) and the proxy must be replaced with a signed server certificate from a trusted certificate authority (CA).

> ℹ️ *The existing self-signed certificate is secure. The warning is displayed because the web browser does not have enough information to decide whether or not the certificate is secure. By following the procedures described here you remove the warning in the client web browser.*

Major steps

The following major steps are required when changing to a signed server proxy. Steps 2-4 have detailed procedures in the subsections.

1. Obtain a valid signed server certificate matching the proxy node URL, from a trusted CA, such as VeriSign or GlobalSign.

2. Import the certificate into Windows Local Computer Certificate Store.

3. Locate the thumbprint for the certificate.

4. Configure the proxy node to use the certificate.

> The certificate itself has to contain a private key regardless of the Qlik Sense version. You can verify if a key is present by reviewing the certificate in the Microsoft Management Console (MMC). You should see a confirmation message: "You have a private key that corresponds to this certificate."

Importing the certificate

Do the following:

1. Launch the MMC on the proxy node.

2. In the MMC, open **File > Add / Remove Snap-in...**.

3. Select **Certificates** and click **Add**.

4. Select **Computer account**, click **Next**, select **Local computer** and click **Finish**.

5. In the MMC, open **Certificates (Local Computer)/Personal**.

6. In the MMC, open **Actions > All Tasks > Import...**.

7. Browse to the certificate file provided by your CA.

8. Follow the instructions on the screen to import the certificate, including the private key.

9. Verify that the new certificate has been imported into **Certificates (Local Computer) > Personal > Certificates** and that it contains a private key.

10. Double-click the **Certificate > Certification Path** and confirm it shows "**This certificate is OK**".

> You must make sure that the certificate is available for the service account that is running the Qlik Sense services. The best way to do this is to run the MMC as the service account and see if the certificate is visible in **Personal > Certificates**. If you are running services with local system, you can use a tool such as Psexec to run the MMC as local system and check that the certificate is available.

Configuring the private key permissions for the certificate

When editing a proxy certificate and the Qlik Sense services run with an account without administrator privileges, you need to configure the private key permissions for the certificate as follows:

1. Launch the **MMC** on the proxy node.

2. In the **MMC**, open **Certificates (Local Computer)/Personal**.

3. Select the certificate provided by your CA.

4. Open **Actions > All Tasks > Manage Private Keys**.

5. In the **Permissions** pop-up, add read permissions to the group "**Qlik Sense Service Users**", alternatively, to the specific service user that is running the Qlik Sense services.

6. Restart the Qlik Sense Proxy Service.

Locating the certificate thumbprint

Do the following:

1. In the MMC, right-click the imported certificate and select **Open**.
2. On the **Details** tab, scroll down and select **Thumbprint**.
3. Mark/highlight the thumbprint hash value and press CTRL+C to copy the hash value to the clipboard.
4. Paste the hash value in a text editor and remove all the spaces.

Configuring the proxy node

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Open **Proxies**.
3. Select your proxy and click **Edit**.
4. In **Properties** to the right, select **Security**.
5. Scroll down and locate **SSL browser certificate thumbprint** in the **Security** section.
6. Paste the thumbprint hash value for the new certificate (from the text editor).
7. Click **Apply**.

You should now be able to access the Qlik Sense proxy without the browser warning.

Exporting certificates through the QMC

If you want to add a third-party tool to your Qlik Sense installation, you need to export the certificates.

You can use the exported certificates to do the following:

- Use external modules, such as authentication, session, and load balancing.
- Move the certificates manually to a node, instead of using the QMC functionality when creating a new node.

> *Export of certificates from the QMC is not intended for backing up and restoring a site. For that purpose, we suggest using Repository Snapshot Manager or Microsoft Management Console.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Certificates** on the QMC start page or from the ▼ menu.
   The **Export** page for **Certificates** is displayed.
3. In the **Machine name** box, type the full computer name of the computer that you are creating the certificates for: *MYMACHINE.mydomain.com* or the *IP address*.

> ⓘ   *There is support for using an IPv6 address as host name.*

You can export certificates for more than one computer. Click ✚**Add machine name** to add a new box. You cannot add the same computer name more than once. Click ✖ to delete a box.

4.   Using a password is optional. If you choose to use a password, the same password applies to exported client and server certificates.

> ⓘ   *The root certificate is exported without a private key due to security reasons.*

   a.   Type a password in the **Certificate password** box.
   b.   Repeat the password in the **Retype password** box.
        The passwords must match.

5.   Select **Include secret key** if you want to add a secret key to the public key.

> ⓘ   *The secret key must be included if you are exporting certificates for a new node. The secret key is used to decrypt entries such as passwords on the new node. These entries are in the database.*

6.   Select file format in the **Export file format for certificates** drop-down list.
     The Windows format is .pfx.

7.   Click **Export certificates** in the action bar.
     The export of certificates is initiated and **Exporting certificates** is displayed.
     When the export is finished, the dialog **Certificates exported** is displayed.
     Certificates will be exported to this disk location displays the target directory where one folder for each computer is added. In every folder the following certificates are created: client.pfx, root.cer, server.pfx. If the export fails, the dialog displays **Certificates export could not complete**.

Configuring Qlik Sense to allow users to publish a link to shared content

You must create a Qlik Sense security rule and configure the Qlik Sense repository to allow QlikView to publish links on the Qlik Sense hub.

Adding a shared content security rule

Enable shared content by creating a new security rule in the QMC.

Do the following:

1.   Open the QMC: *https://<QPS server name>/qmc*
2.   In the QMC, open the **Security rules**.
3.   Click **Create new** at the bottom of the page.
4.   In the **Identification** section, add a name and rule description. You can use the suggestions in the following table.

Identification fields and values suggestions

Field	Value
Name	*SharedContentCreate-AllUsersFromUserGroupName*
Description	*All users from the domain UserGroupName are allowed to create shared content*

5. In the **Basic** section, type *SharedContent_** as a **Resource filter**.

6. Select the **Create** action and ensure that the **Read** action is cleared.

7. Complete the action rule definition using the values in the following image by replacing *UserGroupName* with the name of your authentication user group.

user	▼	userDirectory	▼	=	▼	⊕
value	▼	UserGroupName				

8. (Optional) If you want all authenticated users to be allowed to share QlikView content, type *!user.IsAnonymous()* in the **Conditions** box.

9. Click **Apply**.

The security rule has now been added to the QMC for authenticated users.

Enabling shared content in the Qlik Sense repository

To enable shared content in the Qlik Sense repository, you must update the configuration file. By default, the *Repository.exe.config* file can be found in *C:\Program Files\Qlik\Sense\Repository* on your Qlik Sense machine. Edit the configuration file and change the value of the `SharedContentEnabled` key to `true`. Restart the Qlik Sense Repository Service using the Windows Services application to enable this new configuration.

Configuring the QlikView Distribution Service with the Qlik Sense certificates

You must configure each QlikView Distribution Service (QDS) with Qlik Sense certificates to allow links to QlikView documents to be published to the Qlik Sense hub.

Before you begin

To configure the QDS, you must copy to each QDS machine a new set of certificates including the client.pfx, root.cer, server.pfx. Each QDS machine that you configure requires a new set of Qlik Sense certificates.

Importing the Qlik Sense certificates on the QDS machine

All certificates can be imported using the native Windows Certificate Import Wizard.

> ⓘ *The root.cer certificate must be imported before all other certificates.*

Importing the root.cer certificate

1. Double-click to open the certificate.

2. Click **Install Certificate**.

    The Certificate Import Wizard is initiated.

3. Select **Current User**.

4. Select **Place all certificates in the following store**.

5. Click **Browse** and select the **Trusted Root Certification Authorities** folder.

6. Review the certificate information and click **Finish**.

    The root.cer certificate is imported on the QDS machine.

Importing the client.pfx and server.pfx certificates

1. Double-click to open the certificate.

    The Certificate Import Wizard is initiated.

2. Select **Current User**.

3. On the **Private key protection** screen, type the certificate password.

4. Select **Automatically select the certificate store based on the type of certificate**.

5. Review the certificate information and click **Finish**.

    The certificate is imported on the QDS machine.

Configuring the QDS properties with the Qlik Sense certificate and machine information

The QDS configuration file must be updated on each machine with the associated certificate thumbnail and Qlik Sense and QDS machine information. By default, the *QVDistributionService.exe.config* QDS configuration file is located in *C:\Program Files\QlikView\Distribution Service*.

1. In the `<appSettings>` section, type `<add key="QRSMachineName" value="MySenseMachine.domain.com" />` replacing `QlikSenseMachineName.domain.com` with the name of your machine running the Qlik Sense Repository.

    > ⓘ   *The machine name must include the domain and match the name used when creating the Qlik Sense certificates.*

2. On a separate line, type `<add key="QVWSMachineName" value="QlikViewMachineName" />` replacing `QlikViewMachineName` with the name of your machine running the QlikView Web Server.

    > ⓘ   *The domain is not required.*

3. (Optional) On a separate line, type `<add key="AjaxClientPath" value="/MyAjaxURL/opendoc.htm" />` replacing `MyAjaxURL` with the URL of your Ajax Client. If this configuration option is not added, the default `/QvAJAXZfc/opendoc.htm` is used.

4. Open the Windows Microsoft Management Console.

5. Click the **Certificates - Current User** drop-down arrow.

6. Open the **Personal > Certificates** folder.

7. Double-click the QlikClient certificate.
    The certificate properties are displayed.

8. On the **Details** tab, copy the Thumbprint value.

9. On a separate line in the *QVDistributionService.exe.config* file, type `<add key="SenseClientCertificateThumbprint" value="ThumprintID" />` replacing **ThumbprintID** with the value of the thumbprint found in the certificate properties.

10. Save your changes.
    The QDS is configured to allow you to publish links to QlikView documents in the Qlik Sense hub.

Creating a task to publish a link to a QlikView document in the Qlik Sense hub

You can create a link to a QlikView document in the Qlik Sense hub by using the QMC.

> *QlikView documents in the Qlik Sense hub only support interactions using the Ajax client.*

Before you begin

To publish a link to a QlikView document in Qlik Sense you need a QlikView Server setup with a connection to an Active Directory and source documents.

Configuring the QlikView Management Console

You must configure QlikView Web Server Access Point to connect with the Qlik Sense machine.

Do the following:

1. Click the **System** tab.

2. In the QlikView Web Server folder, open the current QlikView Web Server machine.

3. On the **Access Point** tab, click **Server Connections**.

4. Using the drop-down menu, change the name of the QlikView web server from *local* to the machine name.

Publishing a link to a QlikView document

Do the following task in the QlikView Management Console to publish a link to a document:

1. Click the **Documents** tab.

   The **Source Document** page opens.

   > *Only source documents can be published.*

2. Expand a QDS instance and locate the document you want to share.

3. Click ⊕ to create a new task.

4. On the **Distribute** tab, click ⊕ to add a recipient.

5. Select the **Named User** user type.

6. Click 🖳 to add a user.

   > *The named user must be part of the Active Directory user group in both QlikView and Qlik Sense.*

7. On the **Document Information** tab click ⊕ to add an attribute.

8. Type *ShowInSenseHub* in the **Name** field and `true` in the **Value** field.

9. Click **Apply**.
   The task may be run and will now add a link to the QlikView document on the Qlik Sense hub.

Viewing QlikView documents in the Qlik Sense hub

Do the following:

1. Log in to the Qlik Sense hub using the same credentials as the named user with whom the QlikView document was shared.
2. From the hub, click **QlikView documents**.
3. Click a link to a document to open the QlikView AccessPoint in a new window.

> *QlikView documents cannot be deleted from the Qlik Sense hub.*

Configuring load balancing rules

Within a multi-node site, one instance of the Qlik Sense Repository Service (QRS) runs on each node. The QRS running on the central node is considered to be the primary. The primary QRS load balances the central repository database.

You set up rules for the load balancing of Qlik Sense apps.

Creating load balancing rules

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Load balancing rules** on the QMC start page or from the **Start** ▼ drop-down menu.
3. Click ➕ **Create new** in the action bar.
   A split page is displayed, with the editing pane to the left (with all the properties) and the audit page to the right.
4. Under **Identification**, in the **Create rule from template** drop-down list, select the resource type to create a rule for.

   > *In the **Basic** section, next to the **Resource filter** text box, you can click the arrow to open a popover where you can select multiple resources for the filter.*

   Unspecified
   Load balancing the opening of apps between nodes

5. Under **Identification**, give the rule a name and a description.
6. Select **Disabled** if you do not want to enable the rule at this time.
7. In the **Basic** view, select the type of actions you want to create a rule for.
8. Select a resource condition in the drop-down lists.
   For example, selecting the resource condition **name** and setting **name** = *MyApp*, means that the rule applies to the app named *MyApp* while setting **name** = *MyApp**, will apply the rule to all apps with names beginning with *MyApp*.

> *When using multiple conditions, you can group two conditions by clicking **Group**. After the conditions have been grouped, you have the option **Ungroup**. Additional subgrouping options are **Split** and **Join**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that AND is superior to OR.*

> *Changing the **Create rule from template** selection automatically clears all **Actions**, and changes the **Conditions** text box in the **Advanced** section accordingly.*

Resource

Property descriptions

Property name	Description
@<customproperty>	The custom property associated with the resource.
name	The name of the associated app.
owner.@<customproperty>	Owner property associated with the app. See the corresponding owner property for a description.
owner.environment.browser	Owner property associated with the app. See corresponding owner property for description.
owner.environment.context	Owner property associated with the app. See corresponding owner property for description.
owner.environment.device	Owner property associated with the app. See corresponding owner property for description.
owner.environment.ip	Owner property associated with the app. See corresponding owner property for description.
owner.environment.os	Owner property associated with the app. See corresponding owner property for description.
owner.environment.secureRequest	Owner property associated with the app. See corresponding owner property for description.
owner.name	The user name of the owner of the resource.
owner.userDirectory	The user directory of the owner of the resource.
owner.userId	The user id of the owner of the resource.
stream.@<customproperty>	Owner property associated with the app. See corresponding owner property for description.
stream.name	The name of the associated stream.

9. Click **Preview** to view the access rights of your rule in the currently defined audit grid.

10. Click **Apply** to create and save the rule.

Successfully added is displayed at the bottom of the page.

Editing load balancing rules

You can edit load balancing rules that you have update rights to.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Load balancing rules** on the QMC start page or from the **Start** ▼ drop-down menu.
3. Select the rule you want to edit.
4. Click **Edit** in the action bar.
   A split page is displayed, with the editing pane to the left (with all the properties) and the audit page to the right.
5. Edit the applicable fields for the rule.

> *When using multiple conditions, you can group two conditions by clicking **Group**. After the conditions have been grouped, you have the option **Ungroup**. Additional subgrouping options are **Split** and **Join**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that AND is superior to OR.*

> *In the **Basic** section, next to the **Resource filter** text box, you can click the arrow to open a popover where you can select multiple resources for the filter.*

Resource

Property descriptions

Property name	Description
@<customproperty>	The custom property associated with the resource.
name	The name of the associated app.
owner.@<customproperty>	Owner property associated with the app. See the corresponding owner property for a description.
owner.environment.browser	Owner property associated with the app. See corresponding owner property for description.
owner.environment.context	Owner property associated with the app. See corresponding owner property for description.
owner.environment.device	Owner property associated with the app. See corresponding owner property for description.

Property name	Description
owner.environment.ip	Owner property associated with the app. See corresponding owner property for description.
owner.environment.os	Owner property associated with the app. See corresponding owner property for description.
owner.environment.secureRequest	Owner property associated with the app. See corresponding owner property for description.
owner.name	The user name of the owner of the resource.
owner.userDirectory	The user directory of the owner of the resource.
owner.userId	The user id of the owner of the resource.
stream.@<customproperty>	Owner property associated with the app. See corresponding owner property for description.
stream.name	The name of the associated stream.

6. Click **Disabled** if you do not want to enable the rule at this time.

7. Click **Preview** to view the access rights of your rule in the currently defined audit grid.

8. Click **Apply** to save the edited rule.
    Successfully updated is displayed at the bottom of the page.

Deleting load balancing rules

You can delete load balancing rules that you have delete rights to.

> If a resource is deleted, all load balancing rules and security rules associated with that resource are deleted automatically.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Load balancing rules** on the QMC start page or from the **Start** ▼ drop-down menu.

3. Select the rules that you want to delete.

    > You can filter a column by using the filtering option: ⬜▼

4. Click **Delete** in the action bar.
    A **Delete** dialog is displayed.

5. Click **OK**.

Creating load balancing rules with custom properties

Your company has a number of multi-node Qlik Sense installations, and you need to create load balancing rules for all of your nodes. You can set load balancing rules on individual nodes. However, given the multi-node scenario, it will be easier to manage load balancing if you group nodes.

The following example will show how you can group nodes by function. Let's assume that you want to create load balancing rules to load balance each site node with the apps published on the corresponding departments' streams on the central node.

> *The same method can be applied to schedulers, proxies, and engines.*

Do the following:

1. Create a custom property called *Departments*.
   a. Apply the custom property to the resource types **Nodes** and **Streams**.
   b. Create the following values for the custom property Departments: *Sales*, *Development*, and *Test*.
2. Add the custom property Departments to nodes.
   a. Select the appropriate nodes in the **Nodes** overview using multi-select.
   b. Click **Edit**.
   c. In the **Custom properties** section, set custom property Departments to *Sales*.
   d. Repeat for the departments Development and Test.
3. Add the custom property Departments to streams.
   a. Select the appropriate streams in the **Streams** overview using multi-select.
   b. Click **Edit**.
   c. In the **Custom properties** section, set custom property Departments to *Sales*.
   d. Repeat for the departments Development and Test.
4. Create a load balancing rule that enables Sales nodes to load balance apps in the Sales streams on the central node.
   a. Create a load balancing rule for the resource *App_* * with the following condition (in the **Advanced** section):
      node.@Department= Sales and resource.stream.@Department = Sales
      This means that the load balancing rule will apply to all apps in streams that have the custom property Departments set to the value *Sales*.
   b. Repeat for all departments.

You have now made it possible to administer node load balancing using departments.

Configuring content cache-controls

With content cache-controls, you can modify the cache behavior of the browser. The cache-control is used on endpoints handled by the repository service. This functionality is disabled by default and can be enabled by modifying the files *Repository.exe.conf* and *capabilities.json*, followed by a restart of the Qlik Sense Service Dispatcher and the Qlik Sense Repository Service.

Do the following:

1. Open *C:\Program Files\Qlik\Sense\Repository\Repository.exe.conf* and set the following key to true:
    ```
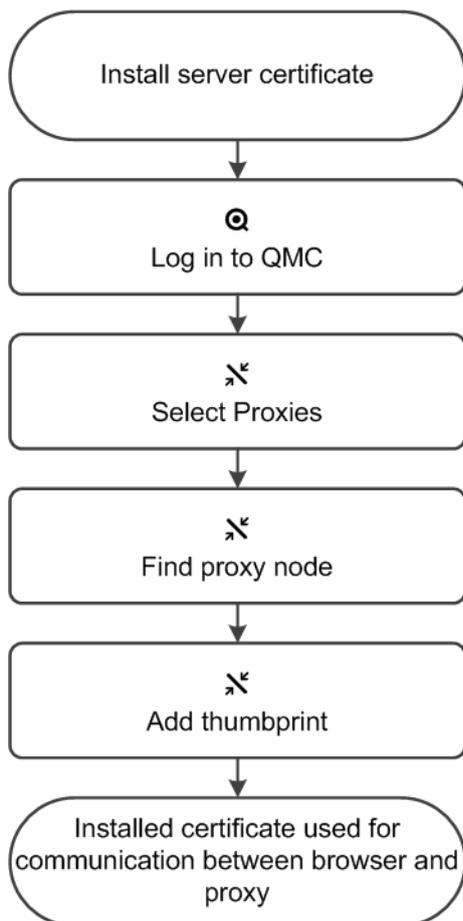    <add key="ContentCacheControl" value="true" />
    ```

2. Open *C:\Program Files\Qlik\Sense\CapabilityService\capabilities.json* and add the following flag:
    ```
    {"contentHash":"2ae4a99c9f17ab76e1eeb27bc4211874","originalClassName":"FeatureToggle","flag":"QMC_CONTENT_CACHE_CONTROL","enabled":true}
    ```

Content cache-controls are added or modified in the Content library associated items section in the Qlik Management Console (QMC), see *Content library: associated items (page 45)*. Once configured, content cache-controls are automatically associated with a particular content library and will only affect requests targeting its content. To create content cache-controls targeting other requests, so-called general content cache-controls, the reference to the content library needs to be removed. You do this by setting the `contentLibrary` value to `null`, using the available API PUT method, see the following example. Content cache-controls can also be created directly through an API request by using the POST method.

```
PUT /qrs/contentcachecontrol/33774a23-ad86-44f7-96bc-0e346c062cc2
{
  "id": "33774a23-ad86-44f7-96bc-0e346c062cc2",
  "createdDate": "2021-12-09T11:59:20.728Z",
  "modifiedDate": "2021-12-09T11:59:20.728Z",
  "modifiedByUserName": "RDLUND\\svc-silver",
  "name": "api",
  "contentLibrary": null,
  "filter": "test",
  "maxAge": 3600,
  "cachePolicy": 0,
  "privileges": null,
  "schemaPath": "ContentCacheControl"
}
```

Requests to fall under defined content cache-control are filtered based on the value of the user-defined regular expression – `regex filter` as seen in the QMC, or `filter` filed as seen in the `ContentCacheControl` model, see *Content library: associated items (page 45)* for examples. Part of the URI's request evaluated consists of the text after the hostname, not including the virtual proxy's prefix. Content library controls associated with content libraries take precedence over the general ones when the Qlik Sense Repository Service is looking for a match. They are implemented in stack, meaning that the first match terminates further lookup. When several controls match the user-defined filter, the match with the latest modified date - `modifiedDate` takes precedence. With the default security rules set, only the RootAdmin role has full CRUD access to content cache-controls. In addition ContentAdmin and SecurityAdmin roles have Read access to all content cache-controls. Users with Read privilege on corresponding content libraries have Read access to content cache-controls associated with those content libraries, see the `ReadContentCacheControl` rule in *Security rules included in Qlik Sense (page 535)*.

Content cache-controls for hub specific requests that include `api` in the URI are fetched on startup of the Hub service. For newly added or modified content cache-controls, targeting those requests to apply, a restart of the Hub service is required by restarting Qlik Sense Service Dispatcher, or by terminating the corresponding node.js process - "*..\HubService\index.js*. For other types of requests, no restart is required after creating a new entry or modifying an existing one.

For new methods as per Open API specification for Repository Main API, see: Contentcachecontrol.

For corresponding models as per Open API specification for Repository Main API, see: ContentCacheControl and ContentCacheControlCondensed.

1.9   Designing access control

There are concepts that are fundamental to understanding how to design access control in Qlik Sense.

The topics in this section describe these concepts together with the conventions, rule syntax, and editor with which you build and activate your attribute-based security rules.

- Access control is property-based.
- Security rules are inclusive by design.

Properties

In Qlik Sense, attributes are referred to as properties. Properties are used to identify the user who is requesting access, the resource that is impacted by the request, and the environment from which the request is made. In Qlik Sense you can use default property types that are supplied out-of-the-box, properties supplied by the directory services through user directory connectors, or you can define your own customized properties.

Custom properties (page 514)

Default properties

Qlik Sense provides default properties that you can use to describe the subject (user), environment, and resources. In the example *One property-value pair in conditions: (page 516)*, the user group membership (AD group) was used as a property to identify the user. We could also have added an environment property, such as IP or request type, to limit the access to one or more IP addresses or HTTPS request types, respectively.

Directory services properties

As you connect Qlik Sense to directory services, using user directory connectors in the QMC, the user properties from the directory services will be made available to you. You can see the properties in the user condition drop-down list when you create rules.

Custom properties

Custom properties enable you to define properties of your own and assign possible values. This enables you to complement default environment properties with properties of your own. Custom properties also enable you to work with user roles or types.

For example, you may have Qlik Sense developers, contributors, and consumers in your organization. Let's assume that these user types are not defined as groups in your directory service. With custom properties you have the option of defining a UserType property. You can then assign the possible values Developer, Contributor, or Consumer to your users and apply rules per user type instead of applying them to individuals or to user group memberships.

You can see the custom properties in the user condition drop-down list when you create rules. Custom properties have the "@" suffix in the list.

Property-based access control

Access control is property-based and the properties are used to describe the parties involved in an access request. In this case the parties involved are the following:

- The *User* making the request
- The *Environment* the request is made from
- The *Resource* the request applies to

Each property is defined by a value in a so called property-value pair such as "group = Sales" or "resourcetype = App". Each request in turn includes the property-value pairs for the users, environments and resources involved in the request together with the action that the requester wants to perform on the resource, for example create, update, or delete.
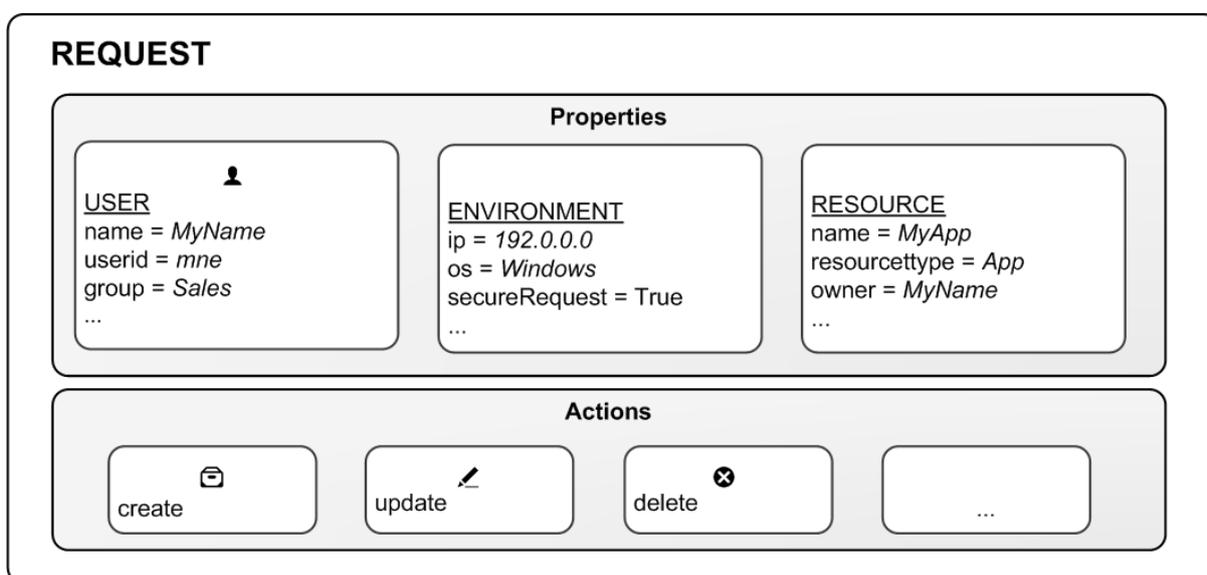
Access request

Evaluating access using rules

You can create rules based on the property-value pairs. By this we mean that requests for an action on a resource is granted only if the property value of the requester matches the property-value conditions defined in a security rule for that resource.

In general a rule can read as a sentence:

"Allow the requester to [action] the [resource] provided that [conditions]."

Each rule must describe the action and the resource or resources the action should be applied to. If you don't define any rules for a resource then no users will have access to that resource.

> *You are not required to provide conditions. However, not doing this will result in the rule applying to all users and/or resources.*

Having received the request, the rule engine will evaluate the request against all rules that are applicable. Applicable rules are those that apply to the same resource type as the request. Each rule comes with a resource filter to save the rule engine from having to evaluate the request against all resources. Finally you can specify exactly which resource a rule applies to by providing resource property conditions in the condition.

The rule evaluation workflow

Example: One property-value pair in conditions:

For example, assume that you work in the sales department at your company and want to read the Quarterly results stream published by the financial department. In this case there is a rule on that stream that states that only users who belong to the Active Directory group finance are allowed to read that stream.

Translating this into a rule could look like this:

"Allow the user to [read] the [Quarterly results stream] provided that [group=finance]."

In this example the rule will evaluate to False, that is to say you do not have read access because group does not equal finance for this user. In practice you will not even see the stream icon.
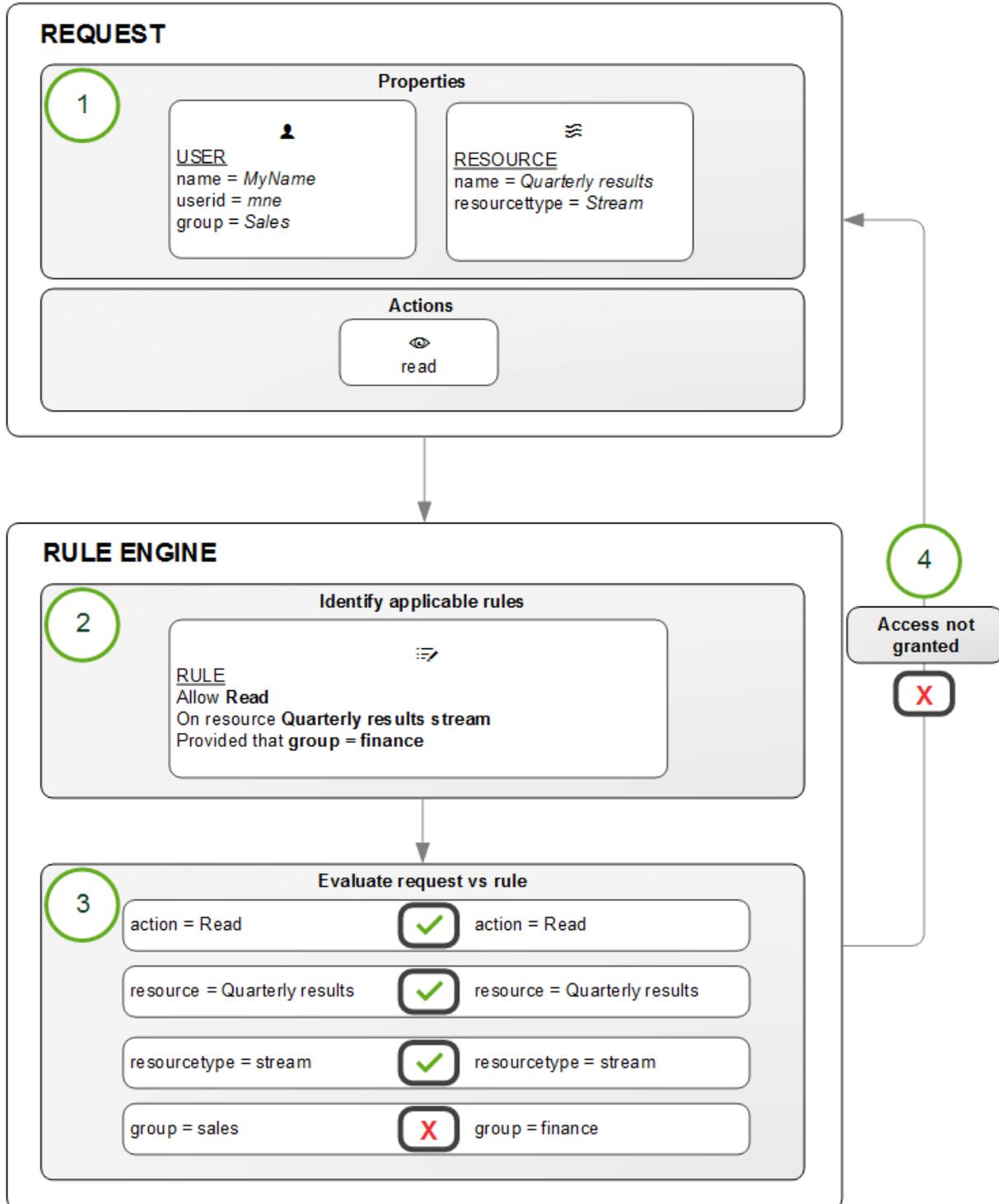
Rule evaluation

The rule evaluation workflow is as follows:

1. Request to [read] the [Quarterly results stream] sent by user
2. The rule engine identifies which rules to evaluate the request against

3.   The request is evaluated by the rule engine

4.   If any criteria is not met, you are not granted access

Example: More than one property-value pair in conditions:

The rule evaluation workflow example was basic in that it has one action on one resource with one condition. However, the strength of the Qlik Sense security rules is that you can apply several actions to multiple resources with different conditions in one rule. Looking at the Quarterly results example, we could extend the rule to provide read and update access to both the finance and the management departments using their Active Directory groups as input:

"Allow the user to read AND update the [Quarterly results stream] provided that group = finance OR group = management."

Predefined security rules in Qlik Sense

Qlik Sense is supplied with predefined sets of rules called **ReadOnly** and **Default** rules. These rules are supplied to make it possible for QMC administrators to maintain the Qlik Sense system and create, update and maintain security rules. ReadOnly rules are ones that are critical to the security and cannot be edited. Default rules can be edited to suit your company and system requirements.

> *If you edit a default rule, that is, a rule that is supplied with Qlik Sense, the rule type definition changes from* **Default** *to* **Custom**. *Keep in mind that changing a default rule, or adding a new rule that affects the default rules, may cause unexpected behavior in Qlik Sense. Use the rule preview feature to check rule behavior before implementing changes to default rules. Remember that only read only and default rules are automatically updated when you upgrade to a new Qlik Sense version.*

How security rules work

In Qlik Sense Enterprise on Windows you can use security rules to grant users access to resources such as apps and streams. All security rules are inclusive by nature, that is, you always grant users access to a resource, you never create a rule to deny users access. The purpose of a security rule is usually to only allow some users access to a resource. Making sure that only the right users have access to a resource is a task for a security rules admin (SecurityAdmin).

Two simple security rules

As a light start, let's look at two of the security rules that are included in an installation of Qlik Sense Enterprise on Windows, *StreamEveryone* and *StreamEveryoneAnonymous*.

Security rule StreamEveryone, installed with Qlik Sense Enterprise on Windows

In the **Identification** section, you can see that the rule is active, because it is not disabled. The purpose of the rule is stated in the **Description** box.

In the **Basic** section, the resource filter pinpoints a specific stream. The first part of the filter identifies the resource type, *Stream*, the second part is a globally unique identifier (GUID). The resource filter indicates the scope of the rule. This is where you define what type of entity that the rule covers. The resource filter makes it possible to, for instance, have a different set of rules that affect which data connections a user is allowed to see compared to the rules defining which apps that users can see.

See: *Defining resource filters (page 567)*

The actions that users can perform are *Read* and *Publish*. All users can access content in the stream, such as apps and app objects. Users can also publish apps and app objects to the stream.

In the **Advanced** section, the condition is !userIsAnonymous(). This rule excludes anonymous users and therefore the statement in **Description** is not true for exactly all users. See *IsAnonymousBoolean function for user conditions that returns True if the user requesting access has logged in as anonymous. Otherwise returns False. user.IsAnonymous() Examples and resultsExamples and resultsExampleResultResource filter: Stream_ *Conditions: user.IsAnonymous()Action: readAnonymous users are allowed to read streams.Resource filter: Stream_*Conditions: !user.IsAnonymous()Action: read, publishAll users that are not anonymous (notice the NOT operator, !, in front of the condition) are allowed to read and publish streams. Anonymous users will have no access to streams. (page 1)* for details about the IsAnonymous() function.

Context: The rule applies both to users accessing the *Everyone* stream from the hub and from the QMC.

Because anonymous users will not have access to the stream *Everyone* through the rule *StreamEveryone*, a separate rule is needed.

Security rule StreamEveryoneAnonymous, installed with Qlik Sense Enterprise on Windows

The rule is *StreamEveryoneAnonymous* is similar to the *StreamEveryone* rule, with three exceptions:

- The only action that can be performed is *Read*, *Publish* is not possible.
- The condition is `userIsAnonymous()`, which means that the rule only applies to anonymous users.
- The context is *Only in hub*. Anonymous users don't have access to the QMC.

The need for two rules for the *Everyone* stream is due to the differences in actions and context. Had it not been for those differences, *StreamEveryone* would have been sufficient.

Creating a stream and a security rule with custom properties

Even if there are many rules installed with Qlik Sense Enterprise on Windows, you will have to create new security rules that meet the specific needs of your organization. When you create security rules, you can facilitate administration by either using custom properties or user roles. Here custom properties are introduced. For user roles, see *Defining user roles for security rules (page 529)*.

With custom properties, you can easily add or remove user access without changing the security rule. In this example there are no custom properties defined yet.

Defining custom properties

Assume that two groups of users, *Finance* and *Sales*, need access to a stream called *Quarterly Report*, where quarterly reports apps are published. These groups are not yet defined in the user directory, and so, you need to define them. You do that by creating a custom property with the values *Finance* and *Sales*.

Creating the custom property

Create a custom property called *Department*, with the values *Finance* and *Sales*.

1. On the QMC start page, select **Custom properties**.
2. Click **Create new**.
   The custom property edit page opens.
3. Enter the name *Department*.
4. For **Resource types**, select **Streams** and **Users**.
   These are the resources that are needed for the security rule.
5. Under **Values**, click **Create new**.
6. Add value *Finance* and click **Create new**.
7. Add value *Sales*.
8. Click **Apply**.

A new custom property called *Department* is created with two values, *Finance* and *Sales*, which you assign to users of the respective groups.

Assigning the custom properties values to users

1. In the QMC, open **Users**.
2. Open the Column selector (▦) and select *@Department*, which might be the last item in the list.
3. Select the users that you want to add to the *Finance* group, multi-select is possible.
4. Select **Edit**.
5. In the **Properties** section, ensure that **Custom properties** is selected.
   The **Custom properties** section is displayed and *Department* is an option.

6. Click the box for *Department* and select the value *Finance*.

7. Repeat the steps until all users in Finance have the value *Finance*.

8. Click **Apply**.

9. Perform the corresponding actions for members of the *Sales* group.

You now have two custom property groups, *Finance* and *Sales*, that can be used in several different security rules. Users can easily be added or removed. You can also add additional departments as values for the custom property.

> *If a group is not easily defined because it consists of people from different parts of the company, you can define a custom property with a name that clearly states its purpose. In the current example StreamQuarterlyReport_Read is a possible name. The only value you need for that custom property is then Read.*

Creating the stream and security rule

You now have your custom property values and can create the stream *Quarterly Report* and the security rule that grants the user groups access to the stream.

1. From the QMC start page, go to **Streams** and click **Create new**.

2. Name the stream *Quarterly Report*.

3. Click **Apply**.
    The security rule editor appears. If you decide to cancel the creation of a security rule, the stream will not have any security rule and all users will have access to that stream. That is most likely not what you want.

4. Name the security rule *StreamQuarterlyReport_Read*. (Section **Identification** needs to be selected.)

5. Optionally, add a description.

6. The **Resource filter** is already present with a unique stream ID.

7. For **Actions**, keep **Read** and clear the **Publish** selection.

8. In the rule editor, select *user*, *@Department*, *=*, *value*, *Finance*, as shown in the image.

Security rule StreamQuarterlyReport_Read

9. Click **Validate rule** to check that the rule syntax is correct. The logic of the rule is not tested.
10. Click **Apply** to save the rule.

You might be wondering about what happened to the *Sales* group. There are different ways of adding that user group. You can make the change directly in the **Conditions** box, but the safest way is to use the rule editor.

1. Under **Associated items**, select **Security rules**.
2. Double-click *StreamQuarterlyReport_Read*.
3. In the **Basic** section, click **+** in the rule editor.
4. Select the operator oʀ and then *user*, *@Department*, *=*, *value*, *Sales*, as shown in the image.
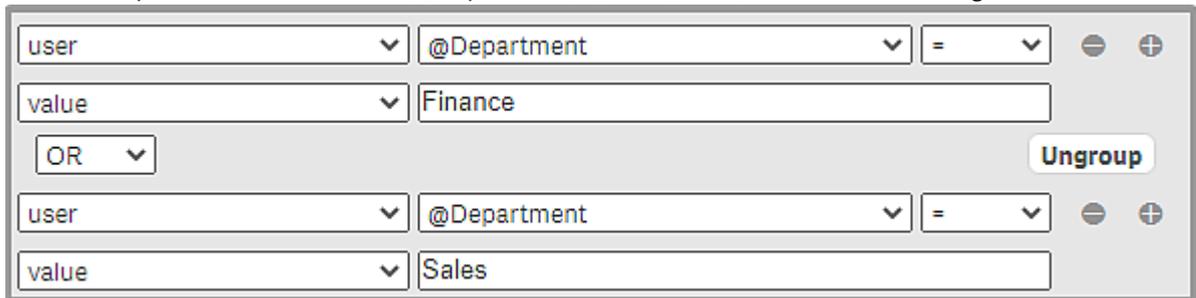
Rule editor with updated conditions

> The string in the **Conditions** box is updated to reflect the change in the rule editor and now looks as follows: `((user.@Department="Finance" or user.@Department="Sales"))`. If you instead had made the change directly in the **Conditions** box, the rule editor would have been updated accordingly.

5. Click **Apply**.

Another option for the *Sales* group could be to create a separate security rule with the actions *Read*, *Publish*, and *Update* that could be relevant to the *Sales* group.

> *For more information about the security rule editor, see The security rule editor (page 562)*

Auditing the new rule

It is important to verify that the new security rule grants the right sort of access to the right users.

1. Still on the page *Stream: associated items*, click **Audit rule** to open the page for editing and auditing the your newly created rule.
2. Auditing of your stream is set up, you just need to click **Audit**.

The new security rule is now tested against the user directory and should result in a list of people from *Sales* and *Finance* having **R** indicating that they have read rights to the stream.

Audit result for users from Finance and Sales with read access to the stream Quarterly Report

Creating a stream and a security rule with a custom property for an existing group

Often a company has a user directory, such as Active Directory, which can be used in a custom property to grant all its users access to a stream.

Creating the custom property

Create a custom property called *ADGroupStream_Read*.

1. On the QMC start page, select **Custom properties**.
2. Click **Create new**.
   The custom property edit page opens.
3. Enter the name *ADGroupStream_Read*.
4. For **Resource types**, select **Streams** and **Users**.
   These are the resources that are needed for the security rule.
5. Click **Apply**.

In this case, no specific custom property values are required. All users belong to the same user directory, and therefore the custom property name can be used in the security rule. Being a member of that directory grants access to the stream.

For more information about directory services properties, see *Properties (page 514)*

Creating the security rule

You now have the custom property and can create the security rule that grants users access to the stream *Quarterly Report*.

1. From the QMC start page, go to **Security rules** and click **Create new**.
2. Name the security rule *ADGroupStreamQuarterlyReport_Read*.
3. For **Resource filter**, enter *Stream_**.
4. For **Actions**, select **Read**.
5. In the rule editor, Select *#Stream, @ADGroupStream_Read*, =, *user*, *group*, as shown in the image.

Security rule ADGroupStreamQuarterlyReport_Read

6. For **Context**, select *Only in hub*.
   This rule only applies to users who access the stream from the hub.

7. Click **Apply** to save the rule.

The new security rule is created and all users in the Active Directory group have read access to the stream *Quarterly Report*.

Defining user roles for security rules

User roles is a way to facilitate rule administration without using custom properties. You define roles and assign them to users. A role can be used in several security rules to grant access to all users with that role.

Creating a stream and security rules with user roles

Let's assume that you want to have two user roles, one for developers and one for testers. These roles have different access needs, so two security rules are required.

Defining security rules for testers and developers

Assume also that it is enough for testers to have read access to the stream.

1. From the QMC start page, go to **Streams** and click **Create new**.
2. Name the stream *TestStream1*.
3. Click **Apply**.
   The **Edit security rule** page appears. If you decide to cancel the creation of a security rule, the stream will not have any security rule and all users will have access to that stream. That is most likely not what you want.

Security rule for Tester access to TestStream1

4. In **Properties**, select **Identification**.

---

5. For **Name**, enter *Tester_<GUID of the stream>*, (GUID from the **Resource filter**).

6. For **Actions**, keep **Read** and clear the **Publish** selection.

7. In the rule editor, select *user*, *roles*, *=*, *value*, and manually enter *Tester*, as shown in the image.
    The access rights defined in the **Resource filter**, **Conditions**, and **Actions** fields are applied to the user role *Tester*. This role will now be available to apply to users.

8. Click **Validate rule** to check that the rule syntax is correct. The logic of the rule is not tested.

9. Click **Apply** to save the rule.

10. Under **Associated items**, click **Security rules**.

> *Here you find all the security rules that are associated with this specific stream.*

11. Click **Create associated rule** to create another rule for the same stream, this time for developers.

12. For **Name**, enter *Developer_<GUID of the stream>*, (GUID from the **Resource filter**).

13. For **Actions**, **Read**, **Update**, **Delete**, and **Publish** should all be selected.

14. In the rule editor, select *user*, *roles*, *=*, *value*, and manually enter *Developer* as shown in the image.
    This role will now be available to apply to users.

Security rule for Developer access to TestStream1

15. Click **Validate rule** to check that the rule syntax is correct. The logic of the rule is not tested.

16. Click **Apply** to save the rule.

You now have two user roles, *Tester* and *Developer*, that can be used in several different security rules. Users can easily be added or removed. Additional user roles can be created in the same way.

Assigning the roles to users

1. In the QMC, open **Users**.

2. Select the users that you want to have the role *Tester*, multi-select is possible.

3. Click **Edit**.

4. Click **Add role** and select *Tester* from the list.

5. Click **Apply**.

6. Click **Users** to open the user overview.
   Verify that the users have the role *Tester* in the **Admin role** column.

7. Perform the corresponding actions for users who should have the role *Developer*.

Auditing the new rules

It is important to verify that the new security rule grants the right sort of access to the right users.

1. Go to **Streams** and double-click *TestStream1*.
   The **Edit stream** page appears.

2. Under **Associated items**, click **Security rules**.
   The security rules associated with this stream are displayed.

3. Select *Tester_<GUID>* and click **Audit rule**.
   (You could also select *Developer_<GUID>*, it's the same stream that is targeted.)

4. Click **Audit**.
   The security rules for this stream are now tested against the user directory and should result in a list of people where testers only have **R** indicating read access, and developers with **RUDP** (**Read**, **Update**, **Delete**, and **Publish**).

Audit result for users with the role Tester or Developer

Rules hierarchy

When designing security rules, it is important to understand the hierarchical relationships between different resource filters. Being unaware of such relationships might result in rules not working as intended. Access to items often involves more than one security rule. To be able to use an app, it is not sufficient to have read access to that app, you also need access to the stream where the app is published. Should you also want to edit an app object in the app, you would need an additional rule granting updating rights to that app object.
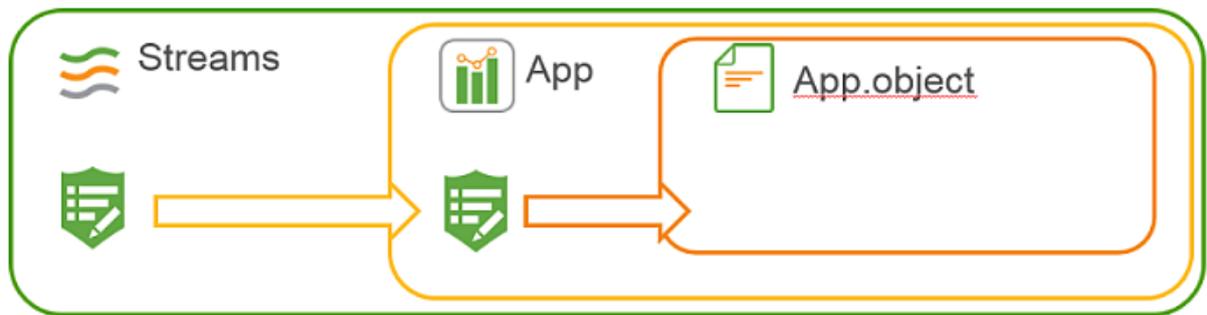
Rules hierarchy. Access to an app object requires app access, which in turn requires stream access.

If you now consider what you have achieved so far, granting users access to the streams, it seems there are more security rules needed before users can open apps and see app object. However, that is not necessary and the reason is that such a rule already exists. As mentioned earlier, a number of security rules are installed with Qlik Sense Enterprise on Windows. Some of these rules are essential for the system to work and can therefore not be edited or deleted. Other rules are present for convenience, and in our case it is convenient that the security rule *Stream* exists. This is what the rule looks like.

Security rule Stream, included in a Qlik Sense Enterprise on Windows installation

The rule description states the following: "*The user should see the resource if he/she has read access to the stream it is published to*". If you have read access to a stream you will, through this rule, also be able to see content that has been added to that stream. Because this rules exists, you needn't create the any rules that grant users read access to the apps and app objects, it's all been taken care of.

Note that the value for **Resource filter** is `App*`. The `App*` value covers both apps and app objects. The default value for app access when you create a rule from template is `App_*` and then only apps are covered, not app objects.

The conditions for the rule might look a little intimidating, but let's look at one part at a time:

First part: `resource.resourcetype = "App" and resource.stream.HasPrivilege("read")`.

This condition requires that you have read access to the stream where the app is published. If you do, you will have read access to apps (as stated in the **Actions** section).

Second part: `or ((resource.resourcetype = "App.Object" and resource.published ="true" and resource.objectType != "app_appscript" and resource.objectType != "loadmodel") and resource.app.stream.HasPrivilege("read"))`

This part of the condition also relies on you having read rights to the stream where the app object is published. If you do, you will have read access to app objects (except `app_appscript` and `loadmodel`), given that the app object is published.

To have a general security rule such as *Stream* is a convenient solution to simplify granting access to content in streams. But if you want to limit access to an app or an app object you have to create a new rule with certain conditions and disable the already existing rule that grants access. Remember, it is enough that there is one security rule granting users access to a resource for them to have access. They will then have access to the resource even if there exists another rule by which they aren't granted access.

Creating a new rule based on an existing rule

Qlik Sense Enterprise on Windows comes with a number of security rules included by default. The rules are of two types: Default and Read only. Read only rules are required for the system to function and can therefore not be edited or deleted. Default rules can be edited, and when you do, the rule type is changed to a third type, Custom. If you want to edit an existing Default rule, it is strongly recommended that you make a copy and edit the copy. You might need the original later on.

Security rules included in Qlik Sense (page 535)

Performance

It's important to think about performance when designing security rules. As the number of apps, streams, and security rules increases, performance can become an issue with slow start-up of the hub and long response times. To be able to design security rules that benefit performance, it's necessary to understand the rule evaluation process.

For an overview of the evaluation steps, see *The evaluation flow (page 591)*.

For best practices in the QMC and guidelines for writing efficient security rules, see *QMC performance – best practices (page 444)*.

Security rules included in Qlik Sense

In a Qlik Sense installation, a number of security rules are included by default and available in the QMC. The security rules can be used to grant users access to areas in Qlik Sense. There are three types of rules: Default, Read only, and Custom. The Read only rules are essential to Qlik Sense and cannot be edited or deleted. The Default rules can be edited. When you edit a Default rule or create a new rule, the type is changed to Custom.

> *If you want to edit a Default rule, we strongly recommend that you create a copy of the original and edit the copy, because you may want to use original rule later on. Remember to disable the original rule before using the copy.*

The following security rules are included by default in a Qlik Sense installation.

AuditAdmin

AuditAdmin security rule properties

Property	Details
Name	AuditAdmin
Description	Audit admin should have read rights to audit entities
Resource filter	*
Actions	Read
Context	Only in QMC
Type	Default
Conditions	user.roles = "AuditAdmin" and !(resource.resourcetype = "TransientObject" and resource.name like "QmcSection_*")

AuditAdminQmcSections

AuditAdminQmcSections security rule properties

Property	Details
Name	AuditAdminQmcSections
Description	Audit admin should have read rights to audit related sections
Resource filter	License_*,TermsAcceptance_*,QmcSection_AppDistributionStatus,QmcSection_ CloudDistribution, QmcSection_Tag,QmcSection_Audit,QmcSection_DeploymentSetup
Actions	Read
Context	Only in QMC

Property	Details
Type	Default
Conditions	((user.roles="AuditAdmin"))

Content library content

Content library content security rule properties

Property	Details
Name	Content library content
Description	Everyone who has read rights to a content library should also have read rights to its corresponding files
Resource filter	StaticContentReference_*
Actions	Read
Context	Both in hub and QMC
Type	Read only
Conditions	resource.ContentLibrarys.HasPrivilege("Read")

Content library manage content

Content library manage content security rule properties

Property	Details
Name	Content library manage content
Description	Everyone who has update rights to a content library should also have rights to manage its corresponding files
Resource filter	StaticContentReference_*
Actions	Create, Read, Update, Delete
Context	Both in hub and QMC
Type	Read only
Conditions	resource.ContentLibrarys.HasPrivilege("Update")

ContentAdmin

ContentAdmin security rule properties

Property	Details
Name	ContentAdmin

Property	Details
Description	Content admin should have rights to manage content related entities
Resource filter	Stream_*,App*,ReloadTask_*,ExternalProgramTask_*,UserSyncTask_*, SchemaEvent_ *,User*,CustomProperty*,Tag_*,DataConnection_*,CompositeEvent_*,Extension_ *,ContentLibrary_*,FileExtension_*,FileExtensionWhiteList_*,SystemNotification_ *,CustomBannerMessage_*
Actions	Create, Read, Update, Delete, Export, Publish, Change owner
Context	Only in QMC
Type	Default
Conditions	((user.roles="ContentAdmin"))

ContentAdminQmcSections

ContentAdminQmcSections security rule properties

Property	Details
Name	ContentAdminQmcSections
Description	Content admin should have read rights to content related sections
Resource filter	License_*,TermsAcceptance_*,QmcSection_Stream,QmcSection_App,QmcSection_ App.Object, QmcSection_AppDistributionStatus,QmcSection_ CloudDistribution,QmcSection_DataConnection, QmcSection_Tag,QmcSection_ User,QmcSection_CustomPropertyDefinition,QmcSection_Task, QmcSection_Event, QmcSection_SchemaEvent,QmcSection_CompositeEvent,QmcSection_Extension, QmcSection_ReloadTask,QmcSection_UserSyncTask,QmcSection_ContentLibrary, QmcSection_Audit,QmcSection_AnalyticConnection,QmcSection_SystemNotification, QmcSection_SystemNotificationPolicy,QmcSection_DeploymentSetup,QmcSection_ CustomBannerMessage
Actions	Read
Context	Only in QMC
Type	Default
Conditions	((user.roles="ContentAdmin"))

ContentAdminRulesAccess

ContentAdminRulesAccess security rule properties

Property	Details
Name	ContentAdminRulesAccess
Description	Content admin should have rights to manage security rules for streams, data connections, content libraries, and extensions

Property	Details
Resource filter	SystemRule_*
Actions	Create, Read, Update, Delete
Context	Only in QMC
Type	Default
Conditions	user.roles = "ContentAdmin" and (resource.category = "Security" and (resource.resourcefilter matches "Stream_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}" or resource.resourcefilter matches "DataConnection_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}" or resource.resourcefilter matches "ContentLibrary_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}" or resource.resourcefilter matches "Extension_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}") or (resource.category = "Generic" and resource.subcategory = "SystemNotification"))

CreateApp

CreateApp security rule properties

Property	Details
Name	CreateApp
Description	Everyone, except anonymous users, should have rights to create apps
Resource filter	App_*
Actions	Create
Context	Only in hub
Type	Default
Conditions	!user.IsAnonymous()

CreateAppObjectsPublishedApp

CreateAppObjectsPublishedApp security rule properties

Property	Details
Name	CreateAppObjectsPublishedApp
Description	Everyone who has read rights to a published app should also have rights to create sheets, stories, bookmarks and snapshots belonging to that app
Resource filter	App.Object_*
Actions	Create
Context	Only in hub
Type	Default

Property	Details
Conditions	!resource.App.stream.Empty() and resource.App.HasPrivilege("read") and (resource.objectType = "userstate" or resource.objectType = "sheet" or resource.objectType = "story" or resource.objectType = "bookmark" or resource.objectType = "snapshot" or resource.objectType = "embeddedsnapshot" or resource.objectType = "hiddenbookmark") and !user.IsAnonymous()

CreateAppObjectsUnPublishedApp

CreateAppObjectsUnPublishedApp security rule properties

Property	Details
Name	CreateAppObjectsUnPublishedApp
Description	Everyone who has read rights to an unpublished app should also have rights to create app objects belonging to that app
Resource filter	App.Object_*
Actions	Create
Context	Only in hub
Type	Default
Conditions	resource.App.stream.Empty() and resource.App.HasPrivilege("read") and !user.IsAnonymous()

CreateOdagLinks

CreateOdagLinks security rule properties

Property	Details
Name	CreateOdagLinks
Description	Non-anonymous users with read access to the ODAG template app can create links and it is possible to create a link without first knowing the template app
Resource filter	OdagLink_*
Actions	Create
Context	Only in hub
Type	Default
Conditions	!user.IsAnonymous() and (resource.templateApp.Empty() or resource.templateApp.HasPrivilege("read"))

CreateOdagLinkUsage

CreateOdagLinkUsage security rule properties

Property	Details
Name	CreateOdagLinkUsage
Description	Non-anonymous users with read access to the selectionApp and read access to the link can create OdagLinkUsages
Resource filter	OdagLinkUsage_*
Actions	Create
Context	Only in hub
Type	Default
Conditions	!user.IsAnonymous() and (resource.selectionApp.Empty() or resource.selectionApp.HasPrivilege("read")) and (resource.link.Empty() or resource.link.HasPrivilege("read"))

CreateOdagRequest

CreateOdagRequest security rule properties

Property	Details
Name	CreateOdagRequest
Description	Non-anonymous users with read access to the link can create new Requests using that link
Resource filter	OdagRequest_*
Actions	Create
Context	Only in hub
Type	Default
Conditions	!user.IsAnonymous() and (resource.link.HasPrivilege("read"))

Custom banner message

Custom banner message security rule properties

Property	Details
Name	Custom banner message
Description	Allows all users to see the custom banner messages
Resource filter	CustomBannerMessage_*
Actions	Read

Property	Details
Context	Only in hub
Type	Default
Conditions	true

DataConnection

DataConnection security rule properties

Property	Details
Name	DataConnection
Description	Data connections can be created for all resource types, except "folder"
Resource filter	DataConnection_*
Actions	Create
Context	Only in hub
Type	Default
Conditions	((resource.type!="folder"))

DataPrepAppCacheAccessRule

DataPrepAppCacheAccessRule security rule properties

Property	Details
Name	DataPrepAppCacheAccessRule
Description	Everyone, except anonymous users, should have read rights to data connections
Resource filter	DataConnection_<Connection_ID>
Actions	Read
Context	Both in hub and QMC
Type	Custom
Conditions	!user.isAnonymous()

Default content library

Default content library security rule properties

Property	Details
Name	Default content library
Description	Everyone should have read rights to the default content library

Property	Details
Resource filter	ContentLibrary_<Content library ID>
Actions	Read
Context	Both in hub and QMC
Type	Default
Conditions	true

DeleteOdagLinkUsage

DeleteOdagLinkUsage security rule properties

Property	Details
Name	DeleteOdagLinkUsage
Description	Non-anonymous users with read access on the selection app can delete OdagLinkUsages for that app
Resource filter	OdagLinkUsage_*
Actions	Read, Delete
Context	Only in hub
Type	Default
Conditions	!user.IsAnonymous() and resource.selectionApp.HasPrivilege("read")

DeploymentAdmin

DeploymentAdmin security rule properties

Property	Details
Name	DeploymentAdmin
Description	Deployment admin should have access rights to deployment related entities
Resource filter	ServiceCluster_*,ServerNodeConfiguration_ *,Engine*,Proxy*,VirtualProxy*,Repository*,Printing*,Scheduler*, User*,CustomProperty*,Tag_*,License*, TermsAcceptance_*,ReloadTask_ *,ExternalProgramTask_*, UserSyncTask_*,SchemaEvent_*,CompositeEvent_*, Deployment_*,IdentityProviderSettings_*, SystemNotification_*,CustomBannerMessage_*
Actions	Create, Read, Update, Delete
Context	Only in QMC
Type	Default
Conditions	((user.roles="DeploymentAdmin"))

DeploymentAdminAppAccess

DeploymentAdminAppAccess security rule properties

Property	Details
Name	DeploymentAdminAppAccess
Description	Deployment admin should have read and update rights to apps in order to handle load balancing rules
Resource filter	App_*
Actions	Read, Update
Context	Only in QMC
Type	Default
Conditions	((user.roles="DeploymentAdmin"))

DeploymentAdminQmcSections

DeploymentAdminQmcSections security rule properties

Property	Details
Name	DeploymentAdminQmcSections
Description	Deployment admin should have read rights to deployment related sections
Resource filter	License_*,TermsAcceptance_*,ServiceStatus_*,QmcSection_AppDistributionStatus, QmcSection_CloudDistribution,QmcSection_Tag,QmcSection_Templates,QmcSection_ ServiceCluster, QmcSection_ServerNodeConfiguration,QmcSection_ EngineService,QmcSection_ProxyService, QmcSection_VirtualProxyConfig,QmcSection_ RepositoryService, QmcSection_SchedulerService,QmcSection_ PrintingService,QmcSection_License*,QmcSection_Token, LoadbalancingSelectList,QmcSection_User,QmcSection_UserDirectory,QmcSection_ CustomPropertyDefinition, QmcSection_Certificates,QmcSection_ Certificates.Export,QmcSection_Task,QmcSection_App,QmcSection_SyncRule, QmcSection_LoadBalancingRule,QmcSection_Event,QmcSection_ ReloadTask,QmcSection_UserSyncTask,QmcSection_Audit, QmcSection_ DistributionPolicy,QmcSection_SystemNotification,QmcSection_SystemNotificationPolicy, QmcSection_DeploymentSetup,QmcSection_CustomBannerMessage
Actions	Read
Context	Only in QMC
Type	Default
Conditions	((user.roles="DeploymentAdmin"))

DeploymentAdminRulesAccess

DeploymentAdminRulesAccess security rules properties

Property	Details
Name	DeploymentAdminRulesAccess
Description	Deployment admin should have rights to manage sync and license rules
Resource filter	SystemRule_*
Actions	Create, Read, Update, Delete
Context	Only in QMC
Type	Default
Conditions	user.roles = "DeploymentAdmin" and (resource.category = "Sync" or resource.category = "License" or resource.category = "Generic")

ExportAppData

ExportAppData security rule properties

Property	Details
Name	ExportAppData
Description	Everyone is allowed to export the app data they are allowed to see, except anonymous users
Resource filter	App_*
Actions	Export data
Context	Both in hub and QMC
Type	Default
Conditions	resource.HasPrivilege("read") and !user.IsAnonymous()

Extension

Extension security rule properties

Property	Details
Name	Extension
Description	Everyone should have read rights to extensions
Resource filter	Extension_*
Actions	Read
Context	Both in hub and QMC

Property	Details
Type	Default
Conditions	true

Extension manage content

Extension manage content security rule properties

Property	Details
Name	Extension manage content
Description	Everyone who has update rights to an extension should have rights to manage its corresponding files
Resource filter	StaticContentReference_*
Actions	Create, Read, Update, Delete
Context	Both in hub and QMC
Type	Read only
Conditions	resource.Extensions.HasPrivilege("Update")

Extension static content

Extension static content security rule properties

Property	Details
Name	Extension static content
Description	Everyone who has read rights to an extension should have read rights to its corresponding files
Resource filter	StaticContentReference_*
Actions	Read
Context	Both in hub and QMC
Type	Read only
Conditions	resource.Extensions.HasPrivilege("Read")

File upload connection object

File upload connection object security rule properties

Property	Details
Name	File upload connection object

Property	Details
Description	Everyone, except anonymous users, should have read rights to data connections used for uploading files to server
Resource filter	DataConnection_<data_connection_ID>
Actions	Read
Context	Both in hub and QMC
Type	Default
Conditions	!user.IsAnonymous()

FolderDataConnection

FolderDataConnection security rule properties

Property	Details
Name	FolderDataConnection
Description	Admins should have rights to manage folder data connections
Resource filter	DataConnection_*
Actions	Create, Read, Update, Delete
Context	Only in hub
Type	Default
Conditions	resource.type = "folder" and (user.roles = "RootAdmin" or user.roles = "ContentAdmin" or user.roles = "SecurityAdmin")

HubAdmin

HubAdmin security rule properties

Property	Details
Name	HubAdmin
Description	Hub admin should have read, create and update rights to reload tasks and schema events
Resource filter	ReloadTask_*,SchemaEvent_*
Actions	Create, Read, Update
Context	Only in hub
Type	Default
Conditions	((user.roles="HubAdmin"))

HubSectionHome

HubSectionHome security rule properties

Property	Details
Name	HubSectionHome
Description	Allows all users to access the home hub section
Resource filter	HubSection_Home
Actions	Read
Context	Both in hub and QMC
Type	Default
Conditions	true

HubSectionTask

HubSectionTask security rule properties

Property	Details
Name	HubSectionTask
Description	Allows all users to access the task hub section
Resource filter	HubSection_Task
Actions	Read
Context	Only in hub
Type	Default
Conditions	true

Installed static content

Installed static content security rule properties

Property	Details
Name	Installed static content
Description	Everyone should have read rights to installed static content
Resource filter	StaticContentReference_*
Actions	Read
Context	Both in hub and QMC
Type	Read only
Conditions	((resource.StaticContentSecurityType="Open"))

ManageAnalyticConnection

ManageAnalyticConnection security rule properties

Property	Details
Name	ManageAnalyticConnection
Description	RootAdmin, ContentAdmin and SecurityAdmin roles should be able to manage an analytical connection
Resource filter	AnalyticConnection_*
Actions	Create, Read, Update, Delete
Context	Both in hub and QMC
Type	Default
Conditions	((user.roles="RootAdmin" or user.roles="ContentAdmin" or user.roles="SecurityAdmin"))

Offline access

Offline access security rule properties

Property	Details
Name	Offline access
Description	Everyone is allowed offline access to the app they are allowed to see except anonymous users
Resource filter	App_*
Actions	Read
Context	Both in hub and QMC
Type	Default
Conditions	resource.HasPrivilege("read") and !user.IsAnonymous()

Owner

Owner security rule properties

Property	Details
Name	Owner
Description	The owner of a resource should have update and delete rights if the resource is not published to a stream
Resource filter	*
Actions	Update, Delete

Property	Details
Context	Both in hub and QMC
Type	Default
Conditions	resource.IsOwned() and (resource.owner = user and !((resource.resourcetype = "App" and !resource.stream.Empty()) or (resource.resourcetype = "App.Object" and resource.published = "true")))

OwnerAnonymousTempContent

OwnerAnonymousTempContent security rule properties

Property	Details
Name	OwnerAnonymousTempContent
Description	An anonymous owner of temporary content should be able to access and delete it
Resource filter	TempContent_*
Actions	Read, Delete
Context	Both in hub and QMC
Type	Read only
Conditions	user.IsAnonymous() and resource.anonymousOwnerUserId = user.userId

OwnerAppApproveAppObject

OwnerAppApproveObject security rule properties

Property	Details
Name	OwnerAppApproveAppObject
Description	The owner of an app should be able to approve app objects belonging to the app
Resource filter	App.Object_*
Actions	Approve
Context	Both in hub and QMC
Type	Default
Conditions	resource.App.owner = user

OwnerPublishAppObject

OwnerPublishAppObject security rule properties

Property	Details
Name	OwnerPublishAppObject
Description	The owner of an app object should have publish rights to the object unless it is approved
Resource filter	App.Object_*
Actions	Publish
Context	Both in hub and QMC
Type	Default
Conditions	resource.IsOwned() and resource.owner = user and resource.approved = "false" and resource.app.stream.HasPrivilege("publish")

OwnerPublishDuplicate

OwnerPublishDuplicate security rule properties

Property	Details
Name	OwnerPublishDuplicate
Description	The owner of an app or a stream should be able to publish, and the owner of an app should be able to duplicate
Resource filter	App_*,Stream_*
Actions	Publish, Duplicate
Context	Both in hub and QMC
Type	Default
Conditions	resource.IsOwned() and resource.owner = user

OwnerRead

OwnerRead security rule properties

Property	Details
Name	OwnerRead
Description	The owner of a resource should have read rights to the resource if it is published to a stream
Resource filter	*
Actions	Read

Property	Details
Context	Both in hub and QMC
Type	Read only
Conditions	resource.IsOwned() and resource.owner = user

OwnerUpdateApp

OwnerUpdateApp security rule properties

Property	Details
Name	OwnerUpdateApp
Description	The owner of an app should be able to update
Resource filter	App_*
Actions	Update
Context	Both in hub and QMC
Type	Default
Conditions	resource.IsOwned() and resource.owner = user

QMCCachingSupport

QMCCachingSupport security rule properties

Property	Details
Name	QMCCachingSupport
Description	Enable this rule along with QmcCacheEnabled flag to support QMC-caching
Resource filter	ExecutionSession_*,ExecutionResult_*,*TaskOperational*
Actions	Read
Context	Only in QMC
Type	Default
Conditions	((user.roles="ContentAdmin" or user.roles="DeploymentAdmin"))

ReadAnalyticConnectionEveryone

ReadAnalyticConnectionEveryone security rule properties

Property	Details
Name	ReadAppContentFiles
Description	Non-anonymous users can read an analytic connection

Property	Details
Resource filter	AnalyticConnection_*
Actions	Read
Context	Only in hub
Type	Read only
Conditions	!user.IsAnonymous()

ReadAppContentFiles

ReadAppContentFiles security rule properties

Property	Details
Name	ReadAppContentFiles
Description	Everyone who has read rights to an app should also have read rights to its content files
Resource filter	StaticContentReference_*
Actions	Read
Context	Both in hub and QMC
Type	Read only
Conditions	resource.AppContents.App.HasPrivilege("Read")

ReadAppContents

ReadAppContents security rule properties

Property	Details
Name	ReadAppContents
Description	Everyone who has read rights to an app should also have read rights to app content belonging to that app
Resource filter	App.Content_*
Actions	Read
Context	Both in hub and QMC
Type	Read only
Conditions	resource.App.HasPrivilege("read")

ReadAppDataSegments

ReadAppDataSegments security rule properties

Property	Details
Name	ReadAppDataSegments
Description	Everyone who has read rights to an app should also have read rights to app data segments belonging to that app
Resource filter	App.DataSegment_*
Actions	Read
Context	Both in hub and QMC
Type	Read only
Conditions	resource.App.HasPrivilege("read") and !user.IsAnonymous()

ReadAppInternals

ReadAppInternals security rule properties

Property	Details
Name	ReadAppInternals
Description	Everyone who has read rights to an app should also have read rights to app internals belonging to that app
Resource filter	App.Internal_*
Actions	Read
Context	Both in hub and QMC
Type	Read only
Conditions	resource.App.HasPrivilege("read")

ReadContentCacheControl

ReadContentCacheControl security rule properties

Property	Details
Name	ReadContentCacheControl
Description	Read-access to parent content library should also give read-access to referencing content cache controls.
Resource filter	ContentCacheControl_*
Actions	Read

Property	Details
Context	Both in hub and QMC
Type	Default
Conditions	((user.roles="ContentAdmin" or user.roles="SecurityAdmin" or resource.contentLibrary.HasPrivilege("read")))

ReadCustomProperties

ReadCustomProperties security rule properties

Property	Details
Name	ReadCustomProperties
Description	Non-anonymous users can read custom property definitions and values
Resource filter	CustomProperty*
Actions	Read
Context	Both in hub and QMC
Type	Default
Conditions	!user.IsAnonymous()

ReadOdagLinks

ReadOdagLinks security rule properties

Property	Details
Name	ReadOdagLinks
Description	Non-anonymous users can read ODAG links
Resource filter	OdagLink_*
Actions	Read
Context	Only in hub
Type	Default
Conditions	!user.IsAnonymous()

ReadOdagLinkUsage

ReadOdagLinkUsage security rule properties

Property	Details
Name	ReadOdagLinkUsage
Description	Non-anonymous users with read access to the selection app can read its OdagLinkUsages

Property	Details
Resource filter	OdagLinkUsage_*
Actions	Read
Context	Only in hub
Type	Default
Conditions	!user.IsAnonymous()

RootAdmin

RootAdmin security rule properties

Property	Details
Name	RootAdmin
Description	Root admin should have full access rights
Resource filter	*
Actions	Create, Read, Update, Delete, Export, Publish, Change owner, Change role, Export data
Context	Only in QMC
Type	Read only
Conditions	((user.roles="RootAdmin"))

SecurityAdmin

SecurityAdmin security rule properties

Property	Details
Name	SecurityAdmin
Description	Security admin should have access rights to security related entities
Resource filter	Stream_*,App*,Proxy*,VirtualProxy*,User*,SystemRule_*,CustomProperty*,Tag_ *,DataConnection_*, ContentLibrary_*,FileExtension_*,FileExtensionWhiteList_ *,Deployment_*, IdentityProviderSettings_*
Actions	Create, Read, Update, Delete, Export, Publish, Change owner
Context	Only in QMC
Type	Default
Conditions	((user.roles="SecurityAdmin"))

SecurityAdminQmcSections

SecurityAdminQmcSections security rule properties

Property	Details
Name	SecurityAdminQmcSections
Description	Security admin should have read rights to security related sections
Resource filter	License_*,TermsAcceptance_*,ServiceStatus_*,QmcSection_Stream,QmcSection_App, QmcSection_App.Object,QmcSection_AppDistributionStatus,QmcSection_ CloudDistribution,QmcSection_SystemRule, QmcSection_DataConnection,QmcSection_ Tag,QmcSection_Templates,QmcSection_Audit,QmcSection_ProxyService,QmcSection_ VirtualProxyConfig,QmcSection_User,QmcSection_CustomPropertyDefinition, QmcSection_Certificates,QmcSection_Certificates.Export,QmcSection_ContentLibrary, QmcSection_AnalyticConnection,QmcSection_DeploymentSetup
Actions	Read
Context	Only in QMC
Type	Default
Conditions	((user.roles="SecurityAdmin"))

SecurityAdminServerNodeConfiguration

SecurityAdminServerNodeConfiguration security rule properties

Property	Details
Name	SecurityAdminServerNodeConfiguration
Description	Security admin should have read rights to the ServerNodeConfiguration entity
Resource filter	ServerNodeConfiguration_*
Actions	Read
Context	Only in QMC
Type	Default
Conditions	((user.roles="SecurityAdmin"))

ServiceAccount

ServiceAccount security rule properties

Property	Details
Name	ServiceAccount
Description	Service accounts should have rights to perform all actions

Property	Details
Resource filter	*
Actions	Create, Read, Update, Delete, Export, Publish, Change owner, Change role, Export data
Context	Both in hub and QMC
Type	Read only
Conditions	((user.UserDirectory="INTERNAL" and user.UserId like "sa_*"))

Shared content manage content

Shared content manage content security rule properties

Property	Details
Name	Shared content manage content
Description	Everyone who has update rights to shared content should also have rights to manage its corresponding files
Resource filter	StaticContentReference_*
Actions	Create, Read, Update, Delete
Context	Both in hub and QMC
Type	Read only
Conditions	resource.SharedContents.HasPrivilege("Update")

Shared content see content

Shared content see content security rule properties

Property	Details
Name	Shared content see content
Description	Everyone who has read rights to shared content should also have read rights to the corresponding files
Resource filter	StaticContentReference_*
Actions	Read
Context	Both in hub and QMC
Type	Read only
Conditions	resource.SharedContents.HasPrivilege("Read")

Stream

	It is not recommended to create rules that allow users to edit published apps in streams.

Stream security rule properties

Property	Details
Name	Stream
Description	Everyone who has read rights to a stream should also have read rights to a resource published to that stream
Resource filter	App*
Actions	Read
Context	Both in hub and QMC
Type	Default
Conditions	(resource.resourcetype = "App" and resource.stream.HasPrivilege("read")) or ((resource.resourcetype = "App.Object" and resource.published ="true" and resource.objectType != "app_appscript" and resource.objectType != "loadmodel") and resource.app.stream.HasPrivilege("read"))

StreamEveryone

StreamEveryone security rule properties

Property	Details
Name	StreamEveryone
Description	Everyone, except anonymous users, should have read and publish rights to the default stream called Everyone
Resource filter	Stream_<stream_ID>
Actions	Read, Publish
Context	Both in hub and QMC
Type	Default
Conditions	!user.IsAnonymous()

StreamEveryoneAnonymous

StreamEveryoneAnonymous security rule properties

Property	Details
Name	StreamEveryoneAnonymous
Description	Anonymous users should have read rights to the default stream called Everyone
Resource filter	Stream_<stream_ID>
Actions	Read
Context	Only in hub
Type	Default
Conditions	user.IsAnonymous()

StreamMonitoringAppsPublish

StreamMonitoringAppsPublish security rule properties

Property	Details
Name	StreamMonitoringAppsPublish
Description	RootAdmin, ContentAdmin, and SecurityAdmin should have publish rights to the default stream called Monitoring apps
Resource filter	Stream_<stream_ID>
Actions	Publish
Context	Only in hub
Type	Default
Conditions	((user.roles="RootAdmin" or user.roles="ContentAdmin" or user.roles="SecurityAdmin"))

StreamMonitoringAppsRead

StreamMonitoringAppsRead security rule properties

Property	Details
Name	StreamMonitoringAppsRead
Description	Default administrators should have read rights to the default stream called Monitoring apps
Resource filter	Stream_<stream_ID>
Actions	Read

Property	Details
Context	Both in hub and QMC
Type	Default
Conditions	((user.roles="RootAdmin" or user.roles="ContentAdmin" or user.roles="SecurityAdmin" or user.roles="DeploymentAdmin" or user.roles="AuditAdmin"))

Temporary content

Temporary content security rule properties

Property	Details
Name	Temporary content
Description	Everyone, except anonymous users, should have rights to create temporary content
Resource filter	TempContent_*
Actions	Create
Context	Both in hub and QMC
Type	Read only
Conditions	!user.IsAnonymous()

UpdateAppContentFiles

UpdateAppContentFiles security rule properties

Property	Details
Name	UpdateAppContentFiles
Description	Everyone who has update rights to an app should also have rights to manage its content files
Resource filter	StaticContentReference_*
Actions	Create, Read, Update, Delete
Context	Both in hub and QMC
Type	Read only
Conditions	resource.AppContents.App.HasPrivilege("Update")

UpdateAppContents

UpdateAppContents security rule properties

Property	Details
Name	UpdateAppContents
Description	Everyone who has update rights to an app should also have update rights to app content belonging to that app
Resource filter	App.Content_*
Actions	Update
Context	Both in hub and QMC
Type	Read only
Conditions	resource.App.HasPrivilege("update")

UpdateAppDataSegments

UpdateAppDataSegments security rule properties

Property	Details
Name	UpdateAppDataSegments
Description	Everyone who has update rights to an app should also have rights to manage app data segments belonging to that app
Resource filter	App.DataSegment_*
Actions	Create, Read, Update, Delete
Context	Both in hub and QMC
Type	Read only
Conditions	resource.App.HasPrivilege("update") and !user.IsAnonymous()

UpdateAppInternals

UpdateAppInternals security rule properties

Property	Details
Name	UpdateAppInternals
Description	Everyone who has update rights to an app should also have rights to manage app internals belonging to that app
Resource filter	App.Internal_*
Actions	Create, Read, Update, Delete

Property	Details
Context	Both in hub and QMC
Type	Read only
Conditions	resource.App.HasPrivilege("update")

The security rule editor

You can create new security rules in the security rule editor.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Security rules** on the QMC start page or from the **Start** ▼ drop-down menu.
3. Click ✚ **Create new** or select an existing rule and click **Edit**.

Depending on your needs, you can either use the **Basic** section, for simple rules, or use the **Conditions** text box in the **Advanced** section to create more advanced rules.

> *When you create rules using the **Advanced** section, you need to specify the **Actions** in the **Basic** section.*

> *Some resource types, such as streams and data connections, provide the possibility to edit and create associated rules directly, without requiring access to the security rules section. Remember that when you delete the parent object, the associated rules are also deleted.*

When do I use the **Basic** section?

The **Basic** section provides an efficient way to do one of the following:

- create rules that apply to one resource type only
- create the base for more advanced rules

Creating rules for one resource type only

Using the **Create rule from template** drop-down list (in the **Identification** section) to select a resource type, will set the **Resource filter** (in the **Basic** section) to that selection. It will also automatically generate a resource filter that explicitly points out that resource type. For example, selecting **App access** will set the resource filter to App_*. This means that the QMC will only evaluate the rule for apps.

Naming resources in the Resource filter (page 567)

To add more resource types from the basic view, click the arrow to the right of the **Resource filter** text box and select the resources.

Creating a base for more advanced rules

You can use the **Basic** section to quickly create the base for a rule. For example, you can define one resource type to apply the rule to and then a set of conditions that you will manipulate with operators other than AND/OR in the **Conditions** text field in the **Advanced**section. In the **Advanced** section you can use the built-in functions provided with the editor.

Backtracking between the **Advanced** and **Basic** sections

To enable synchronization between the **Basic** and **Advanced** sections (so called backtracking), extra parentheses are added to conditions created using the **Basic** section. Similarly, a user definition with an empty condition is automatically included in the **Conditions** text field if you add a resource using the **Basic** section. However, if you create your rule using the **Advanced** section only, and do not need backtracking, you do not need to follow these conventions.

Creating security rules

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Security rules** on the QMC start page or from the **Start** ▼ drop-down menu.

3. Click ➕ **Create new** in the action bar.
   A split page is displayed, with the editing pane to the left (with all the properties) and the audit page to the right.

4. Under **Identification**, in the **Create rule from template** drop-down list, select the resource type to create a rule for.

> 💡 *In the **Basic** section, next to the **Resource filter** text box, you can click the arrow to open a popover where you can select multiple resources for the filter.*

Resource

Resource properties

Property	Security rule will be applied to
Unspecified	All resource types
App access	Apps
App object access	Objects The Objects' objectTypes, for example: sheet, story, bookmark, measure, or dimension.
Content library access	Content libraries
Data connection access	Data connections
Extension access	Extensions

Property	Security rule will be applied to
Reload task access	Reload tasks
Node access	The configuration of Qlik Sense nodes
Stream access	Streams
User access	Users
Security rule access	Security rules
User directory connector access	User directories
User synchronization task access	User synchronization tasks
Analytic connection access	Analytic connections

For example, if you create an **App access** rule and set the resource condition **Name** to *MyApp*, it means that the rule applies to the app named *MyApp*. However, setting **Name** to *MyApp** will apply the rule to all apps with names beginning with *MyApp*.

> *Changing the **Create rule from template** selection automatically clears all **Actions**, and changes the **Conditions** text box in the **Advanced** section accordingly.*

5.   Under **Identification**, give the rule a name and a description.

6.   Select **Disabled** if you do not want to enable the rule at this time.

7.   If needed, add additional resources to the resource filter. Click ▼ next to the **Resource filter** text box to open a pop-up with the available resources.

8.   In the **Basic** section, click ⊕ to add more conditions (optional).

When using multiple conditions, you can group two conditions by clicking **Group**. After the conditions have been grouped, you have the option **Ungroup**. Additional subgrouping options are **Split** and **Join**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that AND is superior to OR.

> *When using a wildcard (*), you must use the "like" operator, instead of "=".*

For a presentation of the resource conditions, see: *Available resource conditions (page 577)*.

9.   Define the resource filters, see: *Defining resource filters (page 567)*.

10.   Select the applicable **Actions** to assign access rights to the user for the resource.

Action properties

Access rule descriptions

Action	Description
Create	Create resource.
Read	Read resource.
Update	Update resource.
Delete	Delete resource.
Export	Export an app from Qlik Sense Enterprise into a qvf file.
Duplicate	Duplicate an app.
Publish	Publish a resource to a stream.
Approve	Approve an object belonging to an app.
Change owner	Change the owner of a resource.
Change role	Change user role.
Export data	Export data from an object. This includes the following actions: • "Export as image" for visualizations. • "Export as PDF" for visualizations. • "Export data" for visualizations. • "Export sheet" in the menu. • "Export story" in storytelling. *You cannot grant access to only a subset of these actions.* *You can enable export of data for anonymous users by creating a copy of the security rule ExportAppData and modifying the copy to only have* `resource.HasPrivilege("read")` *in* **Conditions**. *See Security rules included in Qlik Sense (page 535).*
Access offline	Access apps offline.

11. Select a user condition that specifies which users the rule will apply to.

> *Environment data received from external calls, for example, type of OS or browser, is not secured by the Qlik Sense system.*

User condition properties

> Any user properties contained in connected user directories will be shown in the drop-down list. This could, for example, be an email address or a department name.

Condition properties

Property	Description
@<customproperty>	A custom property associated with the user.
name	A user's full name.
userdirectory	The name of a user directory.
userid	A user's ID.
description	The description of the owner retrieved from the user directory.
email	The email addresses that are available from the connected user directories.
group	The group memberships of the owner retrieved from the user directory.
environment.browser	Security rule will be applied to the type of browser. Supported browsers: Chrome, Firefox, Safari, MSIE, or Unknown. **Example 1:** Define browser and version: Firefox 22.0 Chrome 33.0.1750.154 > If the browser information contains a slash (/), replace it with a space. **Example 2:** Use the wildcard (*) to include all versions of the browser: environment.browser = Chrome*
environment.context	Security rule will be applied only to the Qlik Sense environment that the call originates from. Available preset values: ManagementAccess or AppAccess.
environment.device	Security rule will be applied to the type of device. Available preset values: iPhone, iPad, or Default.

Property	Description
environment.ip	Security rule will be applied to an IP number. *Security rules example: Access to stream by IP address (page 607)*
environment.os	Security rule will be applied to the type of operating system. Available preset values: Windows, Linux, Mac OS X or Unknown.
environment.secureRequest	Security rule will be applied to the type of request. Available preset values: SSL True or False.

12. In the **Advanced** view, you can select where the rule should be applied from the **Context** drop-down list.
    Context properties
    Context Specifies where the rule is applied: **Both in hub and QMC**, **Only in hub**, or **Only in QMC**.

13. Click **Preview** to view the access rights that your rule will create and the users and resources that they apply to.

14. Click **Apply** to create and save the rule.
    Successfully added is displayed at the bottom of the page.

Defining resource filters

To make applying rules as efficient as possible, it is advised that you narrow the number of resources for which the rule editor will evaluate rules. This is done by applying a resource filter to the security rule. The resource filter either explicitly or implicitly defines the types of resources that the rule should be applied to.

You can narrow the number of resources by adding resources and/or user conditions. You can see which resource filters have been used in a security rule, either on the audit page, the security rules overview page, or the security rule edit page.

Naming resources in the Resource filter

The following conventions are available when defining resource filters:

- Explicit naming
  Define the resource using the resource GUID.
  For example "Stream_88ee46c6-5e9a-41a7-a66a-f5d8995454ec"

  > You can see the GUID for data connections, login access, and streams in the Security rules overview page > Resource filter provided that you have created access rights for those resources using their respective overview pages.

- Explicit type naming using wildcard (_*)
  Use the "_*" wildcard to explicitly define the type of resource to apply the rule to.
  For example, "App_*" will apply the rule to all App resources only.

- Implicit type naming using wildcard (*)
  Use wildcard to define the resource or resources.

For example, "App*" will apply the rule to all resources beginning with "App". This means that this rule will apply to apps, sheets, stories, data and objects.

Specifying a single resource

To define a single resource type simply select the resource type from the **Resource** drop-down list in the Basic view of the Security rules Edit page. The **Resources** and **Conditions** fields in the **Advanced** view will automatically be filled in.

Examples and results

Examples and results

Example	Result
Select **App** from the **Resource** drop-down list.	The following texts appear in the Advanced view: **Resource** App* **Conditions** resource.resourcetype="App" and ( )
Stream_88ee46c6-5e9a-41a7-a66a-f5d8995454ec	The rule applies to the stream with the specified GUID.

Defining multiple resource types

Type the names of the resource types you want to apply the rule to in the Resource filter field. You can write explicit resource names that include the resource GUID or use wildcards to imply all resources of a specific type.

Examples and results

Examples and results

Example	Result
App*, Streams*	The rule will apply to apps, sheets, stories, data, objects and streams.
App_*, Streams*	The rule will apply to apps and streams.
Stream_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}	The rule will apply to all existing streams using their resource ID.

Multiple permissions for complex user events

When you work with complex user events, you usually need more than one rule to account for all requirements. The following permission examples involve two or more rules, addressing different resource types, conditions, and actions. In the tables, each task is presented together with the required actions.

Import, Start user sync task, Start reload task

Import, Start user sync task, Start reload task permissions

Task	App	Data Connection	UserSyncTask	ReloadTask	UserDirectory

Import	Create and Update	Create (if there is a new data connection in the imported app)			
Start UserSyncTask			Read		Update
Start ReloadTask	Update			Read	

Duplicate, Publish, Publish and replace

Duplicate, Publish, Publish and replace permissions

Task	**App**	**Stream**	**App.Object**
Duplicate	Read and Duplicate		Read (Otherwise, the app will be duplicated, but only app objects that the user has read access on will be included in duplicated app.)
Publish	Read and Publish	Read and Publish	Read (Otherwise, the app will be published but only app objects that the user has read access on will be published.)
Publish and replace	Read, Update, and Publish	Read and Publish	Read and Update

Task details

Import

Description

To be able to import an app that contains new data connections, you need **Create** permission on the resource type DataConnection and **Create** and **Update** permissions on the resource type App.

Rule 1

Resource filter = App_*

Conditions = (Condition to select users allowed to import apps.)

Actions = Create, Update

Rule 2

Resource filter = DataConnection_*

Conditions = (Condition to select users allowed to import apps.)

Actions = Create

Start UserSyncTasks

Description

To be able to run a user sync task, you need to have **Create** permission on the resource type UserSyncTask and **Update** permission on the resource type UserDirectory.

Rule 1

Resource filter = UserSyncTask_*

Conditions = (Condition to select users and/or user sync tasks allowed to be run.)

Actions = Read

Rule 2

Resource filter = UserDirectory_*

Conditions = (Condition to select users and/or user directories allowed to be updated.)

Actions = Update

Start ReloadTasks

Description

To be able to run a reload task, you need to have **Read** permission on the resource type ReloadTask and **Update** permission on the resource type App.

Rule 1

Resource filter = App_*

Conditions = (Condition to select users and/or apps allowed to be reloaded.)

Actions = Update

Rule 2

Resource filter = ReloadTask_*

Conditions = (Condition to select users and/or reload tasks allowed to be run.)

Actions = Read

Duplicate

Description

To be able to duplicate an app, you need to have **Read** permissions on the resource types App and App.Objects (the objects that are to be part of the duplicated app) and permission to **Duplicate** an app.

Rule 1

Resource filter = App_*

Conditions = (Condition to select users allowed to duplicate apps.)

Actions = Create and Read

Rule 2

Resource filter = App.Object_*

Conditions = (Condition to select users and/or apps allowed to be duplicated.)

Actions = Read

Publish

Description

To be able to publish an app, you need **Read** and **Publish** permissions on the app, **Read** and **Publish** permissions on the resource type Stream, and **Read** permission on the resource type App.Objects (the objects that will be included in the published app).

Rule 1

Resource filter = App_*, Stream_*

Conditions = (Condition to select users allowed to publish apps to the stream.)

Actions = Read, Publish

Rule 2

Resource filter = App.Object_*

Conditions = (Condition to select users and/or App.Objects that will be included in the published app.)

Actions = Read

Publish and replace app

Description

To be able to publish and replace an app, you need **Read**, **Update**, and **Publish** permissions on the resource type App, **Read** and **Publish** permissions on the resource type Stream, and **Read** and **Update** permissions on the resource type App.Objects (the objects that will be included in the published app).

Rule 1

Resource filter = App_*

Conditions = (Condition to select users allowed to publish and replace the app.)

Actions = Read, Publish, Update

Rule 2

Resource filter = Stream_*

Conditions = (Condition to select users and/or streams allowed to publish to.)

Actions = Read, Publish

Rule 3

Resource filter = App.Object_*

Conditions = (Condition to select users and/or App.Objects that will be in the published app.)

Actions = Read, Update

Available resource filters

The following tables list the resource objects and the resource filters that can be used to target them.

> ℹ️ *The lists are not complete, they only display the most common examples of resource filters.*

App related resources

App filters

Resource filter	Filter will target
App	The application
App.Content	The content stored in the app-specific content library
App.DataSegment	A representation of the data which will be loaded and used by the application
App.Internal	Parameters internal to and required by the application
App.Object	All App.Object resources, such as sheets, stories, script, dimensions, measures, master objects, snapshots, and bookmarks
appprops	Visual styling for the theme and sheet title.
ColorMap	Mapping between dimension value and color.
Extension	The extensions installed in Qlik Sense
IAChat	The Insight Advisor Chat
WebExtensionLibrary	The library of web extensions
Widgets	The widgets installed in Qlik Sense

Task resources

Task filters

Resource filter	Filter will target
CompositeEvent	Task triggers in the scheduler
ExecutionResult	Details of executions of tasks
ExecutionSession	Details of active sessions for tasks
ExternalProgramTask	Tasks that trigger a third-party program
ReloadTask	Tasks that perform reload on apps. This also applies to distribution tasks.
SchemaEvent	Details for when a scheduled task will run
UserSyncTask	Tasks that sync users from an external user directory

ContentLibrary related resources

ContentLibrary filters

Resource filter	Filter will target
ContentLibrary	Content libraries
FileReference	Representation of files stored on disk used by the binary sync to sync files between nodes
SharedContent	Links to QlikView documents, Qlik NPrinting generated reports
StaticContentReference	Links to files in a content library
TempContent	Content library for temporary content, such as files from exports

Hub section resources

The following filter can be used to disable user access to the hub.

Hub section filters

Resource filter	Filter will target
HubSection_ Home	Grants access to open the hub and view the resources you have access to. By default, on.
	*Disabling user access to the hub only removes the **Open hub** from the Navigation menu. It is still possible to access the hub by editing the URL.*
HubSection_ Task	Grants access to the task hub section. By default, on.

QMC section resources

The following filters are used to grant access to the different QMC sections. A user with access to a QMC section can open that section, but will only see objects according to the user's access rights.

To get an overview of the available resources, you can log in to the QMC as RootAdmin and check the network traffic.

QMC section filters

Resource filter	Filter will target
QmcSection_AnalyticConnection	The QmcSection_AnalyticConnection resource
QmcSection_App	The QmcSection_App resource
QmcSection_App.Object	The QmcSection_App.Object resource

Resource filter	Filter will target
QmcSection_Audit	The QmcSection_Audit resource
QmcSection_Certificates	The QmcSection_Certificate resource
QmcSection_Certificates.Export	The QmcSection_Certificates.Export resource
QmcSection_CompositeEvent	The QmcSection_CompositeEvent resource
QmcSection_ContentLibrary	The QmcSection_ContentLibrary resource
QmcSection_CustomPropertyDefinition	The QmcSection_CustomPropertyDefinition resource
QmcSection_DataConnection	The QmcSection_DataConnection resource
QmcSection_DistributionPolicy	The QmcSection_DistributionPolicy resource
QmcSection_EngineService	The QmcSection_EngineService resource
QmcSection_Event	The QmcSection_Event resource
QmcSection_Extension	The QmcSection_Extension resource
QmcSection_License	The QmcSection_License resource
QmcSection_Licenses	The QmcSection_Licenses resource
QmcSection_License.AnalyzerAccessRule	The QmcSection_License.AnalyzerAccessRule resource
QmcSection_License.AnalyzerAccessType	The QmcSection_License.AnalyzerAccessType resource
QmcSection_License.ApplicationAccessType	The QmcSection_License.ApplicationAccessType resource
QmcSection_License.LoginAccessType	The QmcSection_License.LoginAccessType resource
QmcSection_License.ProfessionalAccessRule	The QmcSection_License.ProfessionalAccessRule resource
QmcSection_License.ProfessionalAccessType	The QmcSection_License.ProfessionalAccessType resource
QmcSection_License.UserAccessRule	The QmcSection_License.UserAccessRule resource
QmcSection_License.UserAccessType	The QmcSection_License.UserAccessType resource
QmcSection_LoadBalancingRule	The QmcSection_LoadBalancingRule resource
QmcSection_OdagService	The QmcSection_OdagService resource
QmcSection_PrintingService	The QmcSection_PrintingService resource
QmcSection_ProxyService	The QmcSection_ProxyService resource
QmcSection_ReloadTask	The QmcSection_ReloadTask resource
QmcSection_RepositoryService	The QmcSection_RepositoryService resource
QmcSection_SchedulerService	The QmcSection_SchedulerService resource
QmcSection_SchemaEvent	The QmcSection_SchemaEvent resource
QmcSection_ServerNodeConfiguration	The QmcSection_ServerNodeConfiguration resource
QmcSection_ServiceCluster	The QmcSection_ServiceCluster resource

Resource filter	Filter will target
QmcSection_Stream	The QmcSection_Stream resource
QmcSection_SyncRule	The QmcSection_SyncRule resource
QmcSection_SystemRule	The QmcSection_SystemRule resource
QmcSection_Tag	The QmcSection_Tag resource
QmcSection_Task	The QmcSection_Task resource
QmcSection_Token	The QmcSection_Token resource
QmcSection_User	The QmcSection_User resource
QmcSection_UserDirectory	The QmcSection_UserDirectory resource
QmcSection_UserSyncTask	The QmcSection_UserSyncTask resource
QmcSection_VirtualProxyConfig	The QmcSection_VirtualProxyConfig resource

License related resources

License filters

Resource filter	Filter will target
License	The actual license entity Qlik Sense .
License.AnalyzerAccessGroup	Resource for rules used for automatically assigning analyzer access types.
License.AnalyzerAccessType	Analyzer access type. CRUD for manually allocating access for a named user.
License.AnalyzerAccessUsage	Type to keep track of analyzer access type usage. Should not be used in resource filters.
License.LoginAccessType	Login access type. CRUD for allocating tokens for login (time restricted) access and setting up the associated rule.
License.LoginAccessUsage	Type to keep track of login access type usage. Should not be used in resource filters.
License.ProfessionalAccessGroup	Resource for rules used for automatically assigning professional access types.
License.ProfessionalAccessType	Professional access type. CRUD for manually allocating access for a named user.
License.ProfessionalAccessUsage	Type to keep track of professional access type usage. Should not be used in resource filters.
License.UserAccessGroup	Resource for rules used for automatically assigning user access types.

Resource filter	Filter will target
License.UserAccessType	User access type. CRUD for manually allocating tokens for user (named) access.
License.UserAccessUsage	Type to keep track of user access type usage. Should not be used in resource filters.
TermsAcceptance	Resource for accessing the terms and conditions page in the QMC.

Node or service related resources

These filters refer to individual entries in the associated sections of the QMC.

Node/service filters

Resource filter	Filter will target
Certificates	The Certificates resource
Deployment	The Deployment resource
EngineService	The EngineService resource
IdentityProviderSettings	The IdentityProviderSettings resource
LoadbalancingSelectList	The LoadbalancingSelectList resource
OdagService	The OdagService resource
PrintingService	The PrintingService resource
ProxyService	The ProxyService resource
RepositoryService	The RepositoryService resource
SchedulerService	The SchedulerService resource
ServerNodeConfiguration	The ServerNodeConfiguration resource
ServiceCluster	The ServiceCluster resource
ServiceStatus	The ServiceStatus resource
VirtualProxyConfig	The VirtualProxyConfig resource

Other resources

These filters refer to individual entries in the associated sections of the QMC.

Other filters

Resource filter	Filter will target
AnalyticConnection	The AnalyticConnection resource
CustomPropertyDefinition	The CustomPropertyDefinition resource
DataConnection	The DataConnection resource

Resource filter	Filter will target
FileExtension	The FileExtension resource
FileExtensionWhiteList	The FileExtensionWhiteList resource
OdagLink	The OdagLink resource
OdagLinkUsage	The OdagLinkUsage resource
OdagRequest	The OdagRequest resource
Stream	The Stream resource
SystemRule	The SystemRule resource
Tag	The Tag resource
User	The User resource
UserDirectory	The UserDirectory resource

Available resource conditions

The following tables list the available resource conditions.

> The lists are not complete, they only display the most common examples of resource conditions.

General

General properties descriptions and examples

Property	Description	Example
resource.@<customproperty>	Custom property associated with the resource. In the examples, @Department is the custom property name.	`resource.@Department = Finance.` `resource.@Department = user.userDirectory`
resource.name	Name of the resource.	`resource.name like "*US*"`. A string containing "US" will match the condition.
resource.id	ID of the resource.	`resource.id=5dd0dc16-96fd-4bd0-9a84-62721f0db427` The resource in this case is an app.

Resource user and owner of an object

Resource user and owner of an object properties

Property	Description	Example
user.email owner.email	Email of the user. Email of the owner.	user.email="user@domain.com" owner.email="owner@domain.com"
user.environment.browser	Session based attribute for browser. Use the "like" operator instead of the "=" operator, because the browser data is sent in a format that includes version and other details, for example: "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0". You can use the "=" operator instead, but then you need to specify the whole value.	user.environment.browser like "*Firefox*"
user.environment.context	Session based attribute for context. (The QMC has a separate setting for context.)	user.environment.context="Management Access"
user.environment.device	Session based attribute for device.	user.environment.device="iPhone"
user.environment.ip	Session based attribute for IP address.	*Security rules example: Access to stream by IP address (page 607)*
user.environment.os	Session based attribute for operating system.	user.environment.os like "Windows*"
user.environment.secureRequest	Session based attribute for secureRequest. Value true - if SSL is used - otherwise false.	user.environment.secureRequest="true"

Property	Description	Example
user.environment.[SAML attribute]	Session based attribute that is supplied at the time of authentication, such as user.environment.group.	`user.environment.xxx="<attribute name>"`
user.environment.[ticket attribute]	Session based attribute that is supplied at the time of authentication, such as user.environment.group.	`user.environment.xxx="<attribute name>"`
user.environment.[session attribute]	Session based attribute that is supplied at the time of authentication, such as user.environment.group.	`user.environment.xxx="<attribute name>"`
user.group owner.group	Group that the user belongs to. Group that the owner belongs to.	`user.group=resource.app.stream.@AdminGroup` `owner.group=@Developers`
user.userdirectory owner.userdirectory	User directory that the user belongs to. User directory that the owner belongs to.	`user.userdirectory="Employees"` `owner.userdirectory="Employees"`
user.userId owner.userId	ID of the user. ID of the owner.	`user.userId="<userID>"` `owner.userId="<ownerID>"`
user.roles owner.roles	Roles of the user. Roles of the owner.	`user.roles="AuditAdmin"` `owner.roles="SystemAdmin"`

> *To use the user.environment conditions, you must enable **Extended security environment** in the virtual proxy.*
>
> *See: Virtual proxies (page 158)*

Resource app

Resource app properties

Property	Description	Example
stream.name	Name of the stream that the app is published to.	`stream.name="Finance"`

Resource app.object

Resource app.object properties

Property	Description	Example
app.stream.name	Name of the stream that the app object is published to.	`app.stream.name="Test"`
app.name	Name of the app that the object is part of.	`app.name="Q3_Report"`
approved	Indicator of whether the object was part of the original app when the app was published. Values: true or false.	`resource.approved="true"`
description	Object description.	`resource.description="old"`
objectType	Possible values: • app_appscript • bookmark • dimension • embeddedsnapshot • genericvariableentry • hiddenbookmark • loadmodel • masterobject • measure • odagapplink • sheet • snapshot • story	`resource.objectType="sheet"`
published	Indicator of whether the object is published. Values: true or false.	`resource.published="false"`

Resource related to apps such as app.content and reloadtask

Resource related to apps such as app.content and reloadtask properties

Property	Description	Example
app.stream.name	Name of the stream that the app is published to.	`app.stream.name="Test"`
app.name	Name of the app.	`app.name="Q3_Report"`

Resource DataConnection

Resource DataConnection properties

Property	Description	Example
Type	Type of data connection. Possible values: • OLEDB • ODBC • Folder • Internet • Custom (for all custom connectors)	`resource.type!="folder"`

Resource SystemRule

Resource SystemRule properties

Property	Description	Example
Category	System rule category. Possible values: • Security • License • Sync	`resource.category="license"`
ResourceFilter	Resource filter of the rule.	`resource.resourcefilter matches "DataConnection_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}"`
RuleContext	Context for the rule. Possible values: • BothQlikSenseAndQMC • QlikSenseOnly • QMCOnly	`resource.rulecontext="BothQlikSenseAndQMC"`
Type	Type of rule. Possible values: • Default • Read only • Custom	`resource.type!="custom"`

Resource ContentLibrary

Resource ContentLibrary properties

Property	Description	Example
Type	Possible values: • media	resource.type="media"

Resource ServerNodeConfiguration

Resource ServerNodeConfiguration properties

Property	Description	Example
IsCentral	Central node indicator, values: true or false.	resource.iscentral="true"
nodePurpose	Node purpose: development or production.	resource.nodepurpose="production"

Resource UserDirectory

Resource UserDirectory properties

Property	Description	Example
userDirectoryName	Name of the user directory.	resource.userDirectoryname="Employees"

Resource UserSyncTask

Resource UserSyncTask properties

Property	Description	Example
userDirectory.name	Name of the user directory connector.	resource.userDirectory.name="Employees"
userDirectory.userDirectoryName	Name of the user directory.	userDirectory.userdirectoryname="Employees"

Resource Widget

Resource Widget properties

Property	Description	Example
library.name	Name of the library that the widget belongs to.	resource.library.name="Dev"

> For some resources (for example, environment.browser), you need to select **Extended security environment** in the proxy settings.

Operators and functions for conditions

The QMC includes several predefined functions that can be used to return property values from targeted resources.

Logical operator precedence

When more than one logical operator is used in a condition, NOT is evaluated first, then AND, and finally OR. Using parentheses, even when they are not required, can improve the readability of conditions and reduce the risk of making mistakes because of operator precedence.

Example:

How is A OR B AND C interpreted by the Qlik Sense security rules?

It is interpreted as A OR (B AND C).

AND

This operator compares two expressions and returns True only if both evaluate to True.

Syntax:
```
(EXPRESSION) && (EXPRESSION)
(EXPRESSION) and (EXPRESSION)
```

Examples and results:

AND operator examples and results

Example	Result
`(resource.@org = "UK") && (user.name = "John Doe")`	Evaluates to True only if both expressions are True.
`(resource.@org = "UK") and (user.name = "John Doe")`	Same as previous, but using "and" notation instead of "&&".

EQUAL

This operator is case insensitive and returns True if the compared expressions are equal. If a list is used, only one value needs to match.

Syntax:
```
(EXPRESSION) = (EXPRESSION)
```

Examples and results:

EQUAL operator examples and results

Example	Result
Given that @org is "uk" in the access request.	`resource.@org = "UK"` evaluates to True because the operator is case insensitive.
Given that @org is "UK" in the access request.	`resource.@org = "UK"` evaluates to True.
Given that @org is "United Kingdom" in the access request.	`resource.@org = "UK"` evaluates to False.
Given that resource@group is "Sales" in the access request, and user.group contains Sales.	`resource.@group = "Sales"` evaluates to True because user.group contains Sales.

LIKE

The security rules support the regular expression operator "like". This operator is case insensitive.

Syntax:
```
(EXPRESSION) like (EXPRESSION)
```

Examples and results:

LIKE operator example and result

Example	Result
`resource.name like "mya*"`	Evaluates all resources with names beginning with "*mya*" to True, irrespective of case. *The example refers to how the string will look in the **Conditions** box, in the **Advanced** section. Do not use quotation marks in the **Basic** section, because the quotation marks will be interpreted as part of the search string, which they most likely should not be. In the Basic section the search string should look as follows: mya*.*

If possible, avoid using the like operator, as it can have negative impact on rule evaluation performance.

NOT

This operator inverts the Boolean value of an expression and returns True if the expression is False and returns False if the expression is True.

Syntax:
```
!(EXPRESSION)
```

Examples and results:

NOT operator examples and results

Example	Result
Given that @org is "UK" in the access request	`!(resource.@org = "UK")` evaluates to False.
Given that @org is "US" in the access request	`!(resource.@org = "UK")` evaluates to True.

MATCHES

The security rules editor supports the regular expression operator "matches". This operator is case insensitive and returns results that match your expression, irrespective of case. Regex start and end anchors are implicitly added.

Syntax:

```
(EXPRESSION) matches (EXPRESSION)
```

Examples and results:

MATCHES operator examples and results

Example	Result
`resource.name matches ".*yAp.*"`	Evaluates all resources with names containing "*yap*" to True, irrespective of case.
`resource.resourcefilter matches "Stream_\\w{8}-\\w{4}-\\w{4}-\\w{4}-\\w{12}"`	Evaluates to True if the access request resource filter has the correct format.

NOT EQUAL

This operator is case insensitive and returns True if the compared expressions are not equal. If a list is used, only one value needs not to match.

Syntax:

```
(EXPRESSION) != (EXPRESSION)
```

Examples and results:

NOT EQUAL operator examples and results

Example	Result
Given that @org is "uk" in the access request	`resource.@org != "UK"` evaluates to False because the operator is case insensitive.
Given that @org is "UK"in the access request	`resource.@org != "UK"` evaluates to False.

Example	Result
Given that @org is "United Kingdom"in the access request	`resource.@org != "UK"` evaluates to True.
Given that resource@group is "Sales" in the access request, and user.group contains Sales.	`resource.@group != "Sales"` evaluates to False because user.group contains Sales.

OR

This operator compares two expressions and returns True if one or both evaluate to True.

Syntax:
```
(EXPRESSION) || (EXPRESSION)
(EXPRESSION) or (EXPRESSION)
```

Examples and results:

OR operator examples and results

Example	Result
`(resource.@org = "UK") || (resource.@org = "US")`	Evaluates to True only if any of the expressions are True.
`(resource.@org = "UK") or (resource.@org = "US")`	Same as above but using "or" notation instead of "||".

STRICT EQUAL

This operator is case sensitive and returns True if the compared expressions are exactly equal. The full list does not have to match when a value used in an expression exists in a list.

Syntax:
```
(EXPRESSION) == (EXPRESSION)
```

Examples and results:

STRICT EQUAL operator examples and results

Example	Result
Given that @org is "united States" in the access request	`resource.@org == "United States"` evaluates to False because the operator is case sensitive.
Given that @org is "United States" in the access request	`resource.@org == "United States"` evaluates to True.
Given that @org is "US"in the access request	`resource.@org == "United States"` evaluates to False.

STRICT NOT EQUAL

This operator is case sensitive and returns True if the compared expressions are exactly not equal. The full list does not have to match when a value used in an expression exists in a list.

Syntax:

```
(EXPRESSION) !== (EXPRESSION)
```

Examples and results:

STRICT NOT EQUAL operator examples and results

Example	Result
Given that @org is "united states" in the access request	`resource.org !== "United States"` evaluates to True because the operator is case sensitive.
Given that @org is "United States" in the access request	`resource.org !== "United States"` evaluates to False.
Given that @org is "US" in the access request	`resource.org !== "United States"` evaluates to True.

HasPrivilege

Boolean function for resource conditions that returns True if the user making the request has the specified access right for the targeted resource or resources. Otherwise returns False.

Syntax:

```
resource.HasPrivilege("action")
```

Properties:

Syntax properties

Property	Description
action	MANDATORY. The action that you want to evaluate access right for.

Examples and results

Examples and results

Example	Result

Resource filter: *
 	
 Conditions:
 `resource.resourcetype = "App"`
 	
 `and`
 `resource.Stream.HasPrivilege`
 `("read")`
 	
 Action: read
	The user will be given read access to the app provided that the user has read privileges to the stream that the resource is published to.

IsAnonymous

Boolean function for user conditions that returns True if the user requesting access has logged in as anonymous. Otherwise returns False.

Syntax:

```
user.IsAnonymous()
```

Examples and results

Examples and results

Example	Result
Resource filter: `Stream_*` **Conditions:** `user.IsAnonymous()` **Action:** `read`	Anonymous users are allowed to read streams.

Resource filter: `Stream_*`
 	
Conditions:
`!user.IsAnonymous()`
 	
Action: `read,`
`publish`
	All users that are not anonymous (notice the NOT operator, !, in front of the condition) are allowed to read and publish streams. Anonymous users will have no access to streams.

Empty

Boolean function for resource conditions that returns True if the specified resource has no connections (that is, has no value). Otherwise returns False.

Syntax:

```
resource.resourcetype.Empty()
```

Examples and results

Examples and results

Example	Result
Resource filter: `App_*` **Conditions:** `resource.stream.Empty()` **Action:** `update`	This rule lets the user update an app, provided that the app is not connected (published) to a stream.

Example	Result
Resource filter: `App.Sheet_*` **Conditions:** `resource.app.stream.Empty()` **Action:** `update`	This rule lets the user update sheets, provided that the app that the sheet belongs to is not published to a stream.

IsOwned

Boolean function **for resource conditions** that returns True if the specified resource has an owner. Otherwise returns False.

Syntax:

```
resource.IsOwned()
```

Examples and results

Examples and results

Example	Result
Resource filter: `*` **Conditions:** `resource.IsOwned() and resource.owner = user` **Action:** `read, export, publish`	The owner of a resource should be able to read, export and publish his / her resources. Here the conditions specify that the resource must be owned and the owner must be the requesting user for the rule to apply. *This is the definition of the OwnerNonModificationActions rule, a custom rule supplied with the QMC. Complements the Owner rule that provides resource owners with all actions provided that the resource is not published to a stream.*

Editing security rules

You can edit a security rule that you have update rights to. If you edit a default rule, that is, a rule that is supplied with Qlik Sense, the rule type definition changes from **Default** to **Custom**. Keep in mind that changing a default rule, or adding a new rule that affects the default rules, may cause unexpected behavior in Qlik Sense. Use the rule preview feature to check rule behavior before implementing changes to default rules. Remember that only read only and default rules are automatically updated when you upgrade to a new Qlik Sense version.

It is not recommended to create rules that allow users to edit published apps in streams.

Some resource types, such as streams and data connections, provide the possibility to edit and create associated rules directly, without requiring access to the security rules section.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Security rules** on the QMC start page or from the **Start** ▼ drop-down menu.

3. Select the rule you want to edit.

4. Click **Edit** in the action bar.
   A split page is displayed, with the editing pane to the left (with all the properties) and the audit page to the right.

   > *In the **Basic** section, next to the **Resource filter** text box, you can click the arrow to open a popover where you can select multiple resources for the filter.*

5. Click **Preview** to view the access rights of your rule in the currently defined audit grid.

6. Click **Apply** to save the edited rule.
   Successfully updated is displayed at the bottom of the page.

> *Updates to the security rules will not immediately take effect in a client if the client has more than one tab open. The user must then log out and log in again. When only one tab is open, it is sufficient to do a refresh.*

Deleting security rules

You can delete security rules that you have delete rights to.

> *If a resource is deleted, all load balancing rules and security rules associated with that resource are deleted automatically.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Security rules** on the QMC start page or from the **Start** ▼ drop-down menu.

3. Select the rules that you want to delete.

4. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.

5. Click **OK**.

Security rules evaluation

Each time a user requests access to a resource, Qlik Sense evaluates the request against the security rules in the Qlik Sense system. If at least one rule evaluates to True then Qlik Sense will provide the user with access according to the conditions and actions described in the security rule. If no rules evaluate to True then the user will be denied access. The fact that Qlik Sense security rules are property-based makes Qlik Sense very scalable as you can build rules based on properties that apply to groups of users.

This inclusive method of security rule evaluation means that you should keep the following principles in mind when designing security for resources in Qlik Sense:

- Access is provided if at least one rule for the resource in question includes access rights for the user who is requesting access.
- You do not need to write rules that explicitly exclude users.
- Use roles, user types and group properties as far as possible when designing rules.

The rule preview and auditing tools can then be used to verify and validate that your rules work in practice.

The evaluation flow

The following image displays how security rules are evaluated when a user accesses the hub in Qlik Sense. For a detailed description of the steps in the rule evaluation, and how rules can affect performance, see read the blog post Security Rules and Performance in Qlik Sense. There you can also learn about cache invalidation.
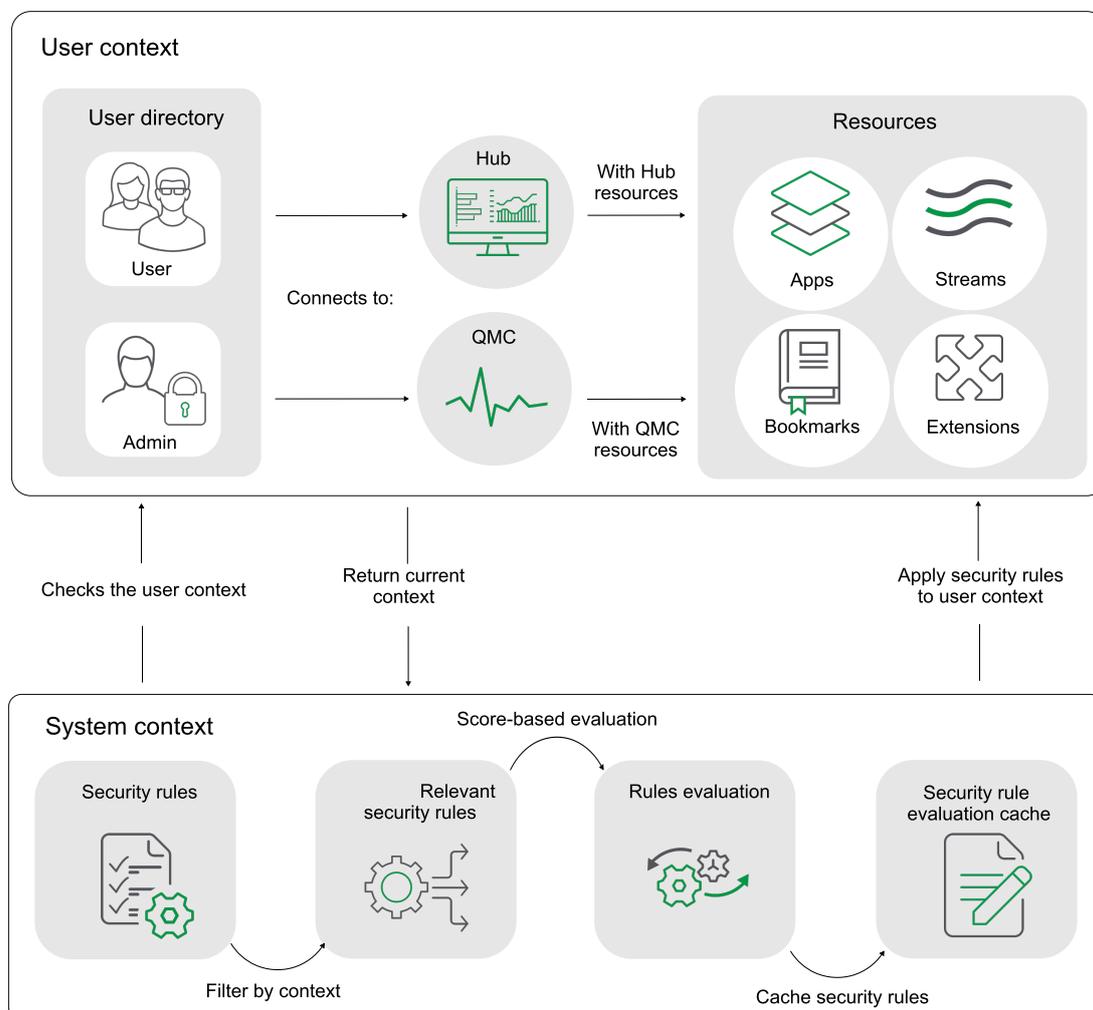
Security rules examples

The following are a few common examples of security rule creation.

Example 1: Only one rule required to provide user access

Your Finance department publishes financial results to a stream called *Quarterly results*. To begin with you only want users from the finance department to be able to read from this stream. In this case you need only create a security rule for finance department users that provides the Read action for the *Quarterly results* stream.

The easiest way to create this security rule is to go to the **Streams** overview in the QMC, select the stream from the list, click **Edit** and then add a user condition for **Read** to the stream in the **System rules** under **Associated items**. You can either edit an existing rule, or create a new rule with the user condition for **Read**. As a condition you would preferably use either group property from the directory service. If available, these properties are shown in the drop-down menus in the **Basic** view. If the directory service does not include an appropriate group property you can create a custom property in the QMC, for example, the custom property **Departments** with the value **Finance**.

Example 2: More than one rule applies to the user

In the *Quarterly results* example we created a rule (Rule 1) that allows users belonging to Active Directory group Finance to read the Quarterly results stream. Assume that another rule (Rule 2) giving users belonging to the Active Directory (AD) group Management read access to the Quarterly results steam.

Finally, assume that the Sales director belongs to both Active Directory groups Sales and Management.

Security rules example 2

-	Rule 1	Rule 2
Allow users to	Read	Read
On resource	Quarterly results stream	Quarterly results stream
Provided that	group=Finance	group=Management
Evaluates to	FALSE	True
Resulting access for Sales director	Provide read access	

Example 3: More than one rule with different access rights

In the Quarterly results example we created a rule (Rule 1) that allows users belonging to Active Directory group Finance to read the Quarterly results stream. Assume that another rule (Rule 2) giving users belonging to the Active Directory (AD) group Management read access to the Quarterly results stream. Finally, Rule 3 allows Management users to update apps in streams that they have read access to.

Assume that the Sales director belongs to both Active Directory groups Sales and Management.

Security rules example 3

-	Rule 1	Rule 2	Rule 3
Allow users to	Read	Read	Update

-	Rule 1	Rule 2	Rule 3
On resource	Quarterly results stream	Quarterly results stream	All apps and sheets if user has read access to stream
Provided that	group=Finance	group=Management	group=Management
Evaluates to	FALSE	True	True
Resulting access for Sales director	Provide read and update access		

Example 4: Out-of-the-box Qlik Sense rules

The Finance office in the UK has published an app to the Quarterly results stream called UK quarterly report. They want Finance users in the UK office to be the only users with read access to that app. For this purpose the UK administrator creates Rule 3 that explicitly states that only users belonging to AD group Finance and UK office have read access. Also assume that Rule 2 from Example 1 and the out-of-the-box Stream rule are also in place.

In this case Finance in the UK may have assumed that the Sales director would not be able to read the UK quarterly report app. However, this is not True since Rule 2 allows management to read the Quarterly reports stream and the Stream rule allows all users that have read access to the Quarterly reports stream to read all apps on that stream.

Security rules example 4

-	Rule 2	Rule 3	Stream rule
Allow users to	Read	Read	Read
On resource	Quarterly reports stream	UK quarterly report app published on Quarterly reports stream	All apps and sheets in a stream
Provided that	group=Management	group=Finance AND office=UK	User has read access to the stream
Evaluates to	True	FALSE	True
Resulting access for Sales director	Provide read access		

Overlapping rules

As you develop rules, you will eventually have rules that overlap. By this we mean that conditions in two or more rules target the same user or users. If rules overlap, the rule that provides access will prevail.

> *Qlik Sense evaluates each rule in turn. If one rule provides access of a certain type, Qlik Sense provides that access.*

If we consider two rules that overlap the following types of overlap can typically occur:

- Identical
  Both rules provide read access to the user. In this case read access will be provided.

- Complementary
  One rule provides read and the other provides update. In this case, the user is provided with both read and update access.

You can view which user security rules apply to a resource using the audit page in the QMC.

Audit (page 72)

You can also preview the effects of a rule.

Editing security rules (page 589)

Example 1:

In the example *One property-value pair in conditions: (page 516)* we created a rule (Rule 1) that allows users belonging to Active Directory group Finance to read the Quarterly results stream. Assume that another rule (Rule 2) giving users belonging to the Active Directory (AD) group Management read access to the Quarterly results steam.

Finally, assume that the Sales director belongs to both Active Directory groups Sales and Management.

Rule results

Result	Rule 1	Rule 2
Allow users to	Read	Read
On resource	Quarterly reports stream	Quarterly reports stream
Provided that	group=Finance	group=Management
Evaluates to	FALSE	TRUE
Resulting access for Sales director	Provide read access	Provide read access

Example 2:

The Finance office in the UK have published an app to the Quarterly reports stream called UK quarterly outlook. They want Finance users in the UK office to be the only users with read access to that app. For this purpose the UK administrator creates Rule 3 that explicitly states that only users belonging to AD group Finance and UK office have read access. Also assume that Rule 2 from Example 1 and the out-of-the-box Stream rule are also in place.

In this case Finance in the UK may have assumed that the Sales director would not be able to read the UK quarterly outlook app. However, this is not true since Rule 2 allows management to read the Quarterly reports stream and the Stream rule allows all users that have read access to a stream to read all apps on that stream.

Rule results

Result	Rule 3	Rule 2	Stream rule
Allow users to	Read	Read	Read
On resource	UK quarterly report published on Quarterly reports stream	Quarterly reports stream	All apps and sheets in a stream
Provided that	group=Finance AND office=UK	group=Management	User has read access to the stream
Evaluates to	FALSE	TRUE	TRUE
Resulting access for Sales director	Provide read access	Provide read access	Provide read access

Security rules examples

The following examples describe using and writing security rules for a number of scenarios.

Security rules example: Creating custom admin roles

Qlik Sense comes with six default admin roles. If you want to create a custom admin role, you need some security rules. In this example, you will create a custom admin role for the management of streams, apps, app objects, and reload tasks.

The following security rules are needed:

- A rule that provides access to the required resources.
- A QMC section access rule, providing the admin with access to the required sections in the QMC.

By creating a generic admin role, rather than creating security rules for a certain user, you make the rules reusable. The custom admin role can be assigned to several users, without changing any of the security rules.

Resource rule

By creating a resource rule, you can provide one or more users with the same admin access rights.

Do the following:

1. Select **Security rules** and click ✚ **Create new**.

2. In the **Name** field, type *CustomAdmin*.

3. Set the resource filter to filter on streams, apps, app objects (such as sheets and stories), and tasks.
   In the **Basic** section, fill in the **Resource filter** field as follows:
   `Stream_*, App_*, App.Object_*, ReloadTask_*`

4. Set the actions that the rule should provide for the specified resources.
   In the **Basic** section, select the **Actions** as follows:
   `Create, Read, Update, Delete, Export, Publish, Export data`

5. Set the conditions to specify the user role.
   In the **Advanced** section, fill in the **Conditions** field as follows:
   `user.roles = "CustomAdmin"`

6. Click **Apply**.

7. Assign the role to the user who will be the custom administrator.
   Go to QMC start page > **Users**.

8. Select the user and click **Edit**.

9. Click ✚ under **Admin roles** and select `CustomAdmin`.

10. Click **Apply**.

This table summarizes the security rule fields for the user role CustomAdmin.

Security rule fields

Field	Code	Comments
Resource filter	`Stream_*, App_*, App.Object_*, ReloadTask_*`	Filters on resource types `Stream`, `App`, `AppObjects`, and `ReloadTasks`. 💡 *Alternatively, you could write* `App*` *instead of* `App_*`, `App.Object_*`, *because the wildcard (*), without the underscore (_), targets all resource types beginning with* `App`.

Field	Code	Comments
Actions	`Create, Read, Update, Delete, Export, Publish, Export data`	These actions will be granted provided the conditions are met.
Conditions	`user.roles = "CustomAdmin"`	The user role `CustomAdmin` will be available in **Users** > **Roles**.

QMC section access

To manage the content, the admin must have section access to the relevant sections in the QMC.

Do the following:

1. Select **Security rules** and click ➕ **Create new**.
2. In the **Name** field, type *QMC_Sections_CustomAdmin*.
3. Set the resource filter to filter on the QMC sections that the *CustomAdmin* needs access to.
   In the **Basic** section, fill in the **Resource filter** field as follows:
   `License_*,QmcSection_Stream,QmcSection_App,QmcSection_App.Object,QmcSection_Task`
4. Set the actions that the rule should provide for the specified resources.
   In the **Basic** section, select the **Actions** as follows:
   `Read`
5. Set the conditions to specify the user role.
   In the **Advanced** section, fill in the **Conditions** field as follows:
   `user.roles = "CustomAdmin"`
6. Set the context for the rule.
   In the **Advanced** section, in the **Context** field, select **Only in QMC**.
7. Click **Apply**.

This table summarizes the security rule for *QMC_Sections_CustomAdmin*.

Security rule properties

Field	Code	Comments
Resource filter	`License_*,QmcSection_Stream,QmcSection_App,QmcSection_App.Object,QmcSection_Task`	The QMC section access rule only grants read access to a QMC section.
Actions	`Read`	The action is granted provided that the conditions are met.
Conditions	`user.roles = "CustomAdmin"`	Users with the admin role `CustomAdmin` are granted access to these sections.
Context	`Only in QMC`	This rule only applies to the QMC.

Security rules example: Creating QMC organizational admin roles

In this example, you organize the administration of access rights for your departments by doing the following:

- Creating an administrator for each department
- Providing each administrator with full access rights to content created by users belonging to that department

To create the organizational admin roles you need to create new security rules and you will use custom properties to connect the roles to the apps.

Security rules

Security rule	The result of the rule
DepartmentAdminQmcSections	Controls which sections in the QMC that are to be visible to the administrator.
DepartmentAdminApp	Controls which resources the administrator is authorized to manage.

Procedure

Do the following:

1. Create a new custom property:
   a. Name the property *Department*.
   b. Under **Resource types**, select **Apps**, **Reload tasks**, and **Users**.
   c. Click **Create new** and enter the value *Finance*.
   d. Click outside the **Values** area.
   e. Click **Create new** and enter the value *Sales*.
   f. Click **Apply**.
2. Create the new security rules (*DepartmentAdminQmcSections* and *DepartmentAdminApp*):
   a. Select **Security rules** and click ➕ **Create new**.
   b. In the **Advanced** and **Basic** sections, fill in the fields **Resource filter**, **Conditions**, **Actions** and **Context** as per *Security rule code (page 599)*
3. Apply the role to the admin users for the departments (repeat this step for all the administrators you want to add):
   a. Select **Users**, select a user and click **Edit**.
   b. Click ➕ under **Admin roles** and select *DepartmentAdmin*.
   c. At **Custom properties** you select value (*Sales* or *Finance*) for your custom property *Department*.
   d. Click **Apply**.
4. Select the apps that the organizational admin user should be able to administer:
   a. Go to the QMC start page > **Apps**, select apps and click **Edit**.
   b. Select value (*Sales* or *Finance*) for your custom property *Department*.
   c. Click **Apply**.

You have now created and assigned the organizational admin role.

Security rule code

The following is the security rule code for this example, with explanatory comments:

Security rule code for "DepartmentAdminQmcSections"

Security rule code information for DepartmentAdminQmcSections

Field	Code	Comments
Resource filter	`QmcSection_Stream,QmcSection_App,QmcSection_App.Sheet, QmcSection_App.Story,QmcSection_Tag, QmcSection_Task, QmcSection_ReloadTask, QmcSection_Event, QmcSection_ SchemaEvent, QmcSection_CompositeEvent`	Specifically filters on streams, apps, sheets, stories, tags, tasks, and triggers.
Conditions	`user.roles = "DepartmentAdmin"`	The rule will apply to all users that have the user role set to `DepartmentAdmin`.
Actions	`read`	Read action will be granted provided that the conditions are met.
Context	**Only in QMC**	The rule is only valid when you use the QMC.

Security rule code for "DepartmentAdminApp"

Security rule code information for DepartmentAdminApp

Field	Code	Comments
Resource filter	`App*,ReloadTask_*,SchemaEvent_*,Tag_*,CompositeEvent_*`	Specifically filters on apps, sheets, stories, tasks, tags and triggers.
Conditions	`user.roles="DepartmentAdmin" and resource.@Department=user.@Department and (resource.resourcetype="App" or (resource.resourcetype="ReloadTask" or resource.resourcetype="App.Object") or resource.resourcetype="SchemaEvent" or resource.resourcetype="CompositeEvent" or resource.resourcetype="Tag")`	The rule will apply to all users that have the user role set to `DepartmentAdmin`.
Actions	`create, read, update, delete, publish`	The actions will be granted provided that the conditions are met.

Field	Code		Comments
Context	**Only in QMC**		The rule is only valid when you use the QMC.

Security rules example: Applying Qlik Sense access rights for user types

In this example, you set access rights according to user types. Your development department comprises the following user types:

- Developer: is allowed to create apps, sheets, stories, objects and can use and create data connections.
- Contributor: is allowed to create stories and sheets for published apps but is not allowed to create new apps.
- Consumer: can only consume and is not allowed to create content.

The following activities with corresponding access rights have been identified.

Activity access rights

Activity	Developer	Contributor	Consumer
Create app	Allowed	Not allowed	Not allowed
Create app object	Allowed	Allowed	Not allowed
Create data connection	Allowed	Not allowed	Not allowed

> *The following assumes that you have the out-of-the-box rule Stream in place that gives users read access to apps on a stream that they have read access to. This will enable Consumers to read apps. Also, when setting up the access rights according to this example, the following out-of-the-box security rules must be disabled: CreateApp, CreateAppObjectsPublishedApp, CreateAppObjectsUnPublishedApp, and DataConnection.*

You set access rights according to user types by using security rules in the following main steps:

1. Define each user type so that it is possible to apply rules to each user type instead of individual users.
2. Apply the custom property to the relevant users.

   > *Alternatively, if you have a user directory with a corresponding group, you can use that instead of custom properties.*

3. Create one rule per activity type.

Procedure

Do the following:

1. Define the user types as values to a custom property.
    a. Create a custom property called UserType.
    b. Apply the custom property to the resource type Users.
    c. Define the custom property values as Developer, Contributor, and Consumer.
    d. Click **Apply**.
2. Apply the UserType custom property to the appropriate users in the **Users** page.
3. Create the four new security rules (CreateApp, CreateAppObjectsPublishedApp, CreateAppObjectsUnPublishedApp, and DataConnection):
    a. Select **Security rules** and click ✚ **Create new**.
    b. In the **Advanced** and **Basic** sections, fill in the fields **Resource filter**, **Conditions**, **Actions** and **Context**.
    Security rule code for "Create app" (page 601).
    c. Set the **Name** to correspond to the activity.
    d. Click **Apply**.
4. Make sure the following out-of-the-box security rules are disabled or deleted:
    a. **CreateApp**
    b. **CreateAppObjectsPublishedApp**
    c. **CreateAppObjectsUnPublishedApp**
    d. **DataConnection**

You have now created rules to give access rights according to user types.

Security rule code

The following is the security rule code for this example, with explanatory comments.

Security rule code for "Create app"

Security rule code fields

Field	Code	Comments
Resource filter	App_ *,FileReference_*	Specifically filters on resource type App.

Field	Code	Comments

Conditions	`!user.IsAnonymous()` and `(user.@usertype= "Developer")`	`!user.IsAnonymous()`
		This condition uses the security rules function **IsAnonymous()** that can be used to evaluate whether the user is logged in as anonymous. In this case, if the user is logged in as an anonymous user, the condition is not met.
		
		`(user.@usertype="Developer")`
		The condition is met by all users that have the custom property `@usertype` set to `Developer`.
		
		Alternatively, if you have a user directory with a corresponding group, you can use that instead of custom properties. In this case the condition could look like this: `user.group="Developer"`.

Action	`create`	The specified action is granted provided that the conditions are met.

Security rule code for "Create app object" (sheets, stories, app objects)

Security rule code fields

Field	Code	Comments
Resource filter	`App.Object_*`	Specifically filters on resource type App.Object.
Conditions	`resource.App.HasPrivilege ("read") and !user.IsAnonymous() and (user.@usertype= "Developer"or user.@usertype= "Contributor")`	`resource.App.HasPrivilege("read")` This condition uses a security rules function **HasPrivilege()** that can be used to evaluate access rights for resource types. In this instance, the function evaluates whether the resource type user is allowed to perform the action update on the resource sheet. This means that a Contributor will be allowed to create objects for sheets that the contributor owns.
Action	`create`	The specified action is granted provided that the conditions are met.

Security rule code for "Data connections"

Security rule code fields

Field	Code	Comments
Resource filter	`DataConnection_*`	Specifically filters on resource type DataConnection.

Field	Code	Comments

Conditions	`resource.resourcetype =`
	`"DataConnection" and`
	`(user.@usertype="Developer")`
		`resource.resourcetype =`
		`"DataConnection"`
		The rule will apply to resources of the type DataConnection.
		
		` user.@usertype="Developer"`
		The rule will apply to users with the custom property @usertype set to "Developer".

Action	`create`	The specified action is granted provided that the conditions are met.

Security rules example: Recreating a document admin by creating a QMC app admin

In this example, you recreate a QlikView document administrator in Qlik Sense. You can recreate the administrator by doing the following:

- Creating a new role (app admin)
- Creating a custom property to connect this role to the apps

The following table presents the security rules for the app admin role.

Security rules and their results

Security rule	The result of the rule
AppAdminQmcSections	Controls the sections in the QMC that are to be visible for the administrator.
AppAdminRead	Controls which resources the administrator is to be able to read.
AppAdminModify	Controls which resources the administrator is to be able to modify.

> *The rules that grant modify and read access have been split. Thereby, the app admin can have access to read and see (but not modify) information that can be important to understand when working with apps – in this example the stream information.*

Procedure

Do the following:

1. Create the three new security rules (AppAdminQmcSections, AppAdminRead and AppAdminModify):
   a. Select **Security rules** and click ➕ **Create new**.
   b. In the **Advanced** and **Basic** sections, fill in the fields **Resource filter**, **Conditions**, **Actions** and **Context** per *Security rule code for "AppAdminQmcSections" (page 604)*.
   c. Set the Name to correspond to the activity.
   d. Click **Apply**.
2. Apply the role to the user to make the user become app admin:

     a. Select **Users**, select a user and click **Edit**.

     b. Click ➕ under **Admin roles** and select *AppAdmin*.

     c. Click **Apply**.

3. Create a new custom property and add the user as a value:

     a. Select **Custom properties** and click **Create new**.

     b. Type *AppAdmin* in the **Name** field.

     c. Under **Resource types**, select **Apps**.

     d. Under **Values**, click ➕ **Create new**, add the **User ID** as a value and click **OK**.

     e. Click **Apply**.

4. Select the apps that this user is to be able to administrate:

     a. Select **Apps**, Ctrl+click to select more than one app and click **Edit**.

     b. Select the **User ID** for the custom property **AppAdmin**.

     c. Click **Apply**.

You have now created and assigned the app admin role. When the user with this role logs in to the QMC the following can be accessed: apps, tasks, sheets, and streams.

Security rule code

The following is the security rule code for this example, with explanatory comments.

Security rule code for "AppAdminQmcSections"

Security rule codes for AppAdminQmcSections

Field	Code	Comments
Resource filter	`QmcSection_Stream, QmcSection_App, QmcSection_App.Sheet,QmcSection_App.Story, QmcSection_Tag,QmcSection_Task, QmcSection_ReloadTask, QmcSection_Event, QmcSection_SchemaEvent, QmcSection_CompositeEvent`	Specifically filters on streams, apps, sheets, stories, tags, tasks, and triggers.
Conditions	`user.roles = "AppAdmin"`	The rule will apply to all users that have the user role set to `AppAdmin`.
Actions	`read`	Read action will be granted provided the conditions are met.
Context	**Only in QMC**	The rule is only valid when you use the QMC.

Security rule code for "AppAdminRead"

Security rule codes for AppAdminRead

Field	Code	Comments
Resource filter	`Stream_*,App*,ReloadTask_*,SchemaEvent_*,Tag_*,CompositeEvent_ *,User*`	Specifically filters on resource types: streams, apps, sheets, stories, tags, tasks, and triggers.
Conditions	`user.roles = "AppAdmin" and ((resource.resourcetype="App" and resource.@AppAdmin=user.userId and user.userDirectory="QVNCycles") or ((resource.resourcetype="ReloadTask" or resource.resourcetype="App.Object") and resource.app.@AppAdmin=user.userId and user.userDirectory="QVNCycles") or resource.resourcetype="SchemaEvent" or resource.resourcetype="CompositeEvent" or resource.resourcetype="Tag" or resource.resourcetype="Stream" or resource.resourcetype="User")`	The rule will apply to all users with the same `userId` as the custom property `AppAdmin` connected to apps.
Actions	`read`	Read action will be granted provided the conditions are met.
Context	**Only in QMC**	The rule is only valid when you use the QMC.

Security rule code for "AppAdminModify"

This rule determines what the app admin can modify in the QMC. This is the same rule as for read except for that streams cannot be modified.

Security rule codes for AppAdminModify

Field	Code	Comments
Resource filter	`App*,ReloadTask_*,SchemaEvent_*,Tag_*,CompositeEvent_*`	Specifically filters on resource types: streams, apps, sheets, stories, tags, tasks, and triggers.
Conditions	`user.roles = "AppAdmin" and ((resource.resourcetype="App" and resource.@AppAdmin=user.userId and user.userDirectory="QVNCycles") or ((resource.resourcetype="ReloadTask" or resource.resourcetype="App.Object") and resource.app.@AppAdmin=user.userId and user.userDirectory="QVNCycles") or resource.resourcetype="SchemaEvent" or resource.resourcetype="CompositeEvent" or resource.resourcetype="Tag")`	The rule will apply to all users with the same userId as the custom property `AppAdmin` connected to apps.
Actions	`create, update, delete, changeowner`	The specified actions will be granted provided the conditions are met.
Context	**Only in QMC**	The rule is only valid when you use the QMC.

Security rules example: Access to stream by user attributes

In this example, you create access rights to a specific stream by using the user attributes that are retrieved from ticket authentication or session and SAML attributes.

To enable using the user attributes you must first add the ticket via the proxy API.

Procedure

Do the following:

1. Select **Security rules** and click ⊕ **Create new**.
2. The resource filter for the rule should be set to filter on a specific stream.
    In the **Advanced** section, fill in the **Resource filter** field with text as per *Security rule code (page 607)*.
3. You now need to set the conditions to specify the users that the rule applies to.

In the **Advanced** section, fill in the **Conditions** field with text as per *Security rule code (page 607)*.

4. Set the actions that the rule should provide.
   In the **Basic** section, select **Actions** as per *Security rule code (page 607)*.

5. Type a name for the security rule in the **Name** field.

6. Click **Apply**.

You have now created access to a specific stream based on ticket authentication user attributes.

Security rule code

The following is the security rule code for this example, with explanatory comments.

Security rule code fields

Field	Code	Comments
Resource filter	`Stream_<GUID>`	Specifically filters on the stream with a specific GUID.
Conditions	`resource.resourcetype="Stream" and (user.environment.<Attribute1>="<Value1a>")`	`resource.resourcetype="Stream"` The rule applies to streams. `( user.environment.<Attribute1>="<Value1a>")` The rule applies to the users where the attribute equals the value.
Actions	`read`	Read actions will be granted provided that the conditions are met.

Security rules example: Access to stream by IP address

In this example, you create access rights to a specific stream through the IP address.

You can use the IP address for access rights in the following cases:

- When you want an app to only be available from an internal network.
- When you want an app to only be available to mobile users.

Procedure

Do the following:

1. Open **Virtual proxies**.
2. Select the virtual proxy that you want to edit and click **Edit**.
3. In the **Advanced** section, select **Extended security environment**.
4. Click **Apply**.
5. Click **OK** in the **Apply changes to virtual proxy** popup.
6. Open **Streams** and create a new stream.
7. Open **Security rules** and click ⊕ **Create new**.

8. In the **Create rule from template** list, select **Stream access**.

9. Enter a name for the rule.

10. Set the resource filter to filter on a specific stream:
In the **Advanced** section, fill in the **Resource filter** field as per *Security rule code (page 608)*.
Example: *Stream_aaec8d41-5201-43ab-809f-3063750dfafd*

11. Set the conditions to specify the resource and IP address that the rule applies to:
In the **Advanced** section, fill in the **Conditions** field as per *Security rule code (page 608)*.
Example: *user.environment.ip = "::ffff:10.88.0.5"*

12. Set the actions that the rule is to provide:
In the **Basic** section, select **Actions** as per *Security rule code (page 608)*.
Select the actions **Read** and **Publish**.

13. Click **Apply**.

You have now created access to a specific stream based on the IP address of the connecting device.

Security rule code

The following is the security rule code for this example, with explanatory comments.

Security rule code fields

Field	Code	Comments
Resource filter	`Stream_<GUID>`	Filters on a specific stream.

Field	Code	Comments
Conditions	`(user.environment.ip="<Your_IP_address>")` There are different formats for the `user.environment.ip` condition. With the implementation of the hybrid dual-stack IPv6/IPv4, it is always the IPv6 format that is used. If the client that makes the call uses IPv6, the IPv6 address is added by the proxy. If the client uses IPv4, the IPv4-mapped addresses are used. **Example 1:** *IPv4 address: 10.88.0.5 => ::ffff:10.88.0.5 (IPv6)* In this case the rule condition can be written in the following ways: • user.environment.ip like "*10.88.0*" • user.environment.ip like "::ffff:10.88*" • user.environment.ip = "::ffff:10.88.0.5" **Example 2:** *IPv6 address: 2001:0db8:85a3:0000:0000:8a2e:0370:7334* In this case the rule condition can be written in the following ways: • user.environment.ip like "*0db8:85a3:0000:0000:8a2e*" • user.environment.ip like "2001:0db8:85a3:0000:0000*" • user.environment.ip = "2001:0db8:85a3:0000:0000:8a2e:0370:7334" ℹ *The asterisks (*) in the examples indicate additional characters.*	`(user.environment.ip="<Your_IP_address>")` The rule applies to the devices that connect from an IP address that corresponds to the value.
Actions	`Read, Publish`	Read and Publish actions will be granted provided that the conditions are met.

Security rules example: Qlik Sense Mobile Client Managed offline access to apps by user attributes

In this example, you create offline access rights to a specific app by using the user attributes that are retrieved from ticket authentication or session and SAML attributes.

To enable using the user attributes you must first add the ticket via the proxy API.

Procedure

Do the following:

1. Select **Security rules** and click ⊕ **Create new**.
2. The resource filter for the rule should be set to filter on a apps.
    In the **Basic** section, fill in the **Resource filter** field with text as per *Security rule code (page 610)*.
3. You now need to set the conditions to specify the users that the rule applies to.
    In the **Advanced** section, fill in the **Conditions** field with text as per *Security rule code (page 610)*.
4. Set the actions that the rule should provide.
    In the **Basic** section, select **Actions** as per Security rule code (page 610).
5. Type a name for the security rule in the **Name** field.
6. Click **Apply**.

You have now created access to a specific stream based on ticket authentication user attributes.

Security rule code

The following is the security rule code for this example, with explanatory comments.

Security rule

Field	Code	Comments
Resource filter	`App_*`	Specifically filters on the resource type App.
Conditions	`resource.resourcetype="App_*" and (user.environment.<Attribute1>="<Value1a>")`	`resource.resourcetype="App_*"` The rule applies to apps. `( user.environment.<Attribute1>="<Value1a>")` The rule applies to the users where the attribute equals the value.
Actions	`read`	Read actions will be granted provided that the conditions are met.

Security rules example: A customer case

The following example presents a customer case where a flexible solution was developed to suit the customer's needs regarding security rules.

User directory structure

The customer had the following user directory structure that they wanted to reuse.

Project

Example user directory structure 1

Role	Access	Content
Developer	Folder connection	Excel files
Admin	QMC access	Apps, App objects, Tasks
Audience 1	Stream	Dashboard 1, Dashboard 2, Dashboard 3
Audience 2	Stream	Dashboard 4, Dashboard 5, Dashboard 6

The structure shows that the customer has multiple projects in their Qlik Sense deployment, which consists of a number of roles:

- Developers, who are allowed to develop material for this project using a folder connection.
- Admins, a kind of super users, who are allowed to administer resources in the project.
- Audiences, users who are allowed to consume defined sets of dashboards through streams connected to the respective audience.

Adding security roles and project groups

The following table reuses the original user directory structure, but adds security role and project group as two new properties.

Project (proj_X)

Example user directory structure 2

Role (security role)	Project (project group)	Content
Developers (role_dev)	DC_ProjectX (projX_dev)	Excel files
Admin (role_admin)	QMC access (projX_admin)	Apps, App objects, Tasks
Audience 1 (role_ext) (No role = Read access)	Proj1_Aud1 (projX_aud1)	Dashboard 1, Dashboard 2, Dashboard 3
Audience 2 (role_ext) (No role = Read access)	Proj1_Aud2 (projX_aud2)	Dashboard 4, Dashboard 5, Dashboard 6

The new properties are used to define the different groups:

- Security role: defines what actions a user is allowed to perform (create apps, add sheets, export data, and so on).
- Project group: decides what projects and which project resources that a user is allowed to access.

Implementing the new properties

Project groups are implemented through the use of custom properties, which give access to projects and resources. Security roles are implemented in the user directory.

There are a number of benefits to this approach:

- The number of rules needed to describe the security policy is reduced.
- Rules change slowly. The system is configured through attributes, and it is only when security needs to be changed that rule changes are required.
- User management and provisioning of permissions are maintained in the user directory.

What rules need to be created?

One rule is needed for resource access.

New resource access rule

Setting	Value
Name	ResourceAccess
Resource filter	`Stream_*, DataConnection_*`
Conditions	`((user.group=resource.@GroupAccess))`
Actions	Read

This rule will grant a user access to a resource, if the resource custom property GroupAccess contains the group name of the user. For this to work, a custom property called GroupAccess is needed, containing all user groups.

This rule can be connected to streams and data connections. The rule makes it is possible to grant users in the groups access to streams using a custom property.
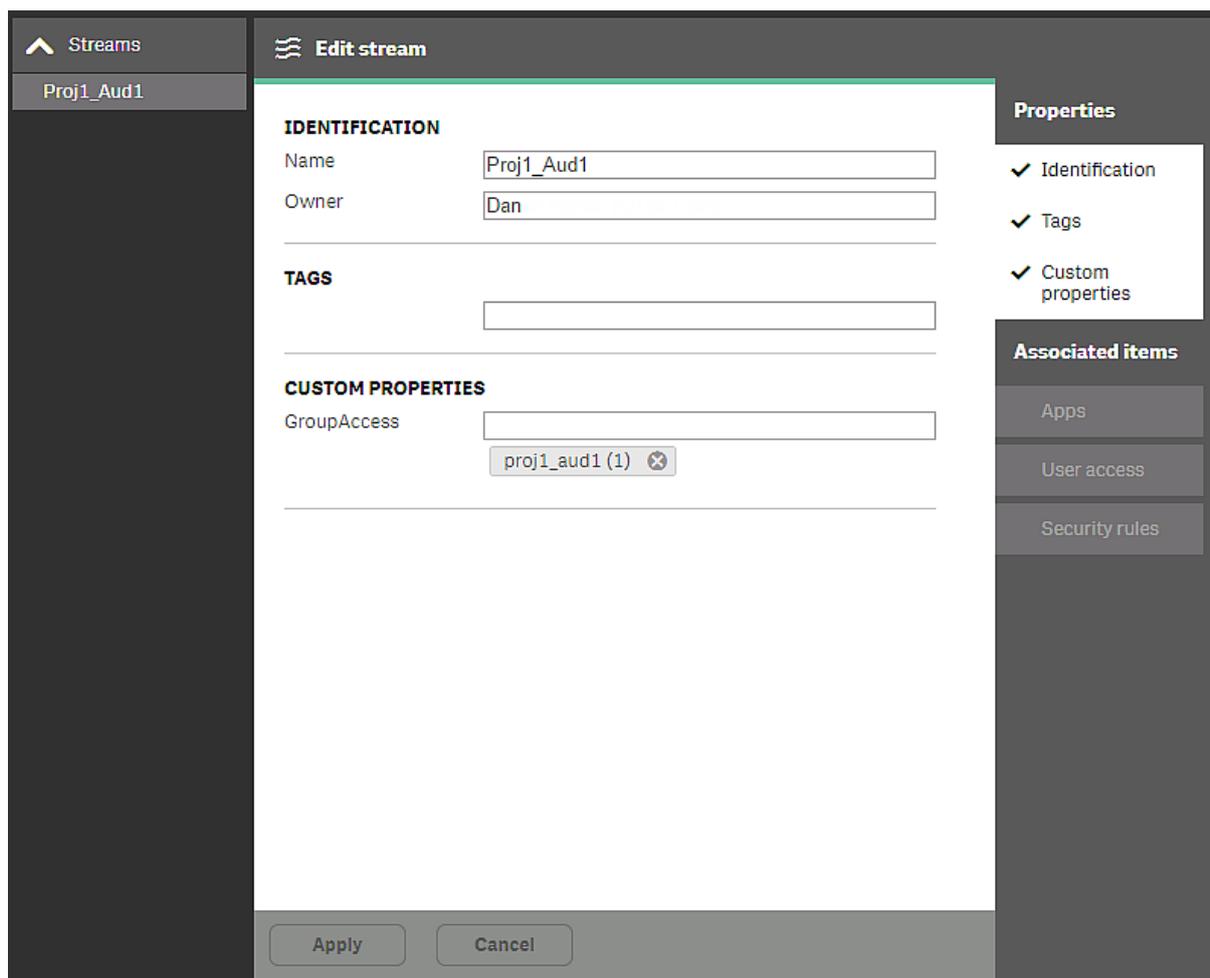
In this example, the proj1_aud1 group has been added in their user directory access to the Proj1_Aud1 stream. If additional groups need access, they can be added to the custom property.

The next rule to be created defines who should be allowed to administer the streams.

Stream administration rule

Setting	Value
Name	TeamAdminRead
Resource filter	Stream*,App*,ReloadTask*,SchemaEvent*,Tag*,CompositeEvent*,ExecutionResult*,CustomProperty*,DataConnection*
Conditions	((resource.resourcetype="App" and user.group = resource.stream.@AdminGroup) or (resource.resourcetype="App.Object" and user.group = resource.app.stream.@AdminGroup) or (resource.resourcetype="ReloadTask" and resource.app.stream.@AdminGroup = user.group) or (resource.resourcetype="DataConnection" and resource.@AdminGroup = user.group) or resource.resourcetype ="SchemaEvent" or resource.resourcetype ="CompositeEvent" or resource.resourcetype = "Tag" or resource.resourcetype ="ExecutionResult")
Actions	Read, Update

Description of the rule: if you are part of the admin group for a stream, you can manage resources related to the apps published in that stream.

For this to work we need to create the custom property AdminGroup containing the names of the groups that contain admins for the projects.

In this example, users in the group proj1_admin have administrative access to resources related to apps in this stream.

What security roles need to be created?

Three different security roles have been defined:

- role_admin: users who need to be able perform admin tasks
- role_dev: users who need to be able to perform development work in projects
- role_ext: users who need to be able to extend apps

The admin role requires two rules. This following rule gives users in the role_admin group access to sections in the QMC.

Admin QMCrule

Setting	Value
Name	TeamAdminSections

Resource filter	QmcSection_App,QmcSection_DataConnection,QmcSection_ContentLibrary,QmcSection_App.Object,QmcSection_Task, QmcSection_ReloadTask, QmcSection_Event, QmcSection_SchemaEvent, QmcSection_CompositeEvent
Conditions	`((user.group="role_admin"))`
Actions	Read

The following rule gives users in the role_admin group the possibility to create, among other things, apps, reload tasks, and data connections.

Admin creation rule

Setting	Value
Name	TeamAdminCreate
Resource filter	App*,ReloadTask*,SchemaEvent*,CompositeEvent*,ExecutionResult*,DataConnection*
Conditions	`((user.group="role_admin"))`
Actions	Create

The role_ext rule is created by tweaking a default rule. Only users in the group role_ext are allowed to extend apps with new sheets. To add flexibility, a new custom property (Extendable) is added to apps. An app marked Extendable allows all users to add sheets to that app.

Extendablerule

Setting	Value
Name	CreateAppObjectsPublishedApp
Resource filter	QmcSection_App,QmcSection_DataConnection,QmcSection_ContentLibrary,QmcSection_App.Object,QmcSection_Task, QmcSection_ReloadTask, QmcSection_Event, QmcSection_SchemaEvent, QmcSection_CompositeEvent
Conditions	`!resource.App.stream.Empty() and resource.App.HasPrivilege("read") and (resource.objectType = "userstate" or resource.objectType = "sheet" or resource.objectType = "story" or resource.objectType = "bookmark" or resource.objectType = "snapshot" or resource.objectType = "embeddedsnapshot" or resource.objectType = "hiddenbookmark") and !user.IsAnonymous() and (user.group="role_dev" or user.group="role_ext" or resource.app.@Extendable="Yes")`
Actions	Create

Finally, for the developers, another rule is tweaked, so that only developers in the role_dev group are allowed to create apps.

Developer creation rule

Setting	Value
Name	CreateApp

Resource filter	App_*
Conditions	`!user.IsAnonymous() and user.group="role_dev"`
Actions	Create

Summary

With this setup you can manage Qlik Sense through the groups in your user directory and when you add content to Qlik Sense, you only use the attributes to define what the groups should have access to.

> This approach, where roles are separated from groups, assumes that users do not have different roles in different projects. If users have different roles, you need to create separate roles for each project.

1.10   Distribution policies - introduction

Qlik Sense Enterprise distribution policies govern how Qlik Sense apps are distributed from an on-premises Qlik Sense Enterprise on Windows node to Qlik Sense Enterprise SaaS.

You will want to distribute apps from Qlik Sense Enterprise to your deployment for consumption by users with multi-cloud access. To be able to distribute apps to multi-cloud, you define distribution policies. With distribution policies, you determine which published apps that are distributed to Qlik Sense Enterprise SaaS. Distribution policies are required for distributing apps to cloud. If a published app is not covered by a distribution policy, then it will not be distributed.

Distribution policies are initially evaluated on Qlik Sense Enterprise when apps are published. The result is a list of deployments on Qlik Sense Enterprise SaaS that will receive a copy of the published app. The distribution policies are re-evaluated when previously published apps are changed, moved, or deleted.

Creating distribution policies

The following is a high-level description of the steps involved when creating distribution policies:

1. Set the resource filter to determine what resource the rule applies to (`App_*`).
2. Select the actions that the rule grants (`Distribute`).
3. In the rule editor, define conditions for the rule.
   App custom properties and stream names from publish actions offer useful values to test in the rule conditions you define.
4. Validate the rule.
5. Apply the rule.

To learn about how you publish apps from the hub to collections, see "Publishing collections" in the Qlik Sense on Windows documentation.

Creating distribution policies

You use distribution policies to enable distribution of apps from Qlik Sense Enterprise to Qlik Sense Enterprise SaaS. Distribution policies are similar to security rules. In both cases, you define what resources the rule applies to and what actions that can be performed.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Cloud distribution** on the QMC start page or from the **Start▼** drop-down menu to display the overview.

3. Click ⊕ **Create new**.

4. Edit the properties in the **Edit distribution policy** window.

Distribution policy identification properties

Property	Description	Default value
Create rule from template	Select a template for your rule to have some values automatically filled in. ⓘ *Changing the **Create rule from template** selection automatically clears all **Actions**, and changes the **Conditions** text box in the **Advanced** section accordingly.*	**Unspecified**
Disabled	Select to disable the rule if you do not want it to be active.	Cleared
Name	Name the rule.	Blank
Description	Optional. Add a description of the rule.	Blank

Distribution policy basic properties

Property	Description	Default value
Resource filter	In the list, select the resource that the rule will apply to. Note that **App_*** means that the rule only applies to apps and not app objects and app sheets.	**App_***
Actions	Select the actions for the rule.	**Distribute**

Distribution policy advanced properties

Property	Description	Default value
Conditions	The text box reflects changes made in the policy editor above. You can define conditions by typing in the text box.	((subject.name=""))

Click **Validate rule** to check that the syntax is correct.

Distribution policy tag properties

Property	Description
Tags	*If no QMC tags are available, this property group is empty.*
	Click the text box to be display a list of the available tags. Start typing to reduce the list. Connected tags are displayed under the text box.

5. Click **Apply** in the action bar to save your changes.

Successfully added is displayed at the bottom of the page.

Distribution policies - using custom properties

You create distribution policies to determine how apps are distributed to your cloud deployments. Distribution policies are mandatory when you want to distribute apps from Qlik Sense Enterprise on Windows to Qlik Sense Enterprise SaaS. Once created, any published app that matches the criteria in the distribution policy is distributed to the defined targets.

The first time an app is distributed to cloud, both app data (if any) and metadata, such as name, owner, stream, and custom properties, is distributed. On subsequent distributions, app data is only distributed if it has been changed more recently than the latest reload, otherwise only metadata is distributed. The app data in the cloud app then remains unchanged. Changes made to app content and app objects do not trigger a distribution of app data, but publishing or reloading an app does.

Prerequisites

- A license that includes multi-cloud. Either of the following:
    - The same signed license key for Qlik Sense Enterprise on Windows and Qlik Sense Enterprise SaaS.
    - Different license keys, where the cloud attributes are enabled and on-prem is activated through a signed license.
- You have two tenants that you can distribute apps to.
- For each tenant you have completed the following:
    - *Setting up a deployment (page 620)*
    - *Creating the identity provider configuration (page 620)*

Once those steps are completed, proceed to *Creating a distribution policy for distributing apps to different deployments (page 621)*

Setting up a deployment

Do the following:

1. In the Qlik Management Console (QMC) of your Qlik Sense Enterprise on Windows server, open **Cloud distribution**.

2. Select **Distribution policies**.

3. Click **Set up new** in the bottom-left corner.

4. Enter a deployment name. Use *Region1* for the first deployment and *Region2* for the second one.
   You will use these names as values in the custom property.

5. Enter the **API endpoint**, that is, your tenant address.
   Example: *https://my-tenant.eu.qlikcloud.com*.

6. For **Audience**, enter *qlik.api*.

7. Select **Use local bearer token**.

> *Using a local bearer token simplifies setup. If you do not use it, you need to enter **Client ID**, **Client secret**, and **Token endpoint** instead.*

8. Click **Copy to clipboard**.
   You need the local bearer token in the identity provider configuration.

9. Click **Apply**.

Creating the identity provider configuration

Do the following:

1. Open the Management Console in your cloud tenant and select **Identity provider** in the menu to the left.

---

2. Click **Create new**.
   The **Create identity provider configuration** window is opened.

3. Under **Type**, select *Multi-cloud*.

4. Optionally, enter a description.

5. In the **Local bearer token** box, paste the token you copied in the deployment setup.

Creating a distribution policy for distributing apps to different deployments

You create the distribution policy in the QMC. When you publish apps, you can use custom properties to define where to distribute the apps.

Begin by creating a custom property and then use it in the distribution policy.

Creating a custom property for deployments

The custom property will have deployment names as values.

Do the following:

1. In the QMC, open the **Custom properties** section.

2. Click ➕ **Create new**.

3. Name the custom property *deployments*.

   > *If you want tags to be displayed under Details in the cloud app, the name of the custom property must be Tags. The custom property values that are selected as tags when publishing the app will then be displayed under Details in the cloud app.*

4. Under **Resource types**, select **Apps**.

5. Under **Values**, click ➕ **Create new**.

6. Type *Region1* as a value.

7. Add the value *Region2* in the same way.

8. Click **Apply**.

Now you have two custom property values that you can use in the distribution policy.

Creating the distribution policy

Distribution policies are used to determine whether a published app can be distributed to one or more of the deployments in Qlik Cloud. Only published apps can be distributed.

Do the following:

1. In the QMC, open the **Cloud distribution** section and select **Distribution policies**.
2. Click ✚ **Create new**.
3. In the **Create rule from template list**, select *Distribution_App*.
4. Name the distribution policy *Distribute to cloud deployments*.
5. Under **Basic**, verify that the resource filter value is *App_** and the action **Distribute** is selected.
6. In the rule editor, keep the values *subject* and *name*. On the second row, in the first drop-down list, select **#App**. In the last field add: *@deployments*.
    The **Conditions** box in the **Advanced** section should have the following string:
    `((subject.name=resource.@deployments))`. This could be read as follows:
    "If the deployment name equals the custom property value applied to the app, the app will be distributed to that deployment."
7. Click **Validate rule**.

The rule syntax is checked, and, if valid, a confirmation is displayed.

8. Click **Apply** to save the rule.

With this setup you can distribute apps to either one of the deployments, or both, depending on which tags are used when publishing the apps in the hub.

Editing distribution policies

You use distribution policies to enable distribution of apps from Qlik Sense Enterprise to Qlik Sense Enterprise SaaS. Distribution policies are similar to security rules. In both cases, you define what resources the rule applies to and what actions that can be performed.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **Distribution policies** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. Select the policy you want to edit.
4. Click **Edit** in the action bar.
5. Edit the properties in the **Edit distribution policy** window.
   Identification

Distribution policy identification properties

Property	Description	Default value
Create rule from template	Select a template for your rule to have some values automatically filled in. ⓘ *Changing the **Create rule from template** selection automatically clears all **Actions**, and changes the **Conditions** text box in the **Advanced** section accordingly.*	**Unspecified**
Disabled	Select to disable the rule if you do not want it to be active.	Cleared
Name	Name the rule.	Blank
Description	Optional. Add a description of the rule.	Blank

Basic

Distribution policy basic properties

Property	Description	Default value
Resource filter	In the list, select the resource that the rule will apply to. Note that **App_*** means that the rule only applies to apps and not app objects and app sheets.	**App_***
Actions	Select the actions for the rule.	**Distribute**

Advanced

Distribution policy advanced properties

Property	Description	Default value
Conditions	The text box reflects changes made in the policy editor above. You can define conditions by typing in the text box.	((subject.name=""))

Click **Validate rule** to check that the syntax is correct.

Tags

Tag properties

Property	Description
Tags	*If no QMC tags are available, this property group is empty.* Click the text box to be display a list of the available tags. Start typing to reduce the list. Connected tags are displayed under the text box.

6. Click **Apply** in the action bar to save your changes.

Successfully updated is displayed at the bottom of the page.

1.11   Auditing access control

The QMC includes the audit tool, which enables you to review and preview access rights and the associated security rules. In the preview, you can see the effects that a new or edited rule will have without disrupting your system.

The audit tools only show rules as they are applied to existing resources. For example, if you create a rule for apps with names that begin with "MyApp", the audit page and preview page only show results if there is actually an app with that name in the Qlik Sense system.

Example:

Your company is organized into the following departments: Finance, Sales, Marketing, and Development. You have created a custom property called Departments with values that match the name of the departments and applied the departments to streams. Finally, you have created security rules using the **Streams** page in the QMC to provide users in Finance with publishing and read rights to the Quarterly reports stream. All other departments have read access rights. You now want to check that your rules have been applied correctly.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Click **Audit** on the QMC start page.
3. On the **Audit** page, select **Streams** from the target resource list.

4. To the right of the target resource list, click ⌕ and select the stream `Quarterly reports`.

5. Click **Audit**.
   The resulting table shows user IDs and the streams (in this case only the stream Quarterly reports). For each user, the grid shows characters that correspond to the access rights that the user has to the stream.
   Finance users should have read and publish access rights, while all other users should have read access (provided they have the custom property Department).
   Only users with access rights to the stream are shown in the grid, if no user filter is specified. This means that a user missing from the list has no access to the resource. Specifying a user filter will force the audit result for the user to be displayed in the grid. The same principle is valid for resources, if no resources are selected, only resources which have any audit results will be displayed in the grid.

6. Double-click a cell in the grid (not an admin user) corresponding to a user belonging to the Finance department.
   The **Associated rules** window opens.
   You should now see the security rules that apply to the selected user with respect to the Quarterly reports stream. The list should include the following rules:

   - Stream_read_Quarterly reports

   - Stream_publish_Quarterly reports

7. Double-click a cell in the grid (not an admin user) corresponding to a user belonging to the Sales department.
   The **Associated rules** window opens.
   You should now see the security rules that apply to the selected user with regard to the Quarterly reports stream. The list should include the following rule:

   - Stream_read_Quarterly reports

Defining an audit query

You can query for security rules, load balancing rules, or license rules.

Defining a security rules query

Do the following:

1. In the target resource list, select a resource type.

2. Next to the target resource list, click ⌕ and select the resources to audit on.

3. To the right of **Users**, click ⌕ and use the search to filter the users to audit on.

4. In the **Environment** list, select the context for the audit.

5. (Optional) Click ⌶ if you want to simulate a certain user environment.
   Example: *OS=Windows; IP=10.88.3.35; Browser=Firefox;*.

6. To the right in the header bar, click **Privileges to audit** and select which privileges to display in the audit table.

7. Click **Audit** to perform the query.
   An audit table is displayed. Click **Transpose** to pivot the table.

Defining a load balancing rules query

1. In the header bar drop-down list, select **Audit load balancing rules**.

2. Select the target resource to audit on, **Apps** or **Nodes**.

3. Next to the target resource list, click Q and select the resources to audit on.

4. In the **Environment** list, select the context for the audit.

5. (Optional) Click ⊡ if you want to simulate a certain user environment.
    Example: *OS=Windows; IP=10.88.3.35; Browser=Firefox;*.

6. Click **Audit** to perform the query.
    An audit table is displayed. Click **Transpose** to pivot the table.

Defining a license rules query

1. In the header bar, select **Audit license rules**.
    The **Audit query** resource is automatically set to **Login access**.

2. Next to the target resource list with **Login access** selected, click Q and use the search to filter the resources to audit on.

3. In the **Environment** list, select the context for the audit.

4. (Optional) Click ⊡ if you want to simulate a certain user environment.
    Example: *OS=Windows; IP=10.88.3.35; Browser=Firefox;*.

5. Click **Audit** to perform the query.
    An audit table is displayed. Click **Transpose** to pivot the table.

Viewing and filtering audit query results

You can filter the query results using the drop-down property lists.

Do the following:

1. Define a query and click **Audit** as appropriate.
    The query results are shown in the table.

    > ⓘ   *Inactive users are not shown.*

2. Click **Privileges to audit** and select the privileges to display.
    By default, the read privileges are displayed. What privileges that are available for a particular audit depends on the selected resource. The following table presents the different cell colors.

    Cell colors

Color	Description
White	No rules exist to provide access.
Green	Access is granted.
Yellow	Access is disabled.

Red	Rule evaluation is broken.
Blue	Preview color when editing or creating a new rule.

3. Double-click a cell in the matrix to open the **Associated rules** window.
   The **Associated rules** window shows the security rules that give access to the selected user/resource combination.
   Select a rule and click **Edit** to open the edit page.

> *You can only view security rules that you have access rights to read.*

1.12   Troubleshooting - QMC

The troubleshooting topics are divided into different categories. The possible causes are described and you are presented with actions to solve the problems.

Troubleshooting - Starting the QMC

This section describes problems that can occur when starting the QMC.

I cannot access the QMC the first time I try to browse to it

When you try to access the QMC for the very first time, you may experience one of the following problems.

Certificate error

Possible cause

The browser has too high security settings, and therefore the Qlik Sense certificate is not trusted. (This certificate is added during installation).

Proposed action

Choose to continue to the website, despite the warning that it is not recommended. However, make sure that the URL is correct.

If you use a third-party certificate, the error will no longer be displayed.

Changing to a signed server proxy certificate (page 501)

The page is blank, and the address bar displays a warning

Possible cause

A third-party certificate is needed.

Proposed action

Access the QMC from the server and add a new third-party certificate.

Changing to a signed server proxy certificate (page 501)

Error message displayed and 401 warning seen in network traffic

Possible cause

Qlik Sense site is not listed as a trusted site.

Proposed action

Add the fully-qualified domain name (FQDN) of the host to the trusted sites.

Do the following:

1. In the Control Panel, select **Internet options**.
2. Select the **Security** tab.
3. Select **Trusted sites**.
4. Click **Sites**.
5. Click **Add**.
6. Enter the FQDN of the host in the text field and click **Add**.
7. Click **Close**
8. Click **OK**.

I cannot access the QMC from the host machine

I am trying to access the QMC from the same machine that hosts the Qlik Sense site, but I receive a **401.1 Access Denied** error from the browser.

Possible cause

Loopback security settings in Windows Server may prevent access using a fully qualified domain name (FQDN), from the same machine that hosts the Qlik Sense site.

Proposed action

Access the QMC using a localhost address: *https://localhost/qmc*.

It is also possible to disable loop checking. For more infomation about this, refer to Microsoft support knowledge base article.

➡ Error message when you try to access a server locally by using its FQDN or its CNAME alias

Unable to get the custom properties definitions is displayed when I start the QMC

Possible cause

Failed to retrieve the custom property data from the repository.

Proposed action

Refresh the QMC.

The page is blank when I open the QMC

Possible cause

There have been multiple DNS entries for your computer (you have been logged on to more than one network), so that your *host.config* file may be pointing to the wrong host name.

Proposed action

Do the following:

1. Stop all running services.
2. Delete all certificates related to your installation of Qlik Sense.
3. Open the folder *%ProgramData%\Qlik\Sense*.
4. Delete the *host.config* file.
5. Do a repair.

The *host.config* file is recreated with default settings.

I cannot open the QMC

The page is blank when I open the QMC, or a warning shows that the certificates are used by another program. Messages may also report an SSL protocol error or that a connection was refused.

Possible cause

The required port is not available, because the port is being used by another program, such as, VMware, Skype, or IIS.

Proposed action

Do the following:

1. Check the proxy system log file in this location: *%ProgramData%\Qlik\Sense\Log\Proxy*.
2. Verify that the proxy is running and that it is able to listen to the required port. By default the proxy runs on port 443 and this port needs to be available.
3. Fully shut down any other programs using port 443 and restart the proxy service. Also, change the port settings in these programs.

"Page cannot be displayed" is shown when I try to open the QMC

Possible cause

There are too many trusted root certificates on the server that runs the Qlik Sense services.

Proposed action

Check the logs for the Qlik Sense Repository Service (QRS) and remove any unnecessary certificates.

> ⚠️ *Do not remove any certificates without checking with your system administrator and IT security team first.*

Do the following:

1. Check if the QRS security log file (available at
   %ProgramData%\Qlik\Sense\Log\Repository\Trace\<MachineName>_Security_Repository.txt) contains
   the following messages:
     - "Trusted root certificates on this node is uncomfortably high: <number of certificates>"
     - "This might impede SSL communication, since Windows truncates too large (300+) lists of
       Trusted root certificates that are sent to client during SSL handshake"
     - "Please consider removing too old or otherwise invalid trusted root certificates (under
       <location>)"

2. Open the Microsoft Management Console (MMC) and remove as many unneeded certificates as
   possible.

   The QRS security log contains information on where to find the certificates (see <location> in the log
   message in step 1).

3. Restart the Qlik Sense services.

Plan and deploy Qlik Sense

Troubleshooting - Managing QMC resources

This section describes problems that can occur when managing QMC resources.

Error message: **400 Bad Request**

There is more than one possible cause when the error message **400 Bad Request** is displayed.

Importing an app in the QMC fails

The logs show an error message: Server:ImportApp_impl caught extended exception 400: Bad Request

Possible cause

The app contains a web connection that makes the URL exceed 1024 characters.

Proposed action

1. Open the app in Qlik Sense Desktop to see if the app contains a web connection that makes the URL
   longer than 1024 characters.
2. Use a service such as bit.ly to shorten the URL.

The REST HTTP request incorrect

Possible cause

The REST HTTP request to the proxy or the repository is incorrectly formatted.

Proposed action

Correct the formatting of the REST HTTP request.

> *A complete request must contain ?XrfKey=<minimum 16 characters> in the URL, and also, in the same request, include the header X-Qlik-XrfKey with exactly the same string as a value (to resist cross-site scripting attacks).*

Error message: **401 Unauthorized**

Authentication of the connector fails when the password contains special characters.

Possible cause

While in the QMC, you have edited the connector password and added one or more of the following special characters:

- %
- =
- ;

Proposed action

Use the data load editor to edit the password.

Error message: **403 Forbidden**

Possible cause

- There are too many root certificates on the computer (> ~300), and as a consequence, the Qlik Sense services are not allowed to communicate.
- You are trying to access a resource that you are not granted access to, according to the rule engine in the repository.

Proposed action

Remove any unused root certificates. See also the following Microsoft help documentation:
SSL/TLS communication problems after you install KB 931125

Error message: **405 Method not allowed**

Possible cause

The URL refers to a non-existent REST function.

Proposed action

Modify the URL.

Error message: **Internal server error 500**

There is more than one possible cause when you get error 500.

App import was unsuccessful

Possible cause

You have attempted to import an app with a name longer than 2500 characters.

Proposed action

Reduce the app name to maximum 2500 characters.

Unidentified error

Possible cause

An unidentified error has occurred.

Proposed action

Check the system log files at the following locations:

- *%ProgramData%\Qlik\Sense\Log\Proxy*
- *%ProgramData%\Qlik\Sense\Log\Repository*

> *If the error message is displayed repeatedly, please contact your Qlik Sense representative and provide the system log files.*

Error message: **Connection lost** is displayed when I try to connect to the Qlik Sense hub

Possible cause

The address being used when accessing the Qlik Sense hub is not present in the host allow list in the Qlik Sense Proxy Service.

The **Connection lost** error message commonly occurs in the following cases:

- The Qlik Sense hub is accessed using the IP address, for example, *https://192.168.0.25/hub*, instead of the host name, *https://myhost/hub*, or the fully qualified name (FQN), *https://myhost.company.com/hub*.
- The Qlik Sense hub is accessed using a different address than the one registered as the default Domain Name System (DNS) name or FQN of the machine. As an example, when using Amazon Web Services, or similar environments, the internally registered DNS name is not the same as the externally facing address.

Proposed action

Do the following:

1. From the QMC, open **Virtual proxies**.
2. Select the virtual proxy and click **Edit**.

3. In the **Properties** list, select **Advanced**.

4. Locate **Host allow list**.

5. Click **Add new value** and add the address used to connect to the Qlik Sense hub from a client.
    IP address: 192.168.0.10, FQN: *myqlikserver.company.com*.

6. Click **Apply**.
    A proxy restart message is displayed.

7. Click **OK**.

> An entire domain can be allow listed by adding company.com to the allow list. This will allow list all other addresses within that domain, such as myqlikserver1.company.com, myqlikserver2.company.com, and so on.

Error message: **ODBC connection failed**

A scheduled reload failed with the error message **ODBC connection failed**.

Possible cause

The data connection uses single sign-on (SSO), which requires that the connection is used by an actual user, and the app uses "SQL SELECT…" to load data.

There is more than one possible solution to this problem:

Proposed action (change data connection not to use SSO)

Specify which user name and password that should be used.

Proposed action (perform the reload manually)

If you do not want to make any changes to the data connection, you can perform manual reloads, instead of using a task.

Proposed action (change from SQL to Direct Discovery tables)

When you use SSO together with Direct Discovery tables, you will be able to reload the app with a task.

User locked out when a REST data connection is used with a user account

Possible cause

If you set up your REST data connections with a regular user account and not a service account available in your AD/LDAP/user directory, the maximum number of parallel sessions for a single user account (5) will be consumed, and the user will be temporarily locked out.

Proposed action

Use a service account instead of a user account, and do not allocate any user/professional/analyzer access to that account.

A task is not executed

Possible cause

The task status is not **Success**.

Proposed action

On the tasks overview page in the QMC, click 🛈 in the status column to display a summary of the execution steps.

You can also check the log file at this location: *%ProgramData%\Qlik\Sense\Log\Scheduler*.

Reload is not working

There is more than one possible cause when the reload does not work.

Reload was unsuccessful

I clicked **Reload now** on an app but the reload is not working.

Possible cause

The task status is not **Success**.

Proposed action

Check the log file at this location: *%ProgramData%\Qlik\Sense\Log\Script*.

Reload failed in a multi-node environment

In a multi-node environment, I selected an app and clicked **More actions > Reload now**, but the reload failed with the following message: **No worker-nodes found to execute Task**.

Possible cause

The Central scheduler is set to **Manager** only.

Proposed action

Re-trigger the task execution.

On the **Edit scheduler** page, under **Advanced**, change **Type** to **Manager and worker**.

The start page displays a number next to Engine, Repository, Proxy, or Scheduler

Possible cause

The service is down.

Proposed action

Check the log file at this location: *%ProgramData%\Qlik\Sense\Log\<Service>*.

I do not know the name of a mandatory SAML attribute

Possible cause

The name of a mandatory attribute, (userID, userDirectory, or an added mandatory attribute) is not available.

Proposed action

Do the following:

1. Type an arbitrary name as the attribute name.
2. Make an authentication attempt.
   The attempt will fail because the attribute name is incorrect.
3. In the Proxy Audit log, find the row that contains "Existing SAML attributes:".
   You will find the name or friendlyName and Value of all available attributes.
4. Find the name of attribute that you want to use and use that name instead of the arbitrary name that you originally entered.

The following are examples of what you can find in the log:

Existing SAML attributes: [Name='uid', Value='jod'] [Name='givenName', Value='John'] [Name='sn', Value='Davidson'] [Name='cn', Value='John Davidson'] [Name='mail', Value='john.davidson@domain.com']

I cannot change the properties of a user

Possible cause

User properties imported from Active Directory (AD) cannot be changed in the QMC.

Proposed action

Change the property in AD and sync again.

Synchronizing with user directories (page 306)

The user sync is not working

- I cannot synchronize users when clicking **Sync all selected user directories** in the **User directory connectors** overview.
- A scheduled user synchronization task is unsuccessful.

The UDC is not configured

Possible cause

The user directory connector is not **Configured**.

Proposed action

Make sure that the **User directory** name is unique and not blank.

The UDC is not operational

Possible cause

The user directory connector is not **Operational**.

Proposed action

Check the *UserManagement_Repository* log at this location:
%ProgramData%\Qlik\Sense\Log\Repository\Trace. If you remove the source file that a user directory connector is based on, it will not be operational.

The UDC property **Page size of search** value is incorrect

Possible cause

The user directory connector property **Page size of search** is incorrect.

Proposed action

Set the user directory connector property **Page size of search** to '0' (zero).

Table names with capital letters are not recognized in a PostgreSQL database

Possible cause

Table names with capital letters or special characters, such as "." in a PostgreSQL database will generate an error when validated.

Proposed action

Use quotation marks for tables containing capital letters or special characters.

Examples:

`"table.Name", public."Table" (or "Table"), testschema."Table"`

I cannot import an extension

Possible cause

- The extension is not zipped.
- The compressed file has the wrong format.
- The zip file contains invalid files.
- The extension password is incorrect.
- The extension is a duplicate of an already existing extension.

Proposed action

- Make sure the extension file is correctly zipped. You cannot use any other file format for compression than .zip.
- Make sure that the zip file only contains relevant extension files.

- ⚠️ *If you import an extension that already exists in QMC, when prompted, replace the existing file with the new one by clicking **Replace**, or click ✕ to cancel.*

I have deleted a .lock file and can no longer open my app

Possible cause

Each app in the *...\Sense\Apps* folder has a .lock file, and if that file is deleted, the app cannot be opened.

Proposed action

Restart the Qlik Sense Repository Service. A new .lock file is generated for the app.

- ℹ️ *The lock files are used for coordinating the locking of the qvf files. A thread that wants to read from a qvf file must wait until the thread that is writing (and holds the exclusive lock) has finished. Similarly, if a thread wants to have an exclusive lock, it must wait until the threads that are reading from the file are finished.*

A node in a multi-node environment is not getting online

I have recreated a node in the QMC (created, deleted, and then created it again) but the node is not getting online. There is a warning message in the log: "Node disabled (most probable cause is having been unregistered from a cluster). Aborting startup...".

Possible cause

Deleted nodes are not allowed to be restarted and reused in a multi-node environment.

Proposed action

Do the following:

1. Delete the node in the QMC.
2. Uninstall the software from the node.
3. Reinstall the software on the node.
4. Create the node again in the QMC.

Multi-node site: Cannot communicate with a rim node that is outside of the domain

Possible cause

Normally, all nodes in a Qlik Sense multi-node site are within the same Windows domain. If one of the rim nodes is outside of the domain with no DNS available for hostname lookup, the nodes within the domain cannot communicate with the node outside the domain unless the Windows host file on each node is updated.

Proposed action

Do the following:

- All nodes within the domain: Update the Windows host file (typically
  C:\Windows\System32\drivers\etc\hosts) with information on how to find the rim node outside the
  domain.

  Example: <IP address of the rim node outside the domain> <hostname of the rim node>

- Rim node outside the domain:
  - Update the Windows host file with information on how to find all the nodes within the domain.

    Example:

    <IP address of node 1 within the domain> <fully qualified domain name of node 1>
    <IP address of node 2 within the domain> <fully qualified domain name of node 2>
  - Update the Windows host file with information on the host name of the rim node itself so that
    the Qlik Sense services on the rim node can communicate with each other.

    Example: <IP address of the rim node outside the domain> <hostname of the rim node>

Troubleshooting - Navigating in the QMC

This section describes problems that can occur when navigating in the QMC.

Icons in the QMC are not displayed correctly

Possible cause

Qlik Sense site is not listed as a trusted site.

Proposed action

Add the QMC site as a trusted site for Microsoft Edge.

Do the following:

1. In the Control Panel, select **Internet options**.
2. Select the **Security** tab.
3. Click **Trusted sites**.
4. Click **Sites**.
5. Enter the website address for the QMC in the text box and click **Add**.
6. Click **Close**.

The icons are correctly displayed.

Error message: **Untrustworthy Proxy SSL-connection/-certificate**

The browser displays **the Proxy SSL-connection/-certificate is untrustworthy!**, and asks if the user wants to make an exception and trust the certificate authority.

Possible cause

The browser does not recognize the root certificate as trustworthy, because it is not a known certificate authority, such as Thawte or VeriSign.

Proposed action

Do the following:

1. Accept making an exception and trusting the certificate authority by answering **Yes** to the question.
2. Verify that you have installed a public SSL certificate (on server), because you need this to be able to use the default Qlik Sense certificate.

Changing a proxy certificate (page 499)

Error message: **404 Not found**

Possible cause

The URL refers to a non-existent resource.

Proposed action

Modify the URL.

Troubleshooting - Designing access control

This section describes problems that can occur when designing access control in the QMC.

I cannot create a security rule for my user directory connector

Possible cause

You are trying to use the user directory connector's value for **Name** in the security rule.

Proposed action

You must use the user directory connector's value for **User directory** in the security rule.

I suspect that a user can access a stream that should not be accessible

Possible cause

One or more security rules include access rights for the user who is requesting access.

Proposed action

Make the following audit query to find out which streams the user can access. Disable or edit the security rules, if necessary.
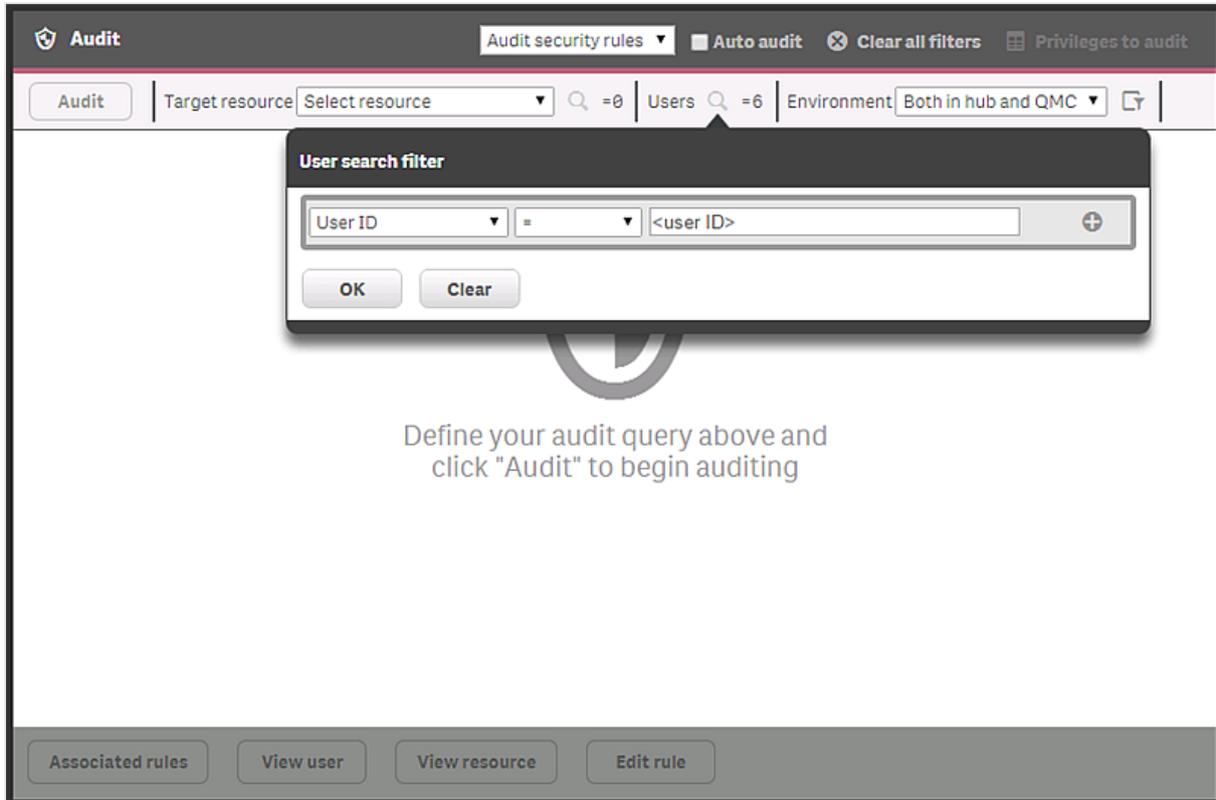
App access problems related to security rules

Badly designed custom security rules can result in the following problems:

- Users cannot open apps that they should be able to open.
- Users can open apps that they should not be able to open.

Possible cause

One or more custom security rules are not working as they should resulting in excessive permissions or lack of permissions.

Proposed action

Follow the methods described here: Troubleshooting Qlik Sense Enterprise Security Rules

Troubleshooting - General

This troubleshooting section presents general problems that are not primarily related to the QMC.

The Search subfolder to Apps has grown considerably

The Search folder that is present in *%ProgramData%\Qlik\Sense\Apps* has grown considerably and can potentially fill the server's hard drive.

Possible cause

The Search folder is used to store cached app searches, and there is no automatic deletion of files.

Proposed action

Delete the Search folder.

1.13   Precedent based learning for Insight Advisor

Insight Advisor can analyze an app to see how fields are used to create charts. The QlikPrecedents Service analyzes apps whenever **Insights** is opened in the app. The service examines the use of data fields and master items in charts. This teaches precedents for making aggregations, dimensions, and measures for the data model of the app. In unpublished apps, Insights can use precedents learned from published apps and from user feedback in the app.

App analysis does not examine the data in fields, only the data tables and field names and how they are used. App analysis is enabled for all published apps with Insight Advisor. You can disable Insight Advisor in a published app if you do not want Insight Advisor to learn precedents from that app.

1.14   Configuring Qlik Insight Advisor Chat in Qlik Sense Enterprise on Windows

Qlik Insight Advisor Chat is a chat-based interface that lets you ask questions using natural language to discover insights in your data. It is available in Qlik Sense Enterprise on Windows, and you can integrate Qlik Insight Advisor Chat to third-party tools such as Slack and Microsoft Teams so users can get insights from their Qlik Sense apps directly in their communication platform.

> *You must have a valid Qlik product license that includes a subscription to Qlik Insight Advisor Chat. For more information about your product license, contact your site administrator.*

> *To include Qlik Sense apps in Qlik Insight Advisor Chat, see Making apps available in Insight Advisor Chat. Once you enable apps be to included, see Exploring apps with conversational analytics for information on how to use Qlik Insight Advisor Chat from the Qlik Sense hub.*

Creating access control for Qlik Insight Advisor Chat

The Qlik Sense admin user can limit access to Qlik Insight Advisor Chat by creating security rules in the QMC.

> ⓘ *The security rules only apply to user and group access in the Qlik Sense hub. Access through third-party communication tools like Slack and Microsoft Team is not affected by security rules in the QMC.*

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*

2. Select **Security rules** on the QMC start page or from the **Start** ▼ drop-down menu.

3. Click ➕**Create new** in the action bar.
   A split page is displayed, with the editing pane to the left (with all the properties) and the audit page to the right.

4. Under **Identification**, give the rule a name and a description.

5. Under **Basic**, enter the following resource filter: *IAChat_** and select **Read** as the action.
   - To provide access for all named users, enter a condition *((user.name!=""))*.
   - To restrict access to a specific user named user1, enter a condition *((user.userId="user1"))*.

6. Under **Advanced**, click **Validate rule** to verify that the rule is set up correctly.

> ⓘ *The rule should be applied when you refresh your browser. The root admin always has access to Qlik Insight Advisor Chat.*

To learn more about designing access control and security rules in the QMC, see [Creating security rules](#).

Configuring Qlik Insight Advisor Chat for external channels

You can connect the Bot Channel Service to third-party tools, such as Slack and Microsoft Teams, to allow users to get insights about Qlik Sense data directly from third-party communication tools.

Prerequisites

- Your Qlik Sense users must have an email address linked to their userId.
- You have access to a Microsoft Azure portal, and you have permissions to create Azure bots.

> ⓘ *The bot and the service do not need to be hosted on Azure, however, the broker for the Microsoft Teams bot and Slack bot uses Microsoft Azure.*

- You have access and permissions to configure communication endpoints on Slack or Microsoft Teams, or both.

Configure a virtual proxy

The first step in configuring Qlik Insight Advisor Chat for external channels is to create a virtual proxy in the QMC. The virtual proxy provides a communication network between the Bot Channel Service and the other Qlik services.

Do the following:

1. Log in to the QMC. By default, the QMC address is *https://<QPS server name>/qmc*.
2. Select **Virtual proxies**.
3. Select **Create new**.
4. On the **Edit virtual proxy** configuration page, select **Identification**, **Authentication**, **Load Balancing**, and **Advanced**, from the right-hand **Properties** menu.

Properties

✔ Identification

✔ Authentication

✔ Load balancing

✔ Advanced

Integration

Client authentication link

Tags

Custom properties
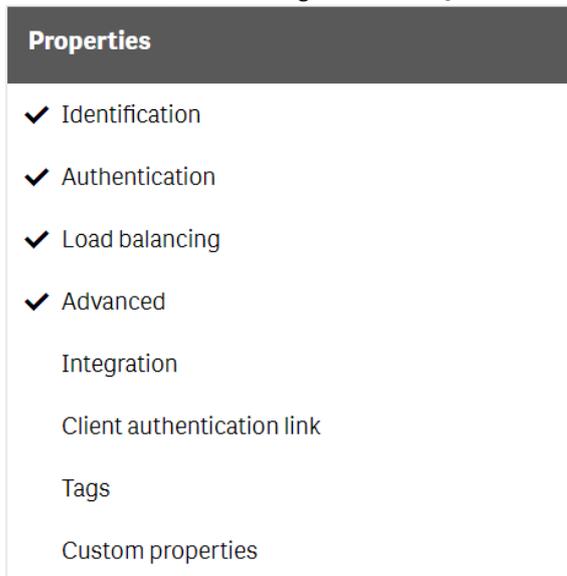
5. Enter the following details:
   Indentification

Description	jwt
Prefix	jwt
Session inactivity timeout (minutes)	30
Session cookie header name	X-Qlik-Session-jwt

Authentication

Anonymous access mode	No anonymous user
Authentication method	JWT
JWT certificate	Paste your JWT certificate.

> *Use the server.pem certificate located in your*
> *%ProgramData%\Qlik\Sense\Repository\Exported Certificates\.Local*
> *Certificates\server.pem.*

| JWT attribute for user ID | userId |
| JWT attribute for user directory | userDirectory |

Load Balancing

Under **Load Balancing**, select **Add new server node**, then select **Central**.

Advanced

Under **Host allow list**, select **Add new value**. Add *localhost*, and any other server that will connect to the Bot Channel Service.

> *All other fields can be left blank or select the default values.*

6. Click **Apply** and agree to restart the Virtual Proxy Service.
7. From the right-hand **Properties** menu, under **Associated items**, select **Proxies**.
8. Click **Link**.
9. Select the central node, then click **Link**.

When you complete the virtual proxy configuration, you can then create a Microsoft Azure Web App Bot. This bot relays communication between the communication platform and the Bot Channel Service.

Creating a Microsoft Azure Bot Service

Once you have configured a virtual proxy, you need to create a Microsoft Azure Bot Service. The Bot Service provides communication between users and the external channels.

> *Before you begin, we recommend that you open a notepad to record usernames, passwords, IDs,*
> *and tokens that you need to complete the configuration. Copy the following template to a notepad:*
> ```
> ====Microsoft Azure Bot Service====
> Bot handle =
> MicrosoftAppId =
> MicrosoftAppPassword =
> ================================
> ================================
> ```

Do the following:

1. Log in to your [Microsoft Azure portal](#).

2. Type *Bot Services* in the search bar. Under **Services**, select **Bot Services**.
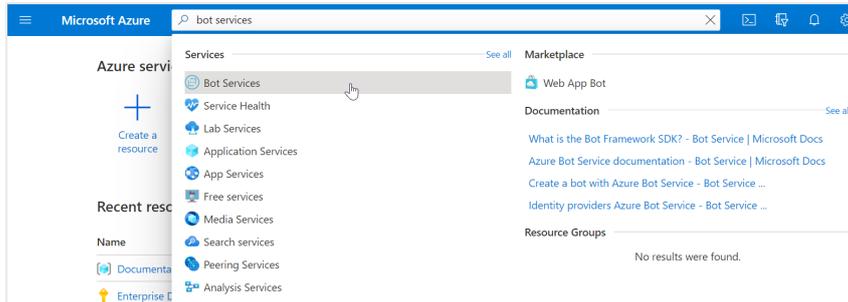
3. Click **Create**.

4. Select **Azure Bot** from the list.

5. Click **Create**.

6. Create an Azure Bot with the following parameters:

Parameters	Value
Bot handle	Enter a unique name.
Subscription	Select your subscription.
Resource group	Select your resource group.
Data residency (preview)	Global
Pricing tier	Select the appropriate pricing tier.
Microsoft App ID	Type of App: Select **Multi Tenant**. Creation Type: Select **Create new Microsoft App ID**.

   When finished, click **Review + Create**.

7. When the Azure Bot validation is complete, click **Create**.
   You are redirected a deployment page. Wait for the deployment to complete.

8. On the left-side menu, click **Inputs**.

9. From the **Inputs** page, copy the **Bot handle** and the **msAppId** (Microsoft App ID) to your notepad.

10. Go to the **Overview** page and click **Go to resource**.

11. On the left-side menu, go to **Settings** > **Configuration**.

12. Enter the messaging endpoint and click **Apply**.
    The messaging endpoint is the URL to the Qlik Sense central node server. Include the messaging endpoint. For example: *https://qliksense.domain.com/api/messages*.

13. To create a client secret, next to the **Microsoft App ID**, click **Manage**.

    a. In the **Client secrets** section, click **New client secret**.

    b. Enter a description and select the expiry date, and then click **Add**.

    c. In the **Value** column, copy the value (MicrosoftAppPassword) to your notepad.

Your Azure Bot is now ready to configure a communication channel.

Configuring the communication channel for Microsoft Teams

After you create a Microsoft Azure Bot, you can enable the Microsoft Teams channel. This lets you query your Qlik Sense data directly from Microsoft Teams using natural language queries.

Do the following:

1. Log in to your Microsoft Azure portal.
2. Click your **Resource group** to see the list of resources.
3. Click the Azure Bot you created earlier.
4. Under **Bot Management**, select **Channels**.
5. Under **Add a featured channel**, select **Microsoft Teams**, then click **Save**.
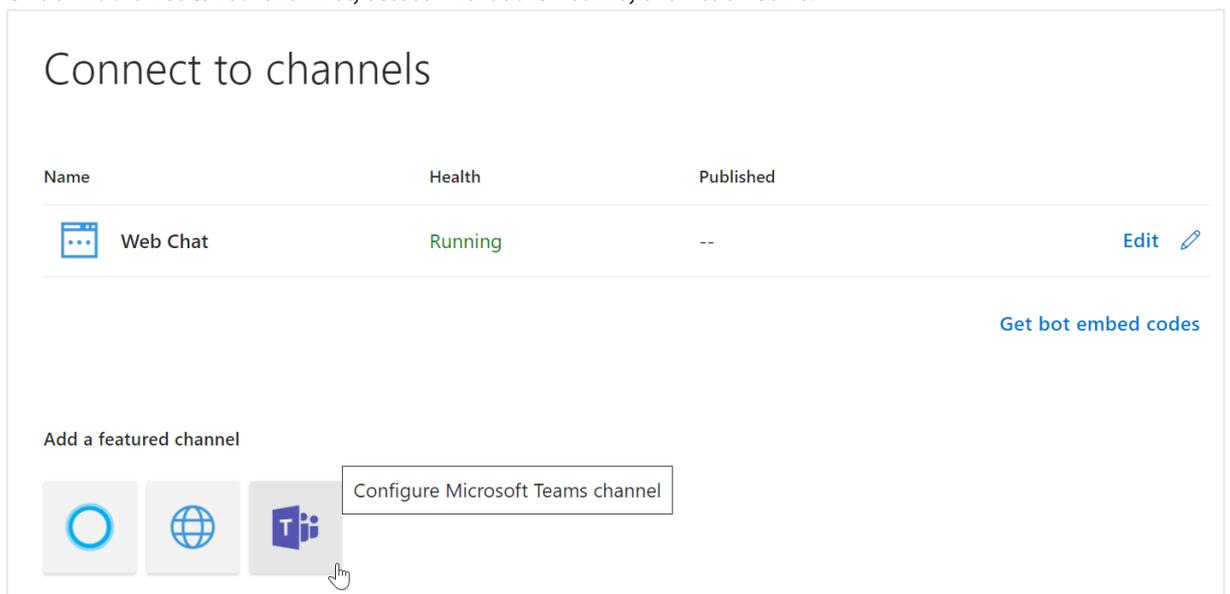
6. Select the appropriate messaging type, then click **Save**.

> *You have to accept the Terms of Service to continue.*
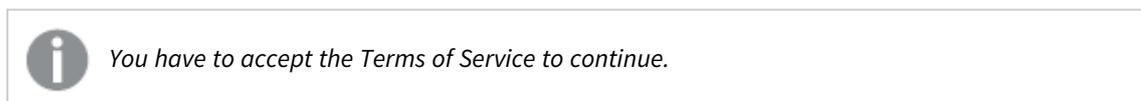
Now you have a communication channel between Microsoft Teams and the Microsoft Azure Bot.

Starting a conversation in Microsoft Teams

Now that a communication channel is set up, you can begin to use Teams to get insights from your Qlik Sense apps.

Do the following:

1. Open Microsoft Teams.

2. Click **New Chat**.

3. In the **To:** field, enter the **MicrosoftAppId** that your copied to the notepad.

   To: ba101750-■■■■-■■■■-■■■■-54f103142a87

   <••>   insightchat

4. Now you can use your Team chat to make queries about your Qlik Sense apps.

Now that you have configured the communication channel, you can configure the Bot Channel Service.

Configuring the communication channel for Slack

After you create a Microsoft Azure Bot, you can enable the Slack channel. This lets you query your Qlik Sense data directly from Slack using natural language queries.

> *Before you begin, we recommend that you open a notepad to record usernames, passwords, IDs, and tokens that you need to complete the configuration. Add this section to the bottom of your notepad:*
> ```
> ====Slack details====
> Slack bot URL =
> Bot User OAuth Access Token =
> Client ID =
> Client Secret =
> Signing secret =
> =================================
> =================================
> ```

Creating a Slack app

Do the following:

> *You must have Slack administrator privileges to use the Slack API.*

1. Go to Slack API.

2. In the top navigation bar, click **Your Apps**.

3. Click **Create an App**.
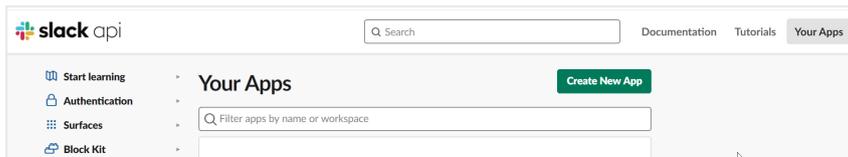
4. Enter an **App Name** and choose the **Development Slack Workspace**, then click **Create App**.

Adding a redirect URL

1. Under **Features** in the left-side menu, select **OAuth & Permissions**.

2. Click **Add New Redirect URL**.

3. Enter *https://slack.botframework.com*, then click **Add**.

4. Click **Save URLs**.

5. Scroll down to the **Scopes** section. Add the following **Bot Token Scopes**:

Creating a Slack bot user

1. Under **Features** in the left-side menu, click **App Home**.

2. Toggle on **Always Show my Bot as Online**.

3. Scroll down and select **Allow users to send Slash commands and messages from messages tab**.

> *In this section, verify or edit your display name and default name.*

Subscribing to Slack bot events

1. Under **Features** in the left-side menu, click **Event Subscriptions**.

2. Toggle on **Enable Events**.

3. In the **Request URL** field, enter the Azure Bot URL you saved to your notepad.

> *The URL should be https://slack.botframework.com/api/Events/{Bot handle}, where {bot handle} is your Azure Bot handle.*

4. Scroll down to **Subscribe to Bot Events** and add the following user events, then click **Save**.
   - member_joined_channel
   - member_left_channel
   - message.channels
   - message.groups
   - message.im
   - message.mpim

Configuring interactive components

1. Under **Features** in the left-side menu, select **Interactive Components**.

2. Toggle on **Interactivity**.

3. In the **Request URL** field, enter *https://slack.botframework.com/api/Actions*, then click **Save Changes**.

Installing the application

1. Under **Settings** in the left-side menu, select **Install App**.

2. Click **Install App to Workspace**.

3. In the permission request window that opens, click **Allow**.

4. Copy the **Bot User OAuth Access Token**.

> Save the OAuth token to your notepad to use later when configuring the Bot Channel Configuration App.

5. Under **Settings** in the left-side menu, select **Basic Information**.

6. Scroll down to **App Credentials**.

7. Copy your **Client ID**, **Client Secret**, and **Signing Secret**.

> Save these to your notepad.

Configure Slack Bot with Azure

Do the following:

1. Log in to your [Microsoft Azure portal](#).

2. Click your **Resource group** to see the list of resources.

3. Click your **Azure Bot** to configure it.

4. Under **Bot Management**, select **Channels**.

5. Under **More channels**, select **Slack**.

6. In the **Client ID**, **Client Secret**, and **Signing Secret** fields, enter the values you saved earlier, then click **Save**.

7. In the permission request window that opens, click **Allow**.

Now that you have configured the communication channel, you can configure the Bot Channel Service.

Configuring the Bot Channel Service

The Bot Channel Service is disabled by default. To enable it, you must configure a parameter in the *services.config* file.

Setting up user configuration for Bot Channel Service

1. Log on to your Qlik Sense Enterprise on Windows server.
2. Navigate to *%ProgramFiles%\Qlik\Sense\BotChannelService\install*.
3. Run the *ChannelConfig.bat* file.
   When you run the batch file (.bat), you are prompted to enter the relevant chat bot parameters:

Parameter	Mandatory	Default value	Description
microsoftAppId	Yes		The Microsoft App ID generated when you created the Azure Web App Bot.
microsoftAppPassword	Yes		The Microsoft App password generated when you created your Azure Web App Bot.
slackBotToken	No	N/A	The Bot User OAuth Token generated when you created your Slack app. Leave empty if you do not want to connect Slack.
qlikRootUserId	Yes		The user's Qlik Sense user ID. It is listed under **Users** in the QMC.
qlikRootUserDir	Yes		The user directory that the user comes from. It is listed under **Users** in the QMC.
virtualProxyPrefix	Yes		The virtual proxy prefix from when you created the Qlik Sense virtual proxy.
externalURL	No	N/A	The Qlik Sense public URL. The URL can include the virtual proxy prefix, for example: *insight.qlik.com/{vp_prefix}*. ⓘ *Do not add the HTTPS to the URL.*
disableParsingInfo	No	*N*	*Y* if you want to disable parsing information.
emailInAttribute	No	*Y*	*N* if the user email is available in the **Name** or **User ID** property. For example, in the image below, the email for John is in **UserID** and the email for Anna is in **Name**. *Y* if the email address is defined in a different property.
emailPropertyName	No	*email*	If you entered *N* for **emailInAttribute**, enter *name* or *userid* to specify in which property the email is located.

Parameter	Mandatory	Default value	Description
			If you entered *Y* for **emailInAttribute**, specify the property name used for the email address. If you do not specify a property name, the default value is used. For example, the email address for Anna is in a custom property **custom_field**. The email for John is in the default property **email**.

User: Anna		User: John	
Property	**Value**	**Property**	**Value**
blacklisted	false	blacklisted	false
custom_field	qlikuser2@qlik.com	deleteProhibited	false
deleteProhibited	false	email	qlikuser1@qlik.com
inactive	false	inactive	false
name	Anna	name	John
removedExternally	false	removedExternally	false
userDirectory	UDC_BDM	userDirectory	UDC_BDM
userId	qlikuser2	userId	qlikuser1

> *You see a **configuration successful** message when complete. If you receive an error message, run the bat file again.*

Enabling the chat bot service

> *In a multi-node site, this must be done on the central node.*

Do the following:

1. Navigate to *%ProgramFiles%\Qlik\Sense\ServiceDispatcher*.

2. Open the *services.config* file in a text editor.

3. Locate the bot-channel-service section, then comment out the `disabled=true parameter`. It should look like the following example:
```
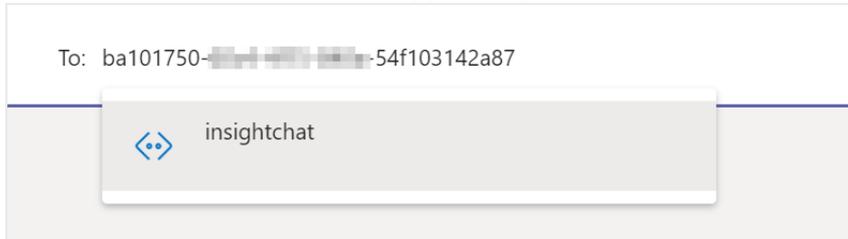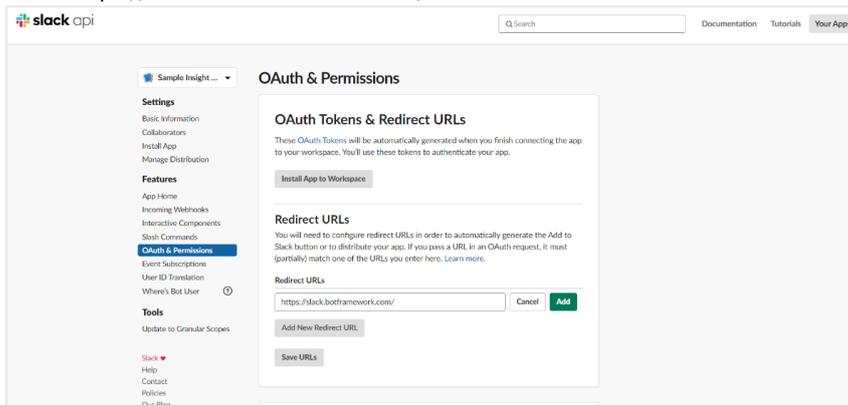[bot-channel-service]
//Disabled=true
Identity=Qlik.bot-channel-service
DisplayName=Bot Channel Service
ExePath=Node\node.exe
Script=..\BotChannelService\index.js
```

4. Save the file.

5. Restart the Qlik Sense Service Dispatcher.

6. Open Insight Advisor Chat by clicking on the **Ask Insight Advisor** button.
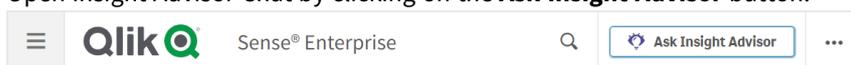
7. Verify that the chat feature opens to the following window.
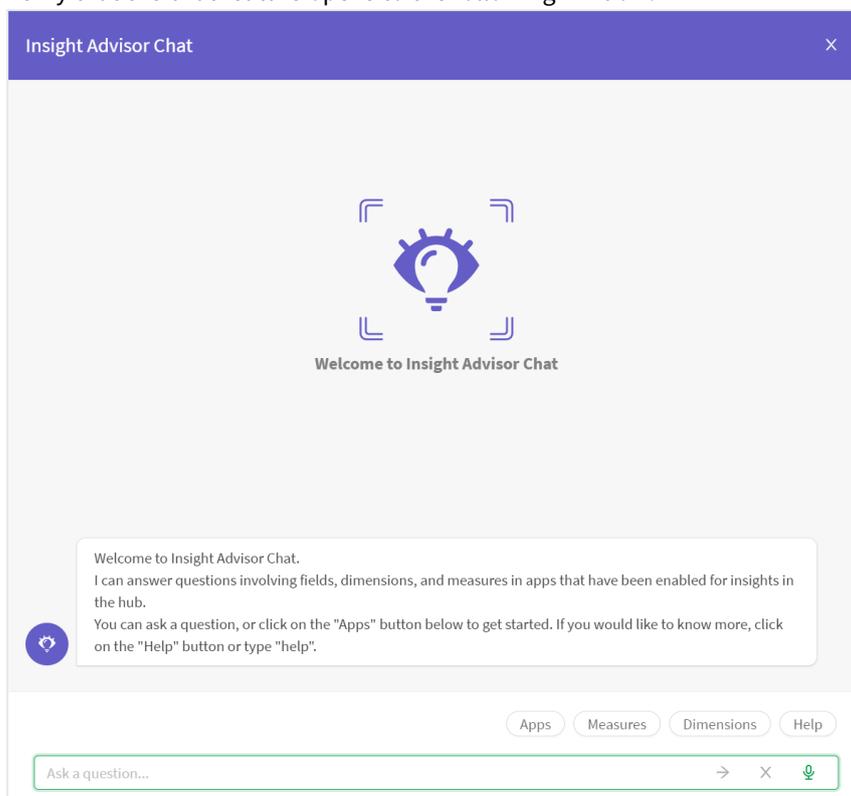
> ⓘ *If it is not working, verify that you have correctly set up the security rules in the QMC. See Configuring Qlik Insight Advisor Chat in Qlik Sense Enterprise on Windows (page 641) for more information.*

8. Restart the Qlik Sense Proxy Service.

Resource utilization in a multi-node deployment

A multi-node deployment consists of a central node and one or more rim nodes. When deploying Insight Advisor Chat in a multi-node deployment, the NLP runtime stack (nl-parser, nl-broker, nl-app-search, data-prep) is part of the service dispatcher which is deployed on each node in a multi-node site.

Requests that are going through Insight Advisor Chat on the central node are handled by the NLP runtime stack that is deployed on the central node. Requests that happen on a rim node are handled by the NLP stack that is running on that same rim node. There are no load balancing rules for the NLP runtime stack and if any part of the NLP stack is disabled on a node, then requests coming through Insight Advisor Chat on that node will fail.

2   Monitoring a Qlik Sense Enterprise on Windows site

The Qlik Management Console (QMC) provides apps for monitoring system performance and usage on Qlik Sense Enterprise on Windows server nodes and for monitoring license usage.

The *Operations Monitor* and *License Monitor* apps are accessed from the QMC start page. The **Monitoring apps** link under **GOVERNANCE** in the navigation panel takes you to the **Monitoring apps** stream where you can start the individual apps.

The *Operations Monitor* app provides information about hardware utilization, such as server memory and CPU usage, active users, and reload task activity. It also provides summary and detailed information about errors, warnings, and log activities in the Qlik Sense server environment that can be used for troubleshooting.

The *License Monitor* app tracks license usage, and it facilitates monitoring changes to license allocation.

Additional *Monitoring apps* can be imported from *%ProgramData%\Qlik\Sense\Repository\DefaultApps*. See *Importing new Monitoring apps (page 658)*.

The additional *Monitoring apps* include:

- The *Log Monitor* app presents nearly all log data available and enables trend analysis and troubleshooting.
- The *Sessions Monitor* app shows log data about usage of apps.
- The *Reloads Monitor* app presents detailed information about reload data, both from the QMC and apps open in the hub.
- The *Sense System Performance Analyzer* app displays Qlik Sense performance across all nodes.
- The *Sense Connector Logs Analyzer* app provides insights into usage and errors of specific Qlik connectors.
- The *App Metadata Analyzer* app provides a holistic view of all your Qlik Sense apps, including granular level detail of an apps data model and its resource utilization.

The Monitoring apps provide historical status and trending data. Real-time status is provided by QMC management resources. Actions taken in response to issues revealed by the Monitoring apps are also performed in the QMC.

2.1   Configuring the Monitoring apps

All installations of Qlik Sense require some level of configuration of the Monitoring apps.

Configuring single node environments

Do the following:

1. Update the data connections *ArchivedLogFolder* by replacing *C:\ProgramData\Qlik\Sense* with the fully-qualified domain name (FQDN) path to the shared folder for Qlik Sense: *\\<FQDN>\<QlikShare>\ArchivedLogs*.

2. Update the `monitor_apps_REST_` data connections by replacing *localhost* in the connection strings URL and *trustedLocation* parameters with the FQDN of the node.

3. The Monitoring apps require Windows authentication to be used on the virtual proxy it uses to connect. If this is not the default virtual proxy, replace *\qrs* with *\<prefix>\qrs* where *<prefix>* is the prefix of a virtual proxy with Windows authentication enabled.
See: *Default virtual proxy with prefix (page 658)*

Configuring multi-node environments

1. Update the data connections *ServerLogFolder*, by replacing *C:\ProgramData\Qlik\Sense\Log* with the FQDN path to the central node: *\\<FQDN>\<UNC_Share>\Log*.

2. Update the `monitor_apps_REST_` data connections by replacing *localhost* in the connection strings URL and *trustedLocation* parameters with the FQDN of the node where the central Qlik Sense repository service is running.

3. If the virtual proxy uses a prefix, the `monitor_apps_REST_` data connections must be updated to include the prefix used.
See: *Default virtual proxy with prefix (page 658)*

4. Share the Qlik Sense log folder (*C:\ProgramData\Qlik\Sense\Log*) on each rim node.

5. Update the data connections *ArchivedLogFolder* by replacing *C:\ProgramData\Qlik\Sense* with the fully-qualified domain name (FQDN) path to the shared folder for Qlik Sense: *\\<FQDN>\<QlikShare>\ArchivedLogs*.

6. Add a new data connection to the *Log* folder for each rim node. This can be accomplished by opening an app, accessing the data load editor, and creating a new data connection. If you have five rim nodes, you need to create five data connections.
For example, the data connection for rim1 points to folder *\\rim_node_1\<UNC_Share>\Log* and is called rim1.

7. Rename the new data connections in the QMC to remove the *(username)*, which is appended to the data connection name. Example: *rim1 (user_183)* is changed to *rim1*.

8. Update the load script of the *Operations Monitor* in section *logFolderList* on line 5 by adding the names of all the new data connections created in step 6 and 7.
Do the following:

   i. Duplicate the *Operations Monitor* app in the QMC.

   ii. Open the duplicate app in the Qlik Sense hub.

   iii. Edit the load script: Each new data connection name needs to be enclosed in single quotes (') and separated by a comma.
Example: *FOR each node in 'ServerLogFolder','rim1','rim2'*.

   iv. Save the app.

v. Replace the existing *Operations Monitor* app by publishing the duplicate app to the **Monitoring apps** stream and selecting **Replace existing app**.

9. Perform step 8 in the *License Monitor*.

> *If you encounter problems when the central node is not a reload node, see: The Monitoring apps fail to reload in a multi-node environment (page 675).*

Default virtual proxy with prefix

For the *Operations Monitor* and *License Monitor* to reload correctly when the default virtual proxy uses a prefix, you need to manually add the prefix to the `qrs` data connections. The default URL is *https://<FQDN>/qrs/app/full*, where the FQDN refers to the node where the repository resides. If the virtual proxy prefix is "qlik", the URL needs to be as follows: *https://<FQDN>/qlik/qrs/app/full*.

The following data connections need to be updated:

- `monitor_apps_REST_app`
- `monitor_apps_REST_appobject`
- `monitor_apps_REST_event`
- `monitor_apps_REST_license`
- `monitor_apps_REST_license_analyzer`
- `monitor_apps_REST_license_login`
- `monitor_apps_REST_license_overview`
- `monitor_apps_REST_license_professional`
- `monitor_apps_REST_license_user`
- `monitor_apps_REST_task`
- `monitor_apps_REST_user_condensed`

Importing new Monitoring apps

The additional Monitoring apps: Log Monitor, Reloads Monitor, Sessions Monitor, Sense System Performance Analyzer, Sense Connector Logs Analyzer and App Metadata Analyzer are not by default available in the QMC. You need to import them to make them appear in the QMC.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. From the QMC start page, open **Apps**.
3. Click ➕ **Import** in the action bar.
4. Click **Choose File** and navigate to *%ProgramData%\Qlik\Sense\Repository\DefaultApps*
5. Select the app to import and click **Import**.
    The app is imported and can be published to the *Monitoring apps* stream.
6. Repeat steps 2-4 for the remaining apps.

> ℹ️ *The Sessions Monitor, Log Monitor, Reloads Monitor, Sense System Performance Analyzer, Sense Connector Logs Analyzer and App Metadata Analyzer apps are not automatically updated during a Qlik Sense upgrade. You must manually import them after an upgrade.*

Customizing the apps

It is possible to extend the Monitoring apps with visualizations you find useful in your particular environment. The Monitoring apps provide assets panels with the dimensions and measures they use. You can use those dimensions and measures to create customized visualizations on separate sheets that you can add to the apps.

The assets panels may also include extra visualizations that are not used on any of the apps' sheets, but which can be useful in a particular environment.

> ℹ️ *Data in the Operations Monitor and License Monitor is not live, it is updated when the apps are reloaded. Reload frequency can be changed by editing the triggers for the task.*

2.2   Starting the Monitoring apps from the QMC

The apps for operations and license monitoring are started by going to the QMC start page. The Monitoring apps are accessed from the **Monitoring apps** link under **GOVERNANCE** in the navigation panel.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Allocate user access to users who will use QMC apps or allocate login access to groups whose users can use apps with login passes.
3. Click the **Monitoring apps** link under **GOVERNANCE** in the navigation panel.
   This takes you to the **Monitoring apps** stream where you can start the individual apps.

> ℹ️ *The first time the Monitoring apps are started, they may not contain data to display because they have not yet been reloaded. In the case of the License Monitor, it has no data until at least one license token has been allocated or an access denial has taken place, so it might display no data even if it has been reloaded. To get fresh data for the apps before their next scheduled reload, return to the Apps overview in the QMC and click **More actions > Reload now**.*

2.3   Upgrading the Monitoring apps

Upgrading from Qlik SenseFebruary 2019 or earlier to Qlik SenseApril 2019 or later

In Qlik SenseApril 2019, the new `monitor_apps_REST_user_condensed` data connection was introduced. Make sure that the new `monitor_apps_REST_user_condensed` data connection is assigned to the same user (same user ID and password) as the other `monitor_apps_REST` data connections.

Also ensure that the URL in the connection string for the new `monitor_apps_REST_user_condensed` data connection has been updated to use the same hostname, and if applicable virtual proxy prefix, as set in the other `monitor_apps_REST` data connections.

> *The user who is assigned to the* `monitor_apps_REST_` *data connections must be rootadmin.*

Upgrading from Qlik Sense 3.2.x to Qlik Sense June 2017

When you upgrade from Qlik Sense 3.2.x to June 2017, or later releases, eight new REST data connections are introduced (`monitor_app_REST_`). The existing `qrs_` data connections will no longer function due to functional changes to the REST connector. These `qrs_` data connections therefore can be removed.

Upgrading from Synchronized persistence to Shared persistence

If you upgrade from Synchronized persistence to Shared persistence, you may need to move the archived logs from the earlier version to the Shared persistence ArchivedLogs share.

Do the following:

1. Create a new folder called *OlderLogs* (or the name of your choice) in the Service Cluster *ArchivedLogs* folder. You can find this in QMC > Service cluster.
2. Move or copy the following subfolders from *Archived Logs* (in the older version) to this new *OlderLogs* folder in step 1.
   a. Default *Archived Logs* folder is *c:\programdata\qlik\sense\repository\archived logs*.
   b. Copy the following folders to the new location:
      i. Engine
      ii. Repository
      iii. Proxy
      iv. Scheduler
      v. Printing

> *The reason to just move/copy these folders is that other log folders (like AppMigration and Script) are not loaded into the Monitoring apps and can be quite large in size.*

3. Verify in the *ArchivedLogs* folder (for the service cluster) that this *OlderLogs* folder is present, as well as folders for each node in your environment.

4. Update the *ArchivedLogsFolder* data connection in QMC to point to the *ArchivedLogs* folder (as defined in QMC > ServiceCluster).

5. Versions prior to 7.x of the governance*.QVDs located in *c:\Programdata\Qlik\Sense\Log* can be removed if wanted (optional).

6. Reload the new Monitoring apps from the QMC.

2.4   Operations Monitor

The *Operations Monitor* loads service logs to populate charts covering performance history of hardware utilization, active users, app sessions, results of reload tasks, and errors and warnings. It also tracks changes made in the QMC that affect the *Operations Monitor*.

> ℹ️ *For a more detailed description of the sheets and visualizations, visit the story About the Operations Monitor that is available from the app overview page, under **Stories**.*

The log files are located in *%ProgramData%\Qlik\Sense\Log\Repository\Trace*.

With the *Operations Monitor*, you can track system performance and investigate activity that might adversely affect it. For example, by analyzing reload tasks and sessions, you can find bottlenecks that might be alleviated by rescheduling reloads or redistributing sessions. Or you can use the **QMC Change Log** sheet to review changes that might explain changes in system performance.

Operations Monitor sheets

The *Operations Monitor* sheets display Qlik Sense performance on the current node, and, when properly configured for multi-node (as described in *Configuring multi-node environments (page 657)*), the app includes information across all nodes.

Operations Monitor sheets

24-Hour Summary	Displays hardware utilization, active users, active apps, and reload tasks over the last twenty-four hours.
Performance	Allows the user to select a time period over which to display hardware utilization, concurrent users, and concurrent apps.
Task Overview	Provides a statistical overview of the success, duration, and failure of reload tasks.
Task Planning	Provides details about reload count, reload CPU spent, and task dependencies.
Task Details	Provides details about the success and failure of individual app reloads, including execution details about duration and start and end times.
Session Overview	Provides summary information about apps, app sessions, and app users over selected periods to show which users use which apps when.

Session Details	Provides details about individual user and app sessions, including number, average duration, days since last session, start and end times, reasons for ending sessions, and the type of client on which the app was run.
Export Overview	Provides summary information about apps, app objects, and app users to show which users export which app objects when.
Sheet Usage	Provides summary and detailed information about users accessing sheets – and which sheets in which apps are not accessed. The *Unused sheets* measures count the number of sheets within an app which have not been used within the selected time frame. For example, 10 "Unused base sheets last <=30 days" means that 10 sheets have not been used in the last 30 days.
Apps	Provides details about the apps in the Qlik Sense Repository Service (QRS), including name and ID of app objects, owners, publishing, and streams.
QMC Change Log	Displays changes made in the QMC that affect a range of factors from system performance to user access, including changes by QMC resource type, by specific QMC resources, by users who made changes, or by a type of action performed in the QMC.
Export Links for Cloud	Provides details about app links to export to Qlik Sense SaaS, which can then be imported in Qlik Sense SaaS as generic links. To be able to add the links to the cloud hub or upload them to the management console, you must first export the links into a CSV file. See Exporting links into .csv files.
Log Details	Provides details about reloads of the *Operations Monitor*, including the time of reloads, results, error messages and warnings, and log entries.

> *Data in the Operations Monitor is updated when the app is reloaded. Data is not live.*

> *Operations Monitor uses the ProxySessionId from the engine's session logs for deriving its session counts like Sessions Monitor. This effectively gives the proxy session counts, which can be slightly lower than License Monitor and Sessions Monitor session counts due to the way those apps calculates their sessions. Operations Monitor excludes short sessions (less than 40 seconds) that get registered in Sessions Monitor due to their respective design choices.*

2.5   License Monitor

The *License Monitor* loads service logs to populate charts and tables covering token allocation, usage of login and user passes, and errors and warnings.

> *For a more detailed description of the sheets and visualizations, visit the story About the License Monitor that is available from the app overview page, under **Stories**.*

The log files are located in *%ProgramData%\Qlik\Sense\Log\Repository\Trace*.

> ℹ️ *If you have a user-based license with professional and analyzer access, you will instead see figures relevant to that license type.*

License Monitor sheets

The License Monitor sheets display Qlik Sense performance on the current node, and, when properly configured for multi-node (as described in *Configuring multi-node environments (page 657)*), the app includes information across all nodes.

License Monitor sheets

Overview	Displays an overview of unallocated access versus total access, the available and total analyzer capacity (in minutes), summary data about login and user access sessions over the last 7, 28, and 90 days, changes in the allocation of license tokens over the last 7 days, and license usage over time.
User Detail	Allows the user to select a time period over which to display user access pass sessions, the number of users starting sessions, and the individual users starting sessions.
Usage by App	Allows the user to select a time period over which to display the apps for which access passes are being used and the number of tokens consumed by each app.
Timeline	The *Timeline* sheet displays token usage over time so administrators can monitor usage and anticipate future token allocation needs.
User Access History	Allows the user to select a time period over which to display user access pass sessions, the number of users starting sessions, and the individual users starting sessions. ℹ️ *Only valid for token-based license.*
Login Access History	Allows the user to select a time period over which to display login pass utilization, login access users, and denials of login access. ℹ️ *Only valid for token-based license.*
Allocation History	Displays the latest changes and changes over selected times to the allocation of license tokens to login and user access passes.
Usage Snapshot	Overview sheet providing snapshot view of license allocation and historical usage.

Unified Licensing History	Displays the license usage for Qlik Sense and QlikView side by side. *To see the QlikView license usage, the new monitor_apps_qlikview_ logs data connection must point to the folder containing the QlikView Server logs. You update the data connection in the QMC.*
Log Details	Lists servers in the cluster and provides details about license usage entered in server's logs.

Data in the License Monitor is updated when the app is reloaded. Data is not live.

License Monitor uses the combination of ProxySessionId and ObjectId from the repository's AuditSecurity logs for deriving its session counts. If the same proxy session opens multiple apps, this count can appear as slightly higher than other monitoring apps due to their respective design choices. The actual token consumed per user session remains unaffected.

2.6   Log Monitor

The *Log Monitor* loads and visualizes almost all available Qlik Sense log data. This gives you the possibility to discover trends and analyze and troubleshoot issues in your Qlik Sense environment. Compared to the Operations Monitor, the Log Monitor loads more log files, but for a shorter period of history (default seven days).

*For a more detailed description of the sheets and visualizations, visit the story About the Log Monitor that is available from the app overview page, under **Stories**.*

The log files are located in *%ProgramData%\Qlik\Sense\Log\Repository\Trace*.

Importing the Log Monitor app to the Monitoring apps in the QMC

The Log Monitor is not available by default from the QMC. To make it available, you need to import the app.

Follow the instructions in the section *Importing new Monitoring apps (page 658)*

Log Monitor sheets

The Log Monitor sheets display Qlik Sense performance on the current node, and, when properly configured for multi-node (as described in *Configuring multi-node environments (page 657)*), the app includes information across all nodes.

Log Monitor sheets

Overview	Summarizes the activities during the last couple of hours and days and enables you to quickly identify irregularities.
Timeline	The Activity Timeline bar chart gives an overview of the logging activities during the last week. Use the alternative dimensions to see how the measures vary over time and find diverging values that may require investigation.
Trends	Shows a collection of timelines displaying performance (CPU and RAM), usage (apps and users), as well as errors and reload status.
Errors & Warnings	Shows a timeline together with a summary and a detailed view of errors and warnings.
Filters	Contains filter panes with a large number of key fields from the logs. Make selections to make discoveries in your data.
Log Details	Shows errors, warnings, and information log entries for the servers in the deployment.

> *Data in the Log Monitor is updated when the app is reloaded. Data is not live.*

2.7 Reloads Monitor

The *Reloads Monitor* loads and presents log data about reloads. Reload data is collected both from QMC tasks and apps open in the hub. You can see which apps are updated, and details about when, where, and how often they are updated.

> *For a more detailed description of the sheets and visualizations, visit the story About the Reloads Monitor that is available from the app overview page, under* **Stories**.

The log files are located in *%ProgramData%\Qlik\Sense\Log\Repository\Trace*.

Importing the Reloads Monitor app to the Monitoring apps in the QMC

The Reloads Monitor is not available by default from the QMC. To make it available, you need to import the app.

Follow the instructions in the section *Importing new Monitoring apps (page 658)*

Reloads Monitor sheets

The Reloads Monitor sheets display Qlik Sense performance on the current node, and, when properly configured for multi-node (as described in *Configuring multi-node environments (page 657)*), the app includes information across all nodes.

Reloads Monitor sheets

Dashboard	Gives an overview of the reload task history. Get different views by using the alternative dimensions and measures that are available for the Reloads by Hour bar chart and the Reload Count and Duration Trend combo chart.
Task Planning	Shows when tasks are reloaded and the associated duration and failure rate. Use the data to re-schedule reloads and thereby optimize performance.
Reload Summary	Gives detailed information about reload history statistics and recently completed reloads.
Log Details	Shows details about specific log events and times.
Intermediate Details	Presents the intermediate states of a task reload, such as Triggered, Started, and Queued.

> *Data in the Reloads Monitor is updated when the app is reloaded. Data is not live.*

2.8   Sessions Monitor

The *Sessions Monitor* loads and displays log data about users' app sessions.

> *For a more detailed description of the sheets and visualizations, visit the story About the Sessions Monitor that is available from the app overview page, under **Stories**.*

The log files are located in *%ProgramData%\Qlik\Sense\Log\Repository\Trace*.

Importing the Sessions Monitor app to the Monitoring apps in the QMC

The Sessions Monitor is not available by default from the QMC. To make it available, you need to import the app.

Follow the instructions in the section *Importing new Monitoring apps (page 658)*

Sessions Monitor sheets

The Sessions Monitor sheets display Qlik Sense performance on the current node, and, when properly configured for multi-node (as described in *Configuring multi-node environments (page 657)*), the app includes information across all nodes.

Sessions Monitor sheets

Dashboard	Gives an overview of the session activity. Get different views by using the alternative dimensions and measures that are available for the Sessions Over Time bar chart and the User and App Count Trend combo chart.
Session Heatmap	Shows when session activity is at its highest and lowest. Use the data to understand peak usage times or optimal times for server maintenance.

Session Details	Gives a more detailed view of the session activity and helps identifying unused apps and extensive users of apps.
Apps	Shows metadata about apps and app objects.
Log Details	Shows details about specific log events and times.

> *Data in the Sessions Monitor is updated when the app is reloaded. Data is not live.*

> *Sessions Monitor uses the ProxySessionId from the engine's session logs for deriving its session counts like Operations Monitor, which effectively gives the proxy session counts. Sessions Monitor also registers short sessions (less than 40 seconds) that are excluded in the Operations Monitor due to their respective design choices. Therefore, the Sessions Monitor session counts can sometimes lie in between the session counts of Operations Monitor and License Monitor.*

2.9   Sense Connector Logs Analyzer

The *Sense Connector Logs Analyzer* app lets you investigate patterns of activity and errors to troubleshoot connector performance.

The app relies on log files generated by REST connector version 1.7 or later and ODBC connector version 5.12 or later.

Log files from older versions of REST and ODBC connectors may not include the necessary column header names which will cause the *Sense Connector Logs Analyzer* app to fail during reload. It is recommended that these older connector log files are removed or moved to a separate folder.

> *For a more detailed description of the sheets and visualizations, visit the story About the Sense Connector Logs Analyzer that is available from the app overview page, under **Stories**.*

Importing the Sense Connector Logs Analyzer app to the Monitoring apps in the QMC

The Sense Connector Logs Analyzer is not available by default from the QMC. To make it available, you need to import the app.

Follow the instructions in the section *Importing new Monitoring apps (page 658)*

General configuration

No configuration is needed for single-node deployments, but it is possible to modify the days of log history to load in the load script. You can also include Engine, Repository, Scheduler and Proxy logs in the app.

> *The configuration is done in the Configuration section of the load script.*

Days of history

The days of history is set as a variable, **`vu_days_of_history`**, in the load script.

Default is `14` and it is not recommended to exceed 90 days of history due to potential volume of data.

Example:

```
SET vu_days_of_history = 14;
```

Historical data

You can include Sense Engine, Repository, Scheduler and Proxy logs in the app setting the **`vu_load_operations_monitor_qvd`** variable.

This gets the Operations Monitor historical QVD from the ServerLogFolder data connection.

> *You must enter the name of the QVD to load without the .qvd extension.*

Example:

```
SET vu_load_operations_monitor_qvd = 'governanceLogContent_7.10.2_db';
```

Multi-node deployment configuration

Multi-node environments require the creation of new data connections to a shared folder, like **`\\FQDN\CustomData`**, of each node. The data connections are then defined in the **`vu_data_connection_list`** variable in the load script.

> *The configuration is done in the Configuration section of the load script.*

1. Share the `C:\ProgramData\Qlik` folder on each node.

    Example:

    Name the shared folder `Custom Data`.
2. Add a new data connection for each rim node. Use the Fully-Qualified Domain Name (FQDN) of each node.

    Example:

    Create a data connection called `connector_logs_rim2` to point to folder `\\rim_node_2\Custom Data\`.
3. In the QMC > Data Connections section, rename the new data connections created in the previous step to remove the user name which is appended to the data connection name.

Example:

`connector_logs_rim2 (my_domain\my_user1)` should be renamed to `connector_logs_ rim2`.

4. In the QMC > Data connections section, update the Connection string of the **monitor_apps_ connector_logs** data connection, located on the Identification tab, so it uses the FQDN of the central node.

Example:

`\\central_node_name\Custom Data`

> *If user permissions were set on the shared folder, you need to define the User ID and Password fields accordingly. Else leave undefined.*

5. Update the load script to add the data connections created and renamed in the previous steps. The data connections are defined in the **vu_data_connection_list** variable. Each data connection is enclosed within the existing single quotes and separated with a comma.

Example:

`SET vu_data_connection_list = 'monitor_apps_connector_logs,connector_logs_ rim2,connector_logs_rim3';`

6. Save the updated app.
7. Reload the app.
   You can reload the app from the QMC or from the data load editor.

Sense Connector Logs Analyzer sheets

The Sense Connector Logs Analyzer sheets display usage and errors for Qlik connectors across all nodes.

Visit the story *About the Sense Connector Logs Analyzer* for details about the sheets, available from the app overview page, under **Stories**.

> *Data in the Sense Connector Logs Analyzer is updated when the app is reloaded. Data is not live.*

2.10   App Metadata Analyzer

The *App Metadata Analyzer* app provides a dashboard to analyze Qlik Sense application metadata across your Qlik Sense Enterprise deployment. It gives you a holistic view of all your Qlik Sense apps, including granular level detail of an app's data model and its resource utilization.

> *This app requires Qlik Sense version June 2018, or later.*

> For a more detailed description of the sheets and visualizations, visit the story About the App Metadata Analyzer that is available from the app overview page, under **Stories**.

The app fetches data from an application level metadata endpoint: **`http(s)://{server}/api/v1/apps/{GUID}/data/metadata`**

where `{server}` is your Qlik Sense Enterprise server and `{GUID}` is the application ID.

Importing the App Metadata Analyzer app to the Monitoring apps in the QMC

The App Metadata Analyzer is not available by default from the QMC. To make it available, you need to import the app.

Follow the instructions in the section *Importing new Monitoring apps (page 658)*

General configuration

There are two configurations required in the load script: defining the central node host name and the virtual proxy prefix (if your Windows authenticated virtual proxy has a prefix).

> The configuration is done in the Configuration section of the load script.

Central node host name

The central node host name is set as a variable, **`vu_central_node_host_name`**, in the load script.

Default is `localhost`.

Example:

```
SET vu_central_node_host_name = 'my_central_node.domain.com';
```

Virtual proxy prefix

The virtual proxy prefix is also set as a variable, **`vu_virtual_proxy_prefix`**, in the load script.

Example:

```
SET vu_virtual_proxy_prefix = 'my_virtual_proxy_prefix';
```
If you do not use a virtual proxy prefix you leave it blank.

Example:

```
SET vu_virtual_proxy_prefix = '';
```

Optional threshold values configuration

Optionally, you can change the default threshold values. The configuration is done in the Thresholds section of the load script.

```
// Optional Configuration (No need to change these unless you desire)
SET vu_months_in_reload_interval = 3;  // Width of app last reload date for grouping apps in
this app
// Visual Thresholds - change these if you want to highlight specific apps based on these
attributes
SET vAppDiskSizeThreshold = 524288000; // 500 MB
SET vAppRAMSizeThreshold = 1073751824; // 1 GB
SET vRAMToFileSizeRatioThreshold = 6; // RAM / File Size is typically between 4-6x
SET vAppRecordCountThreshold = 10000000; // Number of records in an app
SET vTableRecordCountThreshold = 10000000; // Number of records in a table
SET vFieldValueCountThreshold = 10000000; // Number of field records
SET vFieldCardinalityThreshold = 1000000; // Number of distinct field values
SET vNoOfFields = 150; // Number of Distinct Fields
SET vReloadCPUTimeThreshold = 1800000; // CPU Time spent on last reload (milliseconds);
default = 1,800,000 = 30 Minutes
```

App Metadata Analyzer sheets

Visit the story *About the App Metadata Analyzer* for details about the sheets, available from the app overview page, under **Stories**.

> *Data in the App Metadata Analyzer is updated when the app is reloaded. Data is not live.*

2.11   Troubleshooting - Monitoring a Qlik Sense site

This section describes problems that can occur when monitoring a Qlik Sense site.

The Monitoring apps are not backed up correctly

When upgrading Qlik Sense, the Monitoring apps are not backed up correctly.

Normally, when upgrading Qlik Sense, the existing version number of the Monitoring apps is replaced by the corresponding version number appended to the app name. Then, the latest Monitoring apps are also available under **Apps**.

Possible cause

The upgrade process of the Monitoring apps was unsuccessful.

Proposed action

Manually import the latest apps from *%ProgramData%\Qlik\Sense\Repository\DefaultApps*.

Do the following:

1. In the QMC, open **Apps**.
2. Click **Import** and select License Monitor.qvf from *%ProgramData%\Qlik\Sense\Repository\DefaultApps*. If prompted, do not rename the app.
3. Publish the newly imported License Monitor app to the Monitoring apps stream, replacing the existing License Monitor.
4. Repeat step 2 for the Operations Monitor.qvf.
5. Publish the newly imported Operations Monitor app to the Monitoring apps stream, replacing the existing Operations Monitor.
6. Repeat steps 2 and 3 for Log Monitor, Reloads Monitor, and Sessions Monitor.

I have accidentally deleted the Monitoring apps

I accidentally deleted the Monitoring apps and cannot find them in the QMC.

Possible cause

Accidental or intentional removal of the Monitoring apps.

Proposed action

Do the following:

1. In the QMC, open **Apps**.
2. Click **Import** and select License Monitor.qvf from *%ProgramData%\Qlik\Sense\Repository\DefaultApps*. If prompted, do not rename the app.
3. Publish the newly imported License Monitor app to the Monitoring apps stream.
4. Repeat step 2 and 3 for any of the affected Monitoring apps.

The Monitoring apps have become corrupted

The Monitoring apps have become corrupted and are no longer functional.

Possible cause

Technical failure.

Proposed action

Do the following:

1. In the QMC, open **Apps**.
2. Click **Import** and select License Monitor.qvf from *%ProgramData%\Qlik\Sense\Repository\DefaultApps*. If prompted, do not rename the app.
3. Publish the newly imported License Monitor app to the Monitoring apps stream, replacing the existing, corrupt License Monitor.

4. Repeat step 2 for Operations Monitor.qvf.
5. Publish the newly imported Operations Monitor app to the Monitoring apps stream, replacing the existing, corrupt Operations Monitor.

Reload of the Monitoring apps failed

There is more than one possible cause when the reload fails.

Insufficient administration rights in the QMC

Possible cause

The service account running the Qlik Sense services does not have the required RootAdmin role in the QMC.

Proposed action

For the Monitoring apps to successfully retrieve all data, the service account running the Qlik Sense services needs sufficient privileges. The easiest way to achieve that is to give the service account the role of RootAdmin in the QMC. Alternatively, you can change the data connections to use a different account/user which is RootAdmin.

Reload is performed on rim nodes

Possible cause

The load balancing rule *ResourcesOnNonCentralNodes* causes the reloads to fail on rim nodes.

Proposed action

Edit the load balancing rule *ResourcesOnNonCentralNodes*.

Do the following:

1. From the QMC start page, open **Load balancing rules**.
2. Select *ResourcesOnNonCentralNodes* and click **Edit**.
3. Under **Advanced**, edit the **Conditions**, so that they read as follows:
   `((node.iscentral="false"))`
4. Click **Apply**.

Message: "**Error: HTTP protocol error 403 (Forbidden): The server refused to fulfill the request**"

Possible cause

The user configured in *monitor_apps_REST_license_overview* data connection does not have read access to the license and access type entities.

Proposed action

Do the following:

1. Open the **Data connections** overview page in the QMC.
2. Select the *monitor_apps_REST_license_overview* data connection, click **Edit** and enter user ID and password credentials of a user with correct access rights.
3. Save the changes.

Message: "**Error: Field not found...**"

Possible cause

Some fields that are used by the Monitoring apps are missing in the log files.

Proposed action

Upgrade to 2.1.1 or later.

Message: "**Error: Table 'tempDateTimeList' not found...**"

This error can occur after an upgrade, especially if the environment changes from synchronized persistence to shared persistence, or if the Qlik Sense cluster share where Archived Logs are stored is changed.

Possible cause

The app cannot find license history data in the log files because the *ArchivedLogsFolder* data connection is incorrect.

Proposed action

Fix the *ArchivedLogsFolder* data connection to point to the correct folder location.

Message: "**Error: QVX_UNEXPECTED_END_OF_DATA...**"

This error can have different causes.

Customized proxy port

Possible cause

The proxy's HTTPS port has been customized.

Proposed action

Change all the `monitor_apps_REST_` data connections to use the customized port.

Example:

CUSTOM CONNECT TO*"provider=QvRestConnector.exe;url=https://localhost:4443/qrs..."*.

Data connections affected include the following:

- `monitor_apps_REST_app`
- `monitor_apps_REST_appobject`
- `monitor_apps_REST_event`
- `monitor_apps_REST_license_access`
- `monitor_apps_REST_license_login`

- `monitor_apps_REST_task`
- `monitor_apps_REST_user (this connection is now obsolete)`
- `monitor_apps_REST_user_condensed`
- `monitor_apps_REST_license_user`

Changes made to the user account under which the Qlik Sense services are running

Error message: **Error: QVX_UNEXPECTED_END_OF_DATA: HTTP protocol error 401 (Unauthorized): Requested resource requires authentication.**

Possible cause

During installation, a user account is created under which the Qlik Sense services run. If the credentials for that account changes, or a different account is selected for the Qlik Sense services to run under, the data connections must be updated accordingly.

Proposed action

Do the following:

1. Open the **Data connections** overview page in the QMC.
2. For each `monitor_apps_REST_` data connection, click **Edit** and enter the new **User ID** and **Password** credentials.
3. Save the changes.

Reloads of License Monitor, Operations Monitor, or Session Monitor fail

Error message: **Error: QVX_UNEXPECTED_END_OF_DATA: HTTP protocol error 500 (Internal Server Error): Exception of type 'System.OutOfMemoryException' was thrown.**

Possible cause

The number of users and user attributes is too big.

Proposed action

Do the following:

- Clean your user list to reduce its size.
- In the QMC, in the user directory connectors settings, keep **Sync user data for existing users** selected to avoid syncing a large number of users and user attributes.

The Monitoring apps fail to reload in a multi-node environment

There is more than one possible cause when the reload fails.

The central node is not a reload node

The Monitoring apps with default `monitor_apps_REST_` data connection strings fail to reload in a multi-node environment where the central node is not a reload node.

Possible cause

The reload node where the Monitoring apps are reloaded does not have any proxy set up.

Proposed action

Change all the `monitor_apps_REST_` data connections to point to the fully qualified domain name (FQDN) of the central node. This is accomplished by replacing *localhost* in the connection strings URL and *trustedLocation* parameters with FQDN of the central node.

Example:

CUSTOM CONNECT TO *"provider=QvRestConnector.exe;url=https://centralnodeserver.company.com/qrs...".*

Data connections affected include the following:

- `monitor_apps_REST_app`
- `monitor_apps_REST_appobject`
- `monitor_apps_REST_event`
- `monitor_apps_REST_license_access`
- `monitor_apps_REST_license_login`
- `monitor_apps_REST_task`
- `monitor_apps_REST_user (this connection is now obsolete)`
- `monitor_apps_REST_user_condensed`
- `monitor_apps_REST_license_user`

The repository database is on a separate machine

Possible cause

The REST data connections point to the FQDN of the Qlik Sense Repository Database and not the Qlik Sense Repository Service.

Proposed action

In any multi-node or "remote" Qlik Sense Repository Database situation, you need to update the REST data connections to point to the FQDN of the Qlik Sense Repository Service, regardless of where the actual Qlik Sense Repository Database resides.

Operations Monitor App fails to reload after turning off database logging

The Operations Monitor reload task fails after the database logging is turned off.

The following error message is displayed:

`Error: Table 'time_range_working' not found`

Possible cause

The Monitoring apps continue to check for recent logs in the database and use these logs for approximately ten hours after the last log message is written in the database. If the database logging is turned off, no new log entries for the load script can be found, and this can cause the reload process to fail.

Proposed action

The reload fail can be prevented by manually updating the Operations Monitor app's load script.

1. Make sure file logging is enabled.

2. Update the Operations Monitor load script. Because this is a published app, you need to duplicate it first.

   Do the following:

   i. Duplicate the Operations Monitor app in the QMC.

   ii. Open the duplicate app in the Qlik Sense hub.

   iii. Update the load script at line 9 by changing the variable `db_v_file_override` from 0 (default value) to 1 as follows:
       `SET db_v_file_override = 1`
       By setting this variable to 1, the script will not check for log entries in the database logging.

   iv. Save the app.

   v. Replace the existing Operations Monitor app by publishing the duplicate app to the Monitoring apps stream and selecting **Replace existing app**.

3. Launch the Operations Monitor reload task again. If it does not work immediately, wait a few minutes and reload again.

By following this procedure, the database logging can be turned off safely.

Failed to connect to the QRS via the Qlik REST Connector

This problem will only occur when you have apps that work with the Qlik REST Connector.

An error message is displayed that there is a problem connecting to the QRS via the Qlik REST Connector.

Possible cause

The Qlik REST Connector is unavailable, because it has been uninstalled or corrupted.

Proposed action

If the error message appears during a reload, you need to verify that the Qlik Sense installation is working properly. Consider repairing or upgrading Qlik Sense.

3   Troubleshooting Qlik Sense Enterprise on Windows using logs

Troubleshooting may be needed when Qlik Sense Enterprise on Windows does not behave as expected (for example, if the system responds with an error message that needs further investigation or does not respond at all when an error occurs).

The log messages produced by Qlik Sense provide important information that can be used to detect security incidents, operational problems, and policy violations.

The description of how to troubleshoot Qlik Sense using logs is based on "use cases", each of which corresponds to a typical user or system action, such as opening an app or stopping a task.

Each use case is described using the sections listed in the following table.

Use cases

Section	Description
Procedure	This section lists the actions that are performed (and logged) by Qlik Sense when the use case is carried out.
Success	This section lists the log files to which Qlik Sense writes log entries in case of success.
Errors	This section lists errors that may occur when the use case is performed. It is recommended to check the *<MachineName>_Service_<Service>.txt* file in case of an error as all errors are logged in this file. Each error section also includes a description of the actions to perform in case of an error. *For some use cases, there is no Error section. Information on errors will be added in future releases of the Qlik Sense documentation.*

3.1   Conventions

The following conventions are used in the documentation for Qlik Sense.

Style coding

- Menu commands and dialog options are written in **bold**.
- File names and paths are written in *Italics*.
- Sample code is written in `Lucida Console`.

Environment variables

The paths used in the documentation for Qlik Sense may use environment variables. The variables and the equivalent paths in the Microsoft Windows operating system are listed below.

Environment variables

Environment variable	Microsoft Windows
%LocalAppData%	*C:\Users\<username>\AppData\Local*
%ProgramData%	*C:\ProgramData*
%ProgramFiles%	*C:\Program Files*
%UserProfile%	*C:\Users\<username>*

3.2   Qlik Sense Repository Service

This section describes how to use the Qlik Sense logs to troubleshoot problems related to the Qlik Sense Repository Service (QRS).

Update user

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS verifies that the update does not disable any service account that the user is allowed to update.
3. The QRS updates the user.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

Delete user

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS verifies that the user to be deleted is not a service account or the last user with root admin access.
3. The QRS removes the user.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

Open app

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS checks that the app exists.
3. The QRS checks that the user is allowed to open the app.
4. The QRS sends a request to the Qlik Sense Engine Service (QES).
5. The QES checks the access to the data set in the app.
6. The QES loads the app and returns it.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*
- *<MachineName>_AuditActivity_Engine.txt*

Errors

Your account is inactive

Your account is inactive error

Description	Command=Open app;Result=403;ResultText=Error: Security
Message	Your account is inactive. Contact your administrator to activate it. (HTTP code: 403)
Action	Contact the Qlik Sense system administrator to obtain the correct access rights.

Create app

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS checks that the user is allowed to create an app.
3. The QRS sends a request to the Qlik Sense Engine Service (QES).
4. The QES creates the app.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Errors

Forbidden

<div align="center">Forbidden error</div>

Description	Command=Create app;Result=403;ResultText=Error: Security
Message	Forbidden (HTTP code: 403)
Action	The user is not allowed to create an app.

Delete app

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS marks the app as deleted in the repository database.
3. The QRS requests the Qlik Sense Engine Service (QES) to delete the app from disk.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*
- *<MachineName>_AuditActivity_Engine.txt*

Errors

The Delete operation failed

<div align="center">The Delete operation failed error</div>

Description	Command=Delete app;Result=400;ResultText=Error: PersistenceFailed
Message	The Delete operation failed (HTTP code: 400)
Action	Probable cause of error: The app does not exist.

Publish app

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS links the app to a stream.
3. The QRS checks if the published app is renamed.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Export app

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS provides the Qlik Sense Engine Service (QES) with the information needed to find the app.
3. The app ID is downloaded from the QES to the client.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*
- *<MachineName>_AuditActivity_Engine.txt*

Errors

Resource not found

Resource not found error

Description	Command=Export app;Result=9003;ResultText=Error: EngineQix
Message	Resource not found Parameters: QVF header error (read) (HTTP code: 400)
Actions	Proceed as follows: 1. Check that the resource exists in the Qlik Management Console (QMC). 2. Verify that you can open the app in the Qlik Sense hub. 3. Check if the QVF file exists on the central node or on a rim node in the Qlik Sense site.

Import app

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. If you have access to the Qlik Sense system where the app was created, the following happens:
   a. The QRS stores metadata in the repository database.
   b. The QRS contacts the Qlik Sense Engine Service (QES).
   c. The app is migrated (if necessary).
3. The QES imports the app (including objects) and persists it.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*
- *<MachineName>_AuditActivity_Engine.txt*

Errors

Corrupt data

Corrupt data error

Description	Command=Import app;Result=11;ResultText=Error: EngineQix
Message	Corrupt data Parameters: QVF File corrupt (HTTP code: 500)
Action	The format of the app is invalid and it cannot be imported.

Write failed

Write failed error

Description	Command=Import app;Result=9000;ResultText=Error: EngineQix
Message	Write Failed Parameters: REST client response error (HTTP code: 500)
Action	Proceed as follows: 1. Check that the Qlik Sense Engine Service (QES) is up and running as the request may have timed out. 2. Verify that you can open the app where it was created in Qlik Sense. 3. Verify that you can load app data in the data load editor and that you can reload the app in the Qlik Management Console (QMC). 4. Check the reload history of the app.

Resource not found

Resource not found error

Description	Command=Import app;Result=2;ResultText=Error: EngineQix
Message	Resource not found Parameters: QVF object error (HTTP code: 500)
Action	Provide a working QVF file for import.

Reload app

The data in an app can be reloaded in different ways:

- The user manually reloads the app data in the Qlik Management Console (QMC).
- The app data is reloaded by a scheduled task in the repository database.
- The user manually loads data in the data load editor. Information on such reloads is logged in *<MachineName>_AuditActivity_Engine.txt*.

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).

2. The QRS contacts the Qlik Sense Scheduler Service (QSS).

3. The QSS starts the reload task.

4. The QSS contacts the Qlik Sense Engine Service (QES) and initiates a reload of the app.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

- *<MachineName>_AuditActivity_Engine.txt*

- *<MachineName>_AuditActivity_Scheduler.txt*

Duplicate app

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).

2. The QRS checks that the app exists.

3. The QRS checks that the user is allowed to duplicate the app.

4. The QRS sends a request to the Qlik Sense Engine Service (QES).

5. The QES makes a copy of the app.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

- *<MachineName>_AuditActivity_Engine.txt*

Errors

Resource not found

Resource not found error

Description	Command=Duplicate app;Result=-2146233074;ResultText=Error: Resource not found [LOCERR_PERSISTENCE_NOT_FOUND]:Resource not found(QVF header error (read))
Message	Duplicate failed. App 'Test' duplicated to 'Test(1)'. Additional info: 'Resource not found [LOCERR_PERSISTENCE_NOT_FOUND]:Resource not found(QVF header error (read))'
Action	Probable cause of error: The app has been deleted from disk. Try to import the app again.

Add app object

Procedure

Qlik Sense performs the following procedure:

1. The Qlik Sense Engine Service (QES) contacts the Qlik Sense Repository Service (QRS).
2. The app object is added to the repository database in a bulk operation.
3. The QES persists the app object.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Update app object

Procedure

Qlik Sense performs the following procedure:

1. The Qlik Sense Engine Service (QES) contacts the Qlik Sense Repository Service (QRS).
2. The app object is updated in the repository database in a bulk operation.
3. The QES updates the persisted app object.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Delete app object

Procedure

Qlik Sense performs the following procedure:

1. The Qlik Sense Engine Service (QES) contacts the Qlik Sense Repository Service (QRS).
2. The app object is set to be deleted in the repository database in a bulk operation.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Publish app object

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS sets the app object as published in the repository database.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Unpublish app object

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS sets the app object as unpublished in the repository database.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Add extension

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS adds the extension.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Create extension

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS creates the extension.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Upload extension

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS uploads the extension.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Errors

The process cannot access the file

<p align="center">The process cannot access the file error</p>

Description	Command=Upload extension;Result=500;ResultText=Error: IO
Message	The process cannot access the file '<Filename>' because it is being used by another process. (HTTP code: 500)
Action	Try the following measures: • Wait for any ongoing process in the Qlik Management Console (QMC) to finish and then upload the extension again. • Restart the QRS.

Delete extension

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS deletes the extension.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Add extension content

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS adds the extension content.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Delete extension content

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS deletes the extension content.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Add content library

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS adds the content library.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Delete content library

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS deletes the content library.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Upload content library content

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS uploads the content library content.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Errors

Exception of type 'Qlik.Sense.Common.Exceptions.ConflictException' was thrown

Exception of type 'Qlik.Sense.Common.Exceptions.ConflictException' was thrown error

Description	Command=Upload content library content;Result=409;ResultText=Error: Conflict
Message	Exception of type 'Qlik.Sense.Common.Exceptions.ConflictException' was thrown. (HTTP code: 409)
Action	The library content already exists. Rename or replace the library content.

Delete content library content

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS deletes the content library content.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Add user access

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS verifies that the access can be added.
3. The QRS adds the access.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

Errors

Validation failed

Validation failed error

Description	Command=Add User Access;Result=400;ResultText=Error: Bad Request
Message	<BrokenRules>
Action	Make sure that you are allowed to add the access.

Update user access

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS verifies that the access can be updated.
3. The QRS updates the access.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

Delete user access

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS verifies that the access can be deleted.
3. The QRS deletes the access.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

License user access request

Procedure

Qlik Sense performs the following procedure:

- Qlik Sense checks that the user has a valid access pass. This is done every time a user requests access to a resource (such as an app).

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

License user access

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) checks the Qlik Sense license to determine if the user can be given an access pass.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

Errors

Login access denied

Login access denied error

Description	Command=License user access;Result=403;ResultText=Error: Access denied
Message	Login access denied for SessionID: 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx', Hostname: "xx.xx.xx.xx", OperationType: 'UsageDenied'
Action	Contact the Qlik Sense system administrator to obtain the correct access rights.

Add user access from license

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS verifies that the user access can be added.
3. The QRS identifies the user access.
4. The QRS adds the user access.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

Errors

Cannot add user access

<p align="center">Cannot add user access error</p>

Description	Command=Add user access from license;Result=400;ResultText=Error: Bad Request
Message	<BrokenRules>
Action	Check the following: • That the license has not expired • That the license is not deny listed • That there are enough tokens available in the Qlik Sense license

Add app privilege

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) adds app privileges to the appropriate user groups.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*.

Export certificates

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) exports the certificates.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

Download license

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) validates the license and downloads it.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

Errors

License: Invalid serial number or control number

License: Invalid serial number or control number error

Description	Command=Download license;Result=400;ResultText=Error: ValidationFailed
Message	License: Invalid serial number or control number (HTTP code: 400)
Action	Provide a valid Qlik Sense license.

Add license

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) adds the license provided by the user.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

Errors

License: Invalid serial number or control number

License: Invalid serial number or control number error

Description	Command=Update license;Result=400;ResultText=Error: ValidationFailed
Message	License: Invalid serial number or control number (HTTP code: 400)
Action	Provide a valid Qlik Sense license.

Update license

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) adds the license provided by the user.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

Errors

License: Invalid serial number or control number

License: Invalid serial number or control number error

Description	Command=Update license;Result=400;ResultText=Error: ValidationFailed
Message	License: Invalid serial number or control number (HTTP code: 400)
Action	Provide a valid Qlik Sense license.

Delete license

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) deletes the license.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Add rule

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS adds the rule.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Update rule

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS updates the rule.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Delete rule

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS deletes the rule.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Add stream

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS adds the stream.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Delete stream

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS deletes the stream.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Server node registration

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) establishes a connection to the specified server address.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Errors

Cannot reach the following remote host when distributing certificates

Cannot reach the following remote host when distributing certificates error

Description	Command=Server node registration;Result=400;ResultText=Error: REST
Message	Cannot reach the following remote host when distributing certificates: http://<ServerAddress>:4444/setup/certificateDistribution (HTTP code: 400)
Action	Provide a valid server address.

Server node configuration

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) updates the configuration for a server node.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Create task

Procedure

Qlik Sense performs the following procedure:

1. The Qlik Sense Repository Service (QRS) creates a task and stores it in the repository database.
2. The task information is synchronized by the QRS to the rim nodes.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Update task

Procedure

Qlik Sense performs the following procedure:

1. The Qlik Sense Repository Service (QRS) updates the task and stores it in the repository database.
2. The updated task information is synchronized by the QRS to the rim nodes.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Delete task

Procedure

Qlik Sense performs the following procedure:

1. The Qlik Sense Repository Service (QRS) deletes the task and removes it from the repository database.
2. The deletion of the task is synchronized by the QRS to the rim nodes.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Start task

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) requests the Qlik Sense Scheduler Service (QSS) to execute the task.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Errors

Resource not found

	Resource not found error
Description	Command=Start task;Result=-1;ResultText=Error: -----System.Net.WebException: Unable to connect to the remote server ---> System.Net.Sockets.SocketException: No connection could be made because the target machine actively refused it 127.0.0.1:5050 at System.Net.Sockets.Socket.EndConnect(IAsyncResult asyncResult) at System.Net.ServicePoint.ConnectSocketInternal(Boolean connectFailure, Socket s4, Socket s6, Socket& socket, IPAddress& address, ConnectSocketState state, IAsyncResult asyncResult, Exception& exception) --- End of inner exception stack trace --- at System.Net.HttpWebRequest.EndGetRequestStream(IAsyncResult asyncResult, TransportContext& context) at System.Net.HttpWebRequest.EndGetRequestStream (IAsyncResult asyncResult) at System.Net.WebClient.UploadBitsRequestCallback (IAsyncResult result)-----
Message	Trailing task exception in SchedulerClient.StartTask('1xx1111x-111x-111x-1xx1-111xxx1x1x11'): '↓-----↓System.Net.WebException: Unable to connect to the remote server ---> System.Net.Sockets.SocketException: No connection could be made because the target machine actively refused it 127.0.0.1:5050↵ ↓ at System.Net.Sockets.Socket.EndConnect(IAsyncResult asyncResult)↵ ↓ at System.Net.ServicePoint.ConnectSocketInternal(Boolean connectFailure, Socket s4, Socket s6, Socket& socket, IPAddress& address, ConnectSocketState state, IAsyncResult asyncResult, Exception& exception)↵ ↓ --- End of inner exception stack trace ---↵ ↓ at System.Net.HttpWebRequest.EndGetRequestStream(IAsyncResult asyncResult, TransportContext& context)↵ ↓ at System.Net.HttpWebRequest.EndGetRequestStream (IAsyncResult asyncResult)↵ ↓ at System.Net.WebClient.UploadBitsRequestCallback (IAsyncResult result)↓-----'
Action	Check that the Qlik Sense Scheduler Service (QSS) is up and running.

Stop task

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) requests the Qlik Sense Scheduler Service (QSS) to stop the execution of the task.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Synchronize user directory

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) synchronizes the user directory.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*

Start repository

Procedure

Qlik Sense performs the following procedure:

1. Validate the command line parameters for the QRS.
2. The QRS loads the logging framework.
3. The QRS validates the certificates.
4. The QRS establishes a connection to the Qlik Sense Repository Database (QRD).
5. If needed, the QRS performs the migration steps of the repository database schema.
6. Hardware information is collected.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Repository.txt*

Errors

Certificates are not correctly installed

Certificates are not correctly installed error

Description	Command=Start Repository;Result=-1;ResultText=Certificates are not correctly installed
Message	Initializing certificates.
Action	The error is related to an invalid certificate. Contact your system administrator for support regarding the certificates.

Stop repository

Procedure

Qlik Sense performs the following procedure:

1. The internal services are stopped.
2. The background threads are stopped.
3. All Qlik Sense services, except for the Qlik Sense Repository Database (QRD), are stopped.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Repository.txt*

Check service status

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) checks that the communication with the specified Qlik Sense service is working.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Repository.txt*

Errors

The following service account does not exist

The following service account does not exist error

Description	Command=Check service status;Result=403;ResultText=Error: Security
Message	The following service account does not exist: <Service.Name> (HTTP code: 403)
Action	Restart the specified Qlik Sense service.

Load plugin

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) loads the specified plugins during the installation process.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Repository.txt*

Audit rules

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) fetches the specified rules from the repository database.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

Audit security

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) fetches the specified security rules from the repository database.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

Audit license

Procedure

Qlik Sense performs the following procedure:

- A Qlik Sense Repository Service (QRS) thread runs in the background.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

Audit license rule

Procedure

Qlik Sense performs the following procedure:

- A Qlik Sense Repository Service (QRS) thread runs in the background and monitors the license usage.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

License maintenance

Procedure

Qlik Sense performs the following procedure:

- A Qlik Sense Repository Service (QRS) thread runs in the background.
  The thread continuously checks the proxy sessions linked to the license in order to:

  - Prevent users from over-consuming license tokens
  - Check if any changes linked to the license prevent the user from consuming an access pass
  - Check if the proxy session has timed out for the access pass

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Repository.txt*

Distribute certificate

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Repository Service (QRS) distributes a certificate to the rim node.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Repository.txt*

Errors

Certificate distribution failed

Certificate distribution failed error

Description	Command=Distribute certificate;Result=-2146233088;ResultText=Error: Cannot reach the following remote host when distributing certificates: http://<ServerAddress>:4444/setup/certificateDistribution
Message	Certificate distribution failed
Action	Provide a valid server address.

3.3   Qlik Sense Proxy Service

This section describes how to use the Qlik Sense logs to troubleshoot problems related to the Qlik Sense Proxy Service (QPS).

Start proxy

Procedure

Qlik Sense performs the following procedure:

1. The Qlik Sense Proxy Service (QPS) creates a proxy.
2. The QPS starts the proxy.
3. Hardware information is collected.
4. The QPS writes the hardware information in the logs.
5. The QPS installs the certificates.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Proxy.txt*
- *<MachineName>_Service_Proxy.txt*

Errors

Error occurred while retrieving hardware information

Error occurred while retrieving hardware information error

Description	Command=Start proxy;Result= -1;ResultText=Error occurred while retrieving hardware information
Message	The message may vary.
Action	Check the registry settings.

Proxy will not be listening to port '443'

Proxy will not be listening to port '443' error

Description	Port collisions may occur when internal services are started during the startup of the QPS:
	Command=Start internal service;Result=-2147467259;ResultText=Error: Only one usage of each socket address
Message	Proxy will not be listening to port '443' (most likely bound by another process)
Action	Proceed as follows:
	1. Make sure that port 443 is available for Qlik Sense to use.
	2. Restart the Qlik Sense services.

Stop proxy

Procedure

Qlik Sense performs the following procedure:

1. The Qlik Sense Proxy Service (QPS) notifies the Qlik Sense Repository Service (QRS).
2. The QPS settings and notification poller threads are stopped.
3. The QPS checks that the QRS has installed the certificate.
4. The internal services are stopped.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Proxy.txt*

Open connection

Procedure

Qlik Sense performs the following procedure:

- Open a socket to the Qlik Sense Engine Service (QES). This happens every time a user opens an app in Qlik Sense.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Proxy.txt*
- *<MachineName>_Service_Proxy.txt*

Errors

Web socket connection could not be opened

<div align="center">Web socket connection could not be opened error</div>

Description	Command=Open connection;Result=400;ResultText=Error: Web socket connection could not be opened
Message	Connection '<ID of connection>' has been transferred to a streaming state to send a single error message
Action	Proceed as follows: 1. Check if the QES is up and running. If not, start the QES. 2. Check that it is possible to connect to the QES.

Web exception: Protocol error: Response stream exists

<div align="center">Web exception: Protocol error: Response stream exists error</div>

Description	Command=Open connection;Result=400;ResultText=<different from zero>;ResultText=Error: <error message>
Message	Web exception: Protocol error: Response stream exists. Remote endpoint '{0}' + various exception message

Action	Check the following: • That the QES is up and running. • That you can connect to the QES on port 4747 locally on the server.

Web exception: Protocol error: No response stream exists

Web exception: Protocol error: No response stream exists error

Description	Command=Open connection;Result=400;ResultText=<different from zero>;ResultText=Error: <error message>
Message	Web exception: Protocol error: No response stream exists when contacting '{0}' ' + various exception message
Action	Check the following: • That the QES is up and running. • That you can connect to the QES on port 4747 locally on the server.

Web exception when contacting service uri

Web exception when contacting service uri error

Description	Command=Open connection;Result=400;ResultText=<different from zero>;ResultText=Error: <error message>
Message	Web exception when contacting service uri {0} ' + various exception message
Action	Check that service at URI is available.

Connection has been transferred to a streaming state to send a single error message

Connection has been transferred to a streaming state to send a single error message error

Description	Command=Open connection;Result=400;ResultText=<different from zero>;ResultText=Error: <error message>
Message	Connection '{0}' has been transferred to a streaming state to send a single error message + various exception message
Action	Check the following: • That the QES is up and running. • That you can connect to the QES on port 4747 locally on the server.

Web socket connection could not be opened

Web socket connection could not be opened error

Description	Command=Open connection;Result=400;ResultText=<different from zero>;ResultText=Error: <error message>
Message	Web socket connection could not be opened

Action	Check the following: • That the QES is up and running. • That you can connect to the QES on port 4747 locally on the server.

Close connection

Procedure

Qlik Sense performs the following procedure:

• Close the socket to the Qlik Sense Engine Service (QES). This happens every time a user closes an app (for example, by closing a tab in a browser).

Success

In case of success, log entries are written in the following files throughout the procedure:

• *<MachineName>_AuditActivity_Proxy.txt*

Errors

Web socket connection could not be opened

Web socket connection could not be opened error

Description	Command=Open connection;Result=400;ResultText=Error: Web socket connection could not be opened
Message	Connection '<ID of connection>' has been transferred to a streaming state to send a single error message
Action	Proceed as follows: 1. Check if the QES is up and running. If not, start the QES. 2. Check that it is possible to connect to the QES.

Command=Open connection;Result=<different from zero>

Command=Open connection; Result=<different from zero>

Description	Command=Open connection;Result=<different from zero>;ResultText=Error: <error message>
Message	Search for any log message related to Close connection. If you find a log entry similar to the one described above, evaluate the information in the Message field.

Action	Proceed as follows: 1. Analyze the memory consumption and run netstat (TCP sockets in illegal state). If you encounter any issues, restart the QPS as connections (that is, web sockets to the QES) are disposed by the Qlik Sense Proxy Service (QPS). 2. If the problem persists, check that the QES is up and running. 3. Contact Qlik support.

Start session

Procedure

Qlik Sense performs the following procedure:

- A new proxy session starts when a user accesses Qlik Sense.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Proxy.txt*

Errors

Cannot start session

<div align="center">Cannot start session error</div>

Description	If a user cannot start a new proxy session, it is most likely related to: - The configuration of the Qlik Sense Proxy Service (QPS) - Installation-specific issues Search for any log message with the following information: Command=Start session;Result=<different from zero>;ResultText=Error: <error message>
Message	If you find a log entry similar to the one described above, evaluate the information in the Message field.
Action	If there are no log entries for Start session, check the configuration of the QPS by examining the log entries for the Start proxy command.

Stop session

Procedure

Qlik Sense performs the following procedure:

- A proxy session stops when the user logs out, or when the proxy session times out.
  If the user closes the browser where the session is running, the proxy session stops when the *Session inactivity timeout (minutes)* setting has been exceeded, calculated from the moment the browser was closed.
  Session inactivity timeout (minutes) is defined under the virtual proxy, see [Virtual proxies](#).

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Proxy.txt*

Errors

Cannot stop session

Cannot stop session error

Description	Search for any log message with the following information: Command=Stop session;Result=<different from zero>;ResultText=Error: <error message>
Message	If you find a log entry similar to the one described above, evaluate the information in the Message field.
Action	If there are no log entries for Stop session, check the configuration of the Qlik Sense Proxy Service (QPS) by examining the log entries for the Start proxy command. As a last resort, restart the QPS.

Log out

Procedure

Qlik Sense performs the following procedure:

- The user is logged out when the proxy session times out or when the user actively logs out.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Proxy.txt*

Errors

Command=Logout;Result=<return code not zero>

Command=Logous;Result=<return code not zero> error

Description	Command=Logout;Result=<return code not zero>;ResultText=Error: <error message>
Message	If you find a log entry similar to the one described above, evaluate the information in the Message field.

Action	Proceed as follows, if a user repeatedly experiences problem when logging out: 1. Restart the Qlik Sense Proxy Service (QPS). 2. Analyze the status of the sockets by running netstat and search for sockets in CLOSE_WAIT, SYN_SENT, or FIN_WAIT_2 state.

Log in

Procedure

Qlik Sense performs the following procedure:

1. Check if the user is linked to a valid user directory.
2. Check if the user exists in the repository database.
3. Check if the user has access to Qlik Sense.
4. Check if the user has access linked to the license.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Proxy.txt*

Errors

Logon failed

Logon failed error

Description	Command=Login;ResultCode=403;ResultText=Error: Access Denied
Message	Login failed for user '<username>' wrong credentials?
Action	Proceed as follows: - Check that the user exists in the repository database. - Check that the user has access rights to Qlik Sense linked to a license. - Check that the user is not blocked.

Install certificate

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Proxy Service (QPS) waits for the certificates to be installed in the repository database.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditSecurity_Proxy.txt*

3.4   Qlik Sense Scheduler Service

This section describes how to use the Qlik Sense logs to troubleshoot problems related to the Qlik Sense Scheduler Service (QSS).

Start task

Procedure

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The manager Qlik Sense Scheduler Service (QSS) on the central node communicates with each worker QSS to see which ones are available to perform the task.
3. The task is given to the currently available worker QSS with the least load according to the load balance rules.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Scheduler.txt*
- *<MachineName>_AuditActivity_Repository.txt*

Errors

Task not found

Task not found error

Description	Command=Start task;Result=5;ResultText=Error: Failed
Message	Task not found
Action	Try the following measures: • If the repository database is accessible, search the database for the task. • Check if the task has been successfully synchronized to the rim nodes. • Create a new, identical task and see if it works.

Scheduler is not licensed

Scheduler is not licensed error

Description	Command=Start task;Result=10;ResultText=Error: Failed
Message	Scheduler is not licensed. Not allowed to run Tasks
Action	Provide a valid Qlik Sense license.

Scheduler is not Manager

Scheduler is not Manager error

Description	Command=Start task;Result=15;ResultText=Error: Failed
Message	Scheduler is not Manager. Not allowed to run Tasks
Action	Make sure that the QSS on the central node is "Manager" or "Manager and Worker".

Found active session for Task

Found active session for Task error

Description	Command=Start task;Result=20;ResultText=Error: Failed
Message	Found active session for Task. Task not started
Action	Try the following measures: • Wait until the task has completed. • Stop the task. • Restart the QSS.

Task disabled

Task disabled error

Description	Command=Start task;Result=25;ResultText=Error: Failed
Message	Task disabled
Action	Enable the task.

TaskExecutionSession already exists

TaskExecutionSession already exists error

Description	Command=Start task;Result=30;ResultText=Error: Failed
Message	TaskExecutionSession already exists for App <App.Name>
Action	Try the following measures: • Wait until the task that is reloading the app has completed. • Stop the task that is reloading the app. • Restart the QSS.

No worker nodes found to execute Task

No worker nodes found to execute Task error

Description	Command=Start task;Result=40;ResultText=Error: Failed
Message	No worker-nodes found to execute Task: <Task.Name>

Action	Proceed as follows:
	1. Check the status of the worker nodes to determine if they can perform a reload.
	2. Check that the app to reload exists on the worker nodes.

Unable to create TaskExecutionSession

Unable to create TaskExecutionSession error

Description	Command=Start task;Result=45;ResultText=Error: Failed
Message	Unable to create TaskExecutionSession
Action	Restart the QSS.

Unexpected exception when starting task

Unexpected exception when starting task error

Description	Command=Start task;Result=50;ResultText=Error: Failed
Message	Unexpected exception when starting task. Exception message: <Exception.Message>
Action	Restart the QSS.

Unexpected exception when trying to start task

Unexpected exception when trying to start task error

Description	Command=Start task;Result=55;ResultText=Error: Failed
Message	Unexpected exception when trying to start task. Exception message: <Exception.Message>
Action	Restart the QSS.

Max number of retries reached for task

Max number of retries reached for task error

Description	Command=Start task;Result=80;ResultText=Error: Failed
Message	Max number of retries (<Amount>) reached for task (id/name) <Task.ID>/<Task.Name>
Action	Restart the QSS.

Not possible to initiate retry

Not possible to initiate retry error

Description	Command=Start task;Result=90;ResultText=Error: Failed
Message	Not possible to initiate retry. TaskExecutionSession is null
Action	Restart the QSS.

Finish task

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Scheduler Service (QSS) on the worker node that performed the task communicates the result to the manager QSS.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Scheduler.txt*
- *<MachineName>_AuditActivity_Repository.txt*

Errors

Failed in TaskCompletedFail

Failed in TaskCompletedFail error

Description	Command=Finished task;Result=60;ResultText=Error: Failed
Message	Failed in TaskCompletedFail. Forcing task to Error
Action	Check if the task has been successfully synchronized to the rim nodes.

Task finished with state <State>

Task finished with state <State> error

Description	Command=Finished task;Result=65;ResultText=Error: Failed
Message	Task finished with state <State>
Action	Check if the task has been successfully synchronized to the rim nodes.

Failed to remove session

Failed to remove session error

Description	Command=Finished task;Result=70;ResultText=Error: Failed
Message	Failed to remove session with Id <Session.ID> for TaskId <Task.ID>
Action	Restart the QSS.

Unexpected exception in TaskCompletedSuccess

Unexpected exception in TaskCompletedSuccess error

Description	Command=Finished task;Result=50;ResultText=Error: Failed
Message	Unexpected exception in TaskCompletedSuccess. Exception message: <Message>
Action	Restart the QSS.

Unexpected exception in TaskCompletedFail

Unexpected exception in TaskCompletedFail error

Description	Command=Finished task;Result=50;ResultText=Error: Failed
Message	Unexpected exception in TaskCompletedFail. Exception message: <Message>
Action	Restart the QSS.

Task failed

Task failed error

Description	Command=Finished task;Result=0;ResultText=Error: Failed
Message	Task failed
Action	Check the task for indications of why it failed. If the task is a reload task, check the engine logs and script logs for indications of why the reload failed.

Execute task

Procedure

Qlik Sense performs the following procedure:

- The Qlik Sense Scheduler Service (QSS) logs different states in the task execution chain during the execution of a task.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Scheduler.txt*

Errors

Trying to set task id to state

Trying to set task id to state error

Description	Command=Task execution;Result=55;ResultText=Error: Failed
Message	Trying to set task (id) <Task.ID> to state <State>. Not allowed. No statechange will take place!
Action	Proceed as follows: 1. Re-run the task. 2. Restart the QSS.

TaskExecutionSession cannot be null

TaskExecutionSession cannot be null error

Description	Command=Task execution;Result=90;ResultText=Error: Failed
Message	TaskExecutionSession cannot be null. Unable to proceed with state change due to deleted task with proposed state: <State>
Action	Proceed as follows: 1. Re-run the task. 2. Restart the QSS.

Suppressed state change

Suppressed state change error

Description	Command=Task execution;Result=85;ResultText=Error: Failed
Message	Suppressed state change to <State> for <Task.Name> with Id <Task.ID>
Action	No action is required. The state was suppressed when the task was stopped.

Unable to get <Task.Name>

Unable to get <Task.Name> error

Description	Command=Task execution;Result=5, 75;ResultText=Error: Failed
Message	Unable to get <Task.Name> with Id <Task.ID> for AuditActivityLog, only logging Id and Name for Task not for App.
Action	Proceed as follows: 1. Re-run the task. 2. Restart the QSS.

Start manager

Procedure

Qlik Sense performs the following procedure:

- The manager scheduler starts when the Qlik Sense Scheduler Service (QSS) starts on the central node.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Scheduler.txt*

Start worker

Procedure

Qlik Sense performs the following procedure:

- The worker scheduler starts when the Qlik Sense Scheduler Service (QSS) starts.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Scheduler.txt*

Resume manager

Procedure

Qlik Sense performs the following procedure:

- Resume a paused manager Qlik Sense Scheduler Service (QSS).

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Scheduler.txt*

Resume worker

Procedure

Qlik Sense performs the following procedure:

- Resume a paused worker Qlik Sense Scheduler Service (QSS).

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Scheduler.txt*

Read initial settings

Procedure

Qlik Sense performs the following procedure:

- Log the initial settings when the Qlik Sense Scheduler Service (QSS) starts.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Scheduler.txt*

Log hardware information at the startup of the service

Procedure

Qlik Sense performs the following procedure:

- Log hardware information during the startup of the Qlik Sense Scheduler Service (QSS).

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Scheduler.txt*

Errors

Failed when logging hardware information

Failed when logging hardware information error

Description	Command=Start scheduler;Result=50;ResultText=Error: Failed
Message	Failed when logging hardware information
Action	Restart the QSS.

Stop manager

Procedure

Qlik Sense performs the following procedure:

- The manager scheduler stops when the Qlik Sense Scheduler Service (QSS) shuts down on the central node.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Scheduler.txt*

Stop worker

Procedure

Qlik Sense performs the following procedure:

- The worker scheduler stops when the Qlik Sense Scheduler Service (QSS) shuts down.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Scheduler.txt*

Pause manager

Procedure

Qlik Sense performs the following procedure:

- Pause a running manager Qlik Sense Scheduler Service (QSS).

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Scheduler.txt*

Pause worker

Procedure

Qlik Sense performs the following procedure:

- Pause a running worker Qlik Sense Scheduler Service (QSS).

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Scheduler.txt*

Settings change for worker

Procedure

Qlik Sense performs the following procedure:

- Log the change of settings for a worker Qlik Sense Scheduler Service (QSS).

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Scheduler.txt*

3.5   Qlik Sense Engine Service

This section describes how to use the Qlik Sense logs to troubleshoot problems related to the Qlik Sense Engine Service (QES).

Open app

Procedure

Qlik Sense performs the following procedure:

1. Check if the app is already open.

2. If not, load the QVF file.

3. Read the app properties from the file.

4. Read the script from the file.

5. Open the app.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Engine.txt*

Errors

Already opened in different mode

Already opened in different mode error

Description	Command=Open app;Result=1009;ResultText=Error: App already open in different mode
Message	<AppId>
Action	Make sure that the app is not opened without data when you try to open it with data or vice versa.

Already opened

Already opened error

Description	Command=Open app;Result=1002;ResultText=Error: App already opened
Message	<AppId>
Action	Make sure that the app is not already open.

Invalid path

Invalid path error

Description	Command=Open app;Result=4;ResultText=Error: Invalid Path
Message	Malformed parameters
Action	Make sure that the app name, password, user name, and serial number are UTF-8 encoded strings.

Resource not found

Resource not found error

Description	Command=Open app;Result=9003;ResultText=Error: Resource not found
Message	QVF header error (read)
Action	Probable cause of error: The app has been deleted from disk. Try to import the app again.

Create app

Procedure

Qlik Sense performs the following procedure:

1. Check if the app name is valid.
2. Create the app.
3. Save the QVF file.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Engine.txt*

Errors

Invalid name

Invalid name error

Description	Command=Create app;Result=3001;ResultText=Error: App save failed
Message	<AppName>
Action	Make sure that the app name does not contain any of the following: • Special characters: <>:\"/|?* • Device names that are reserved in Microsoft Windows (for example, "COM1" and "LPT1")

Delete app

Procedure

Qlik Sense performs the following procedure:

1. Unload all app instances for the app.
2. Delete the QVF file.
3. Request the Qlik Sense Repository Service (QRS) to delete the file.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Engine.txt*

Errors

Delete failed

Delete failed error

Description	Command=Delete app;Result=9002;ResultText=Error: Delete failed
Message	<REST client response error>
Action	As there is no response from the QRS, check if it has stopped running or if it cannot process requests.

Export app

Procedure

Qlik Sense performs the following procedure:

1. Open the QVF file.
2. Copy to a new QVF file.
3. Export the app contents.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Engine.txt*

Errors

Disk is full

Disk is full error

Description	Command=Export app;Result=9009;ResultText=Error: The disk it out of space
Message	CopyQvfFile
Action	Free up some space on the disk.

File corrupt

File corrupt error

Description	Command=Export app;Result=3002;ResultText=Error: File corrupted
Message	CopyQvfFile
Action	Make sure that the file that is exported to can be written to.

Import app

Procedure

Qlik Sense performs the following procedure:

1. Check if the app can be migrated to the current version of Qlik Sense (if needed).

2. Open a copy of the app to import.

3. Remove unwanted objects (such as connections) from the copy.

4. Request the Qlik Sense Repository Service (QRS) to save the app.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Engine.txt*

Errors

File corrupt

<div align="center">File corrupt error</div>

Description	Command=Import app;Result=9008;ResultText=Error: App was created in a newer product version
Message	Migration
Action	Make sure that the app was not created in a newer version of Qlik Sense.

Internal error

<div align="center">Internal error error</div>

Description	Command=Import app;Result=10;ResultText=Error: Internal error
Message	Could not import file (ImportApp)
Action	During import, the QVF file is copied to the local *\App* folder first. If this fails, the folder is probably write-protected. Therefore check for any write-protection on the folder.

Reload app

Procedure

Qlik Sense performs the following procedure:

- Execute the reload script.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Engine.txt*

Duplicate app

Procedure

Qlik Sense performs the following procedure:

1. Compare the app IDs of the source and target apps.
2. Request the Qlik Sense Repository Service (QRS) to open the app.
3. Copy the QVF file.
4. Import the copy of the file.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Engine.txt*

Errors

Duplication failed

Duplication failed error

Description	Command=Duplicate app;Result=8;ResultText=Error: Invalid parameters
Message	Could not copy file. SrcAppId and TargetAppId are identical
Action	Make sure that the source and target IDs are not identical.

Publish app

Procedure

Qlik Sense performs the following procedure:

1. Check if the app is a session app. If so, publishing is not supported. A session app only exists in the Qlik Sense Engine Service (QES) memory and is not linked to any file.
2. Save the object in the repository database.
3. Request the Qlik Sense Repository Service (QRS) to publish the app.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Engine.txt*

Errors

Access denied

Access denied error

Description	Command=Publish app;Result=8;ResultText=Error: Access Denied
Message	Could not save objects
Action	Check if the disk is write-protected as the publish operation could not flush the objects needed before publishing the app.

REST connection failure

REST connection failure error

Description	Command=Publish app;Result=18;ResultText=Error: Rest connection failed
Message	REST client response error
Action	As there is no response from the QRS, check if it has stopped running or if it cannot process requests.

Unpublish app

Procedure

Qlik Sense performs the following procedure:

1. Check if the app is a session app. If so, publishing is not supported. A session app only exists in the Qlik Sense Engine Service (QES) memory and is not linked to any file.
2. Save the object in the repository database.
3. Request the Qlik Sense Repository Service (QRS) to unpublish the app.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Engine.txt*

Errors

Access denied

Access denied error

Description	Command=Unpublish app;Result=8;ResultText=Error: Access Denied
Message	Could not save objects
Action	Check if the disk is write-protected as the publish operation could not flush the objects needed before unpublishing the app.

REST connection failure

REST connection failure error

Description	Command=Unpublish app;Result=18;ResultText=Error: Rest connection failed
Message	REST client response error
Action	As there is no response from the QRS, check if it has stopped running or if it cannot process requests.

Replace app

Qlik Sense performs the following procedure:

1. A request is sent to the Qlik Sense Repository Service (QRS).
2. The QRS updates the repository database.
3. The QRS contacts the Qlik Sense Engine Service (QES).

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_AuditActivity_Repository.txt*
- *<MachineName>_AuditActivity_Engine.txt*

Start engine

Procedure

Qlik Sense performs the following procedure:

1. The Qlik Sense Engine Service (QES) sets the current execution mode (that is, server or desktop).
2. The QES parses the command line arguments.
3. The QES configures the logging.
4. The QES detects the operating system and version.
5. The QES initializes the collate and memory structures.
6. The QES sets the termination handlers, starts the internal threads, and checks the license.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Engine.txt*

Errors

Registration failure

Registration failure error

Description	Command=Start engine;Result=-1;ResultText=Error:Server crash
Message	Server crashed on registration
Action	Proceed as follows: 1. Check that the default *\App* folder exists. 2. Check the status of the network controller. 3. Check the status of the network port.

Stop engine

Procedure

Qlik Sense performs the following procedure:

1. The Qlik Sense Engine Service (QES) stops the cache trimmer.
2. The QES clears the cache.
3. The QES terminates the process handlers.
4. The QES exits the threads.

Success

In case of success, log entries are written in the following files throughout the procedure:

- *<MachineName>_Service_Engine.txt*

Errors

Cache trimmer never stopped

Cache trimmer never stopped error

Description	Command=Stop engine;Result=-1;ResultText=Warning
Message	Cache Trimmer never stopped
Action	Contact Qlik support.