# Manage Qlik Sense sites

Qlik Sense®
April 2018

# 1 Introduction

This document describes how to use the Qlik Management Console (QMC) to perform common Qlik Sense site tasks. This document does not cover every possible way of performing a task, but rather explains and gives examples of the following:

- Initial configuration of the Qlik Sense environment
- Administration of the Qlik Sense environment

Please use the Install and upgrade Qlik Sense document to plan the deployment and make the Qlik Sense site operational. It also documents the system requirements and the supported browsers.

## 1.1 Style coding

- Menu commands and dialog options are written in **bold**.
- File names and paths are written in *italic*.
- Sample code is written in `Lucida Console`.

## 1.2 Environment variable

The paths described in this document use the environment variable *%ProgramData%*. The equivalent path in the Microsoft Windows operating system is *C:\ProgramData*.

## 1.3 Additional server documentation

The following documentation is also available for Qlik Sense in a server deployment:

- Plan and deploy Qlik Sense: Describes Qlik Sense server and provides reference information on the architecture, security, logging, and licensing.
- Install and upgrade Qlik Sense: Describes how to install the Qlik Sense site and what you may want to consider before installing Qlik Sense.
- Qlik Sense repository service API: Provides reference information on the Qlik Sense repository service API.
- Qlik Sense proxy service API: Provides reference information on the Qlik Sense proxy service API.
- Qlik Sense User Directory Connector API: Provides reference information on the Qlik Sense User Directory Connector API.

## 1.4 Managing a Qlik Sense site

The QMC is a web-based application for configuring and administrating your Qlik Sense 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 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

## 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 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 system, which allows the RootAdmin user to set up security rules.*

### Access types

The License Enabler File (LEF) defines the terms of your license and the access types that you can allocate to users. There are two license types: one that is user-based and one that is token-based.

- User-based license: you can allocate professional access and analyzer access. The LEF determines the distribution of the two access types.
- Token-based license: you can allocate user access and login access. The LEF determines the number of tokens that you can allocate to the two access types.

An access type allows users to access streams and apps within a Qlik Sense site.

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

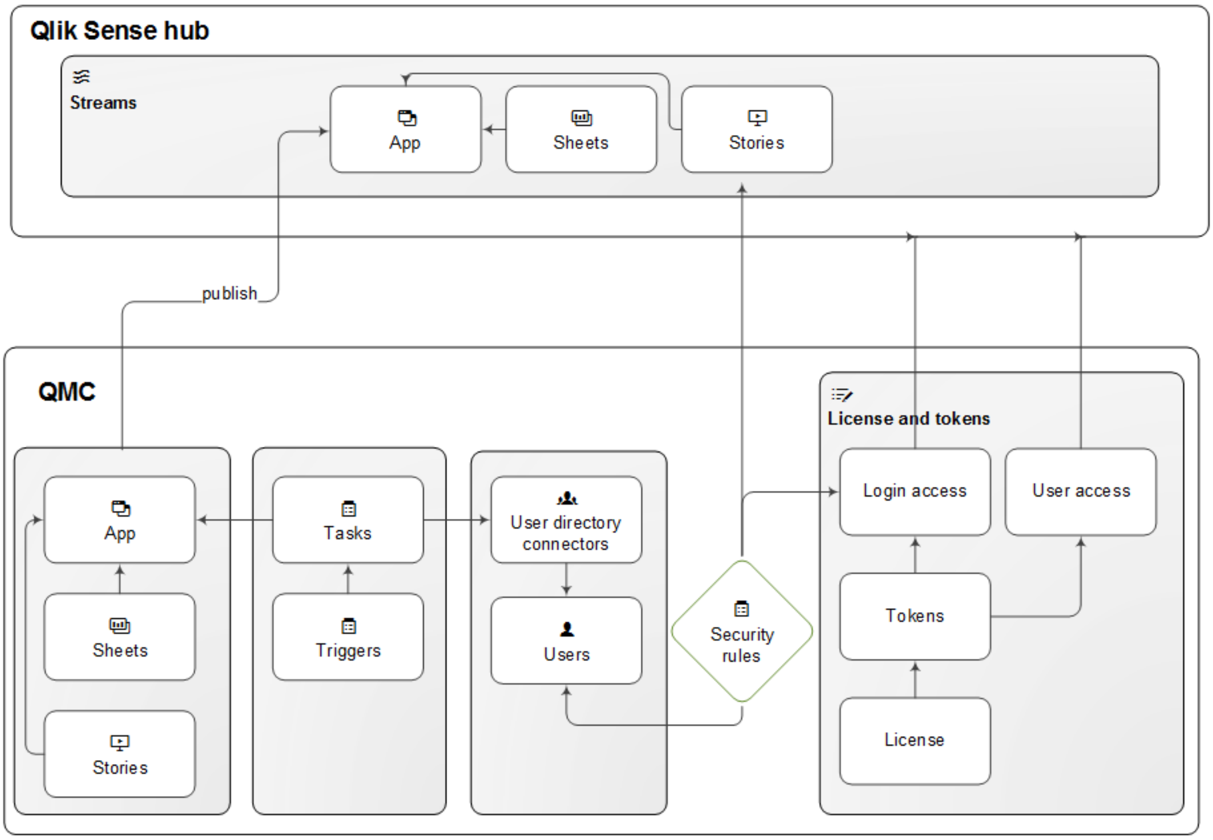
All user data is stored in the Qlik Sense repository service (QRS) database. You create user directory connectors in the QMC to be able to synchronize and retrieve the user data from a configured directory service. When a user logs in to Qlik Sense or the QMC, the user data is automatically retrieved. 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.

## 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 hub and published to a stream 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.*

# 1.5 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. The License Enabler File (LEF) defines the terms of your license and the access types that you can allocate to users. There are two license types: one that is user-based and one that is token-based.
    - User-based license: you can allocate professional access and analyzer access. The LEF determines the distribution of the two access types.
    - Token-based license: you can allocate user access and login access. The LEF determines the number of tokens that you can allocate to the two access types.

   An access type allows users to access streams and apps within a Qlik Sense site.

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

See: *Managing user access (page 255)*

See: *Managing professional access (page 246)*

## 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.*

# 1.6 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.*

## Keyboard shortcuts in QMC

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

| **Shortcut** | **Action** |
|---|---|
| Esc | Close a filter dialog |
| Up arrow | Scroll up in tables |
| 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 | Go back in navigation |
| | Mac OS only: Delete selected item |
| **In tables** | |
| Ctrl+A | Select all rows in the table<br>*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.* |
| Esc | Deselect all selected rows |
| S | Open the Search popover |
| C | Open the Column selector |
| R | Refresh the table |
| **On overview pages** | |
| Enter | Edit the selected rows |
| Delete | Delete the selected rows |
| **On edit pages** | |

| | |
|---|---|
| Esc | Undo all changes, equivalent to clicking Cancel |
| Ctrl+S | Save and apply all the changes, equivalent to clicking Apply |
| **In confirmation dialogs** | |
| Esc | Cancel |
| Enter | OK |

## 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.

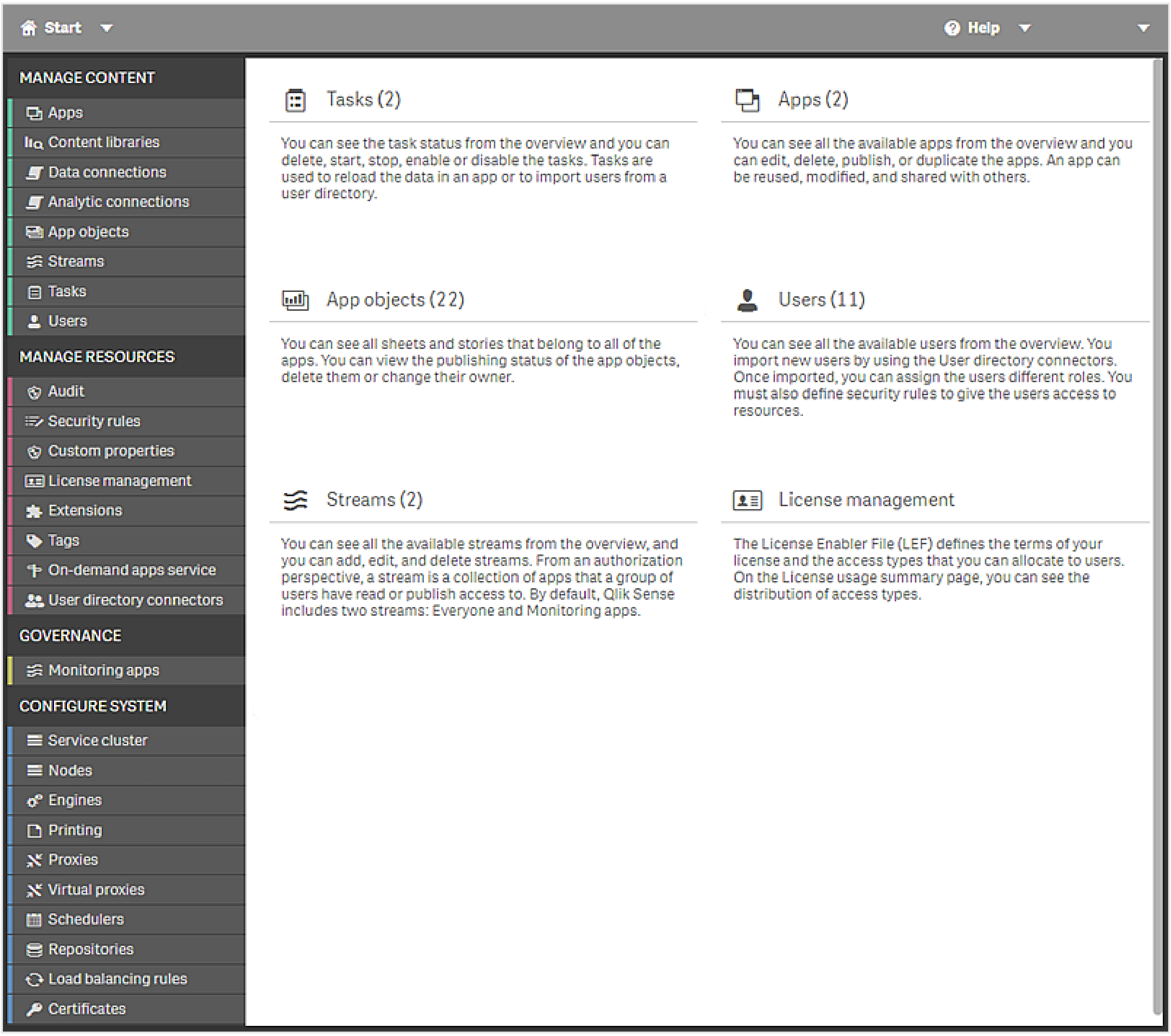
| | |
|---|---|
| ⊕ | Create new |
| 🗗 | Apps |
| 🔍 | Content libraries |
| 📜 | Data connections |
| 📜 | Analytic connections |
| 📊 | App objects |
| ≋ | Streams |
| 📋 | Tasks |
| 👤 | Users |
| 🛡 | Audit |
| ☰✎ | Security rules |
| 🛡 | Custom properties |
| 🪪 | License management |
| 🧩 | Extensions |
| 🏷 | Tags |
| 🪧 | On-demand apps service |
| 👥 | User directory connectors |
| ≋ | Monitoring apps |

| | |
|---|---|
| ≣ | Service cluster |
| ≣ | Nodes |
| ⚙ | Engines |
| 🗋 | Printing |
| ⤡ | Proxies |
| ⤡ | Virtual proxies |
| 📅 | Schedulers |
| 🛢 | Repositories |
| 🔄 | Load balancing rules |
| 🔑 | Certificates |
| 🔗 | 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 |
| ℹ | Information |
| ! | Information |
| 🔒 | Locked |

| | |
|---|---|
| 🔓 | Unlocked |
| 🔍 | Search |
| ↶ | Undo |
| ⚙ | Settings |
| ▲ | Arrow up |
| ▼ | Arrow down |
| ◀ | Arrow left |
| ▶ | Arrow right |

## 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.



Tasks (2)

You can see the task status from the overview and you can delete, start, stop, enable or disable the tasks. Tasks are used to reload the data in an app or to import users from a user directory.

Apps (2)

You can see all the available apps from the overview and you can edit, delete, publish, or duplicate the apps. An app can be reused, modified, and shared with others.

App objects (22)

You can see all sheets and stories that belong to all of the apps. You can view the publishing status of the app objects, delete them or change their owner.

Users (11)

You can see all the available users from the overview. You import new users by using the User directory connectors. Once imported, you can assign the users different roles. You must also define security rules to give the users access to resources.

Streams (2)

You can see all the available streams from the overview, and you can add, edit, and delete streams. From an authorization perspective, a stream is a collection of apps that a group of users have read or publish access to. By default, Qlik Sense includes two streams: Everyone and Monitoring apps.

License management

The License Enabler File (LEF) defines the terms of your license and the access types that you can allocate to users. On the License usage summary page, you can see the distribution of access types.

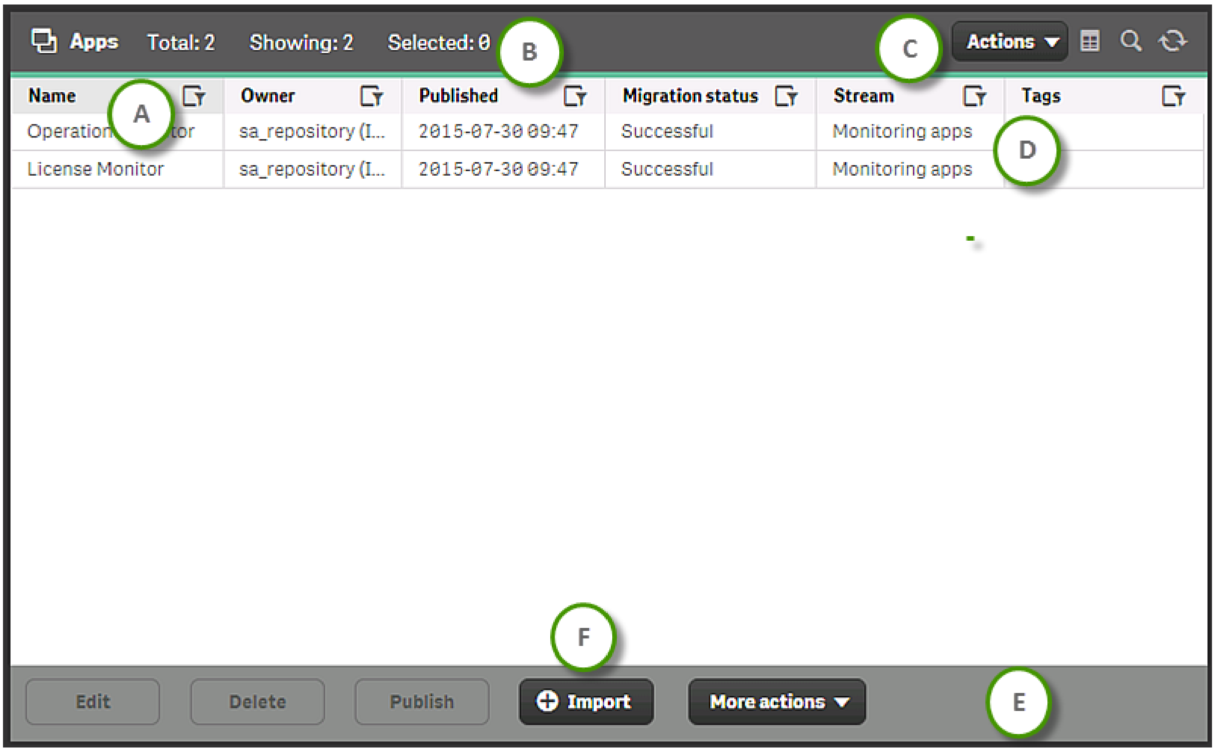
*The QMC start page*

| **QMC start page** | |
|---|---|
| A | The top bar is displayed from all pages to enable you to navigate the QMC efficiently. The following is possible:<br>Click 🏠 **Start** to access the QMC start page.<br>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.<br>Click ❓ **Help** to access the (QMC) help.<br>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.<br>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. The number in parentheses indicates the number of occurrences of 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.



| Name | Owner | Published | Migration status | Stream | Tags |
|---|---|---|---|---|---|
| Operations Monitor | sa_repository (I... | 2015-07-30 09:47 | Successful | Monitoring apps | |
| License Monitor | sa_repository (I... | 2015-07-30 09:47 | Successful | Monitoring apps | |

*Apps overview page*

| Apps overview | |
|---|---|
| A | Click a column heading to sort that column ascending ▼ or descending ▲ .<br>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, you get a summary of the status of the current data set.<br>**Total**: shows the total number of resources.<br>**Showing**: shows the number of resources currently displayed.<br>**Selected**: shows the number of selected resources. |

| | |
|---|---|
| C | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.*<br>Click ▤ to open the **Column selector**, where you can select which columns to display in the overview. Click ↩ to reset to default columns. |
| 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.<br>When you do not have update rights for the selected items, **Edit** is replaced by **View**.<br>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.<br>In this example, click ⊕ **Import** to open the **Import app** dialog. |

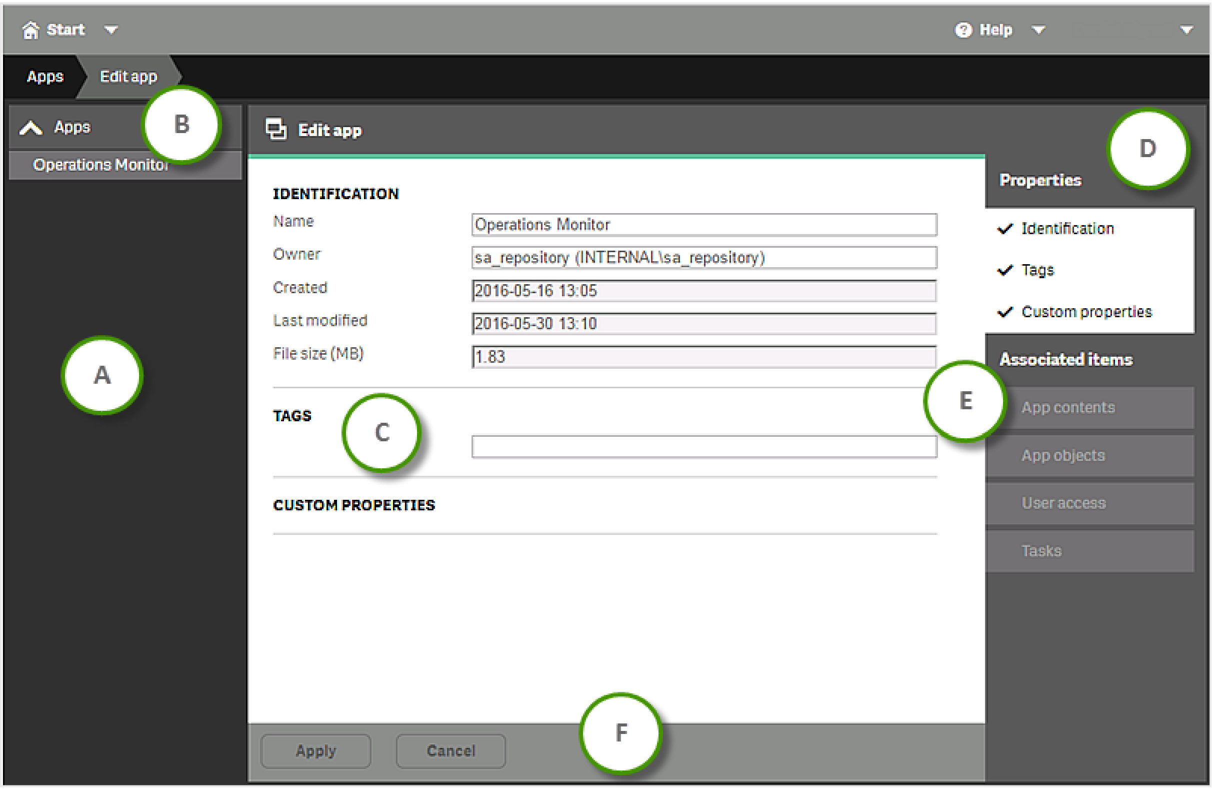
### Selections

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.



| | |
|---|---|
| Name | Operations Monitor |
| Owner | sa_repository (INTERNAL\sa_repository) |
| Created | 2016-05-16 13:05 |
| Last modified | 2016-05-30 13:10 |
| File size (MB) | 1.83 |

*Example: The Edit app page*

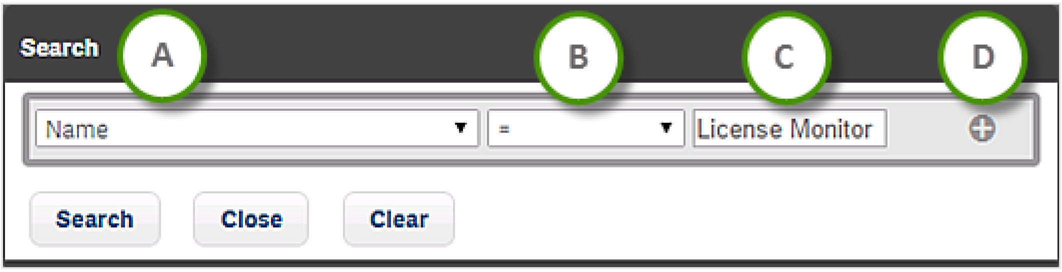
| Edit app | |
|---|---|
| A | The selections panel, to the left, displays the resources you are currently editing. You can edit several resources at the same time to manage the QMC content efficiently. |
| B | Click **Apps** to return to the overview page where you can change your selection. |
| C | 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.

## Search options

The following four options are available when you open search.



| 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.

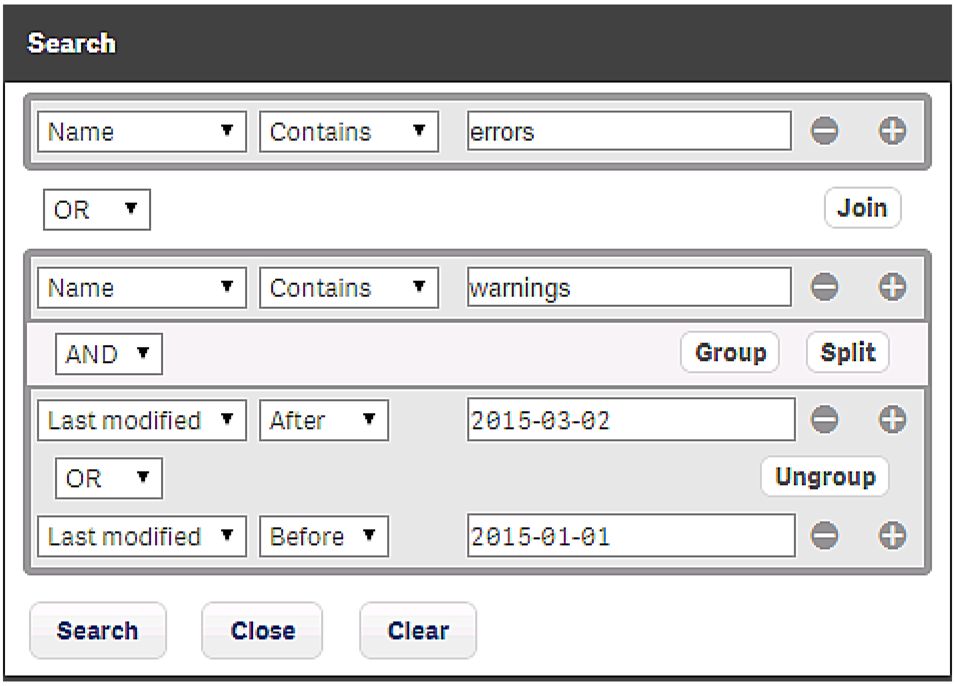
*You clear search and filters by clicking* ⊗ *in the table header.*

## 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.



Name ▼ Contains ▼ errors ⊖ ⊕

OR ▼ Join

Name ▼ Contains ▼ warnings ⊖ ⊕

AND ▼ Group Split

Last modified ▼ After ▼ 2015-03-02 ⊖ ⊕

OR ▼ Ungroup

Last modified ▼ Before ▼ 2015-01-01 ⊖ ⊕

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, or, when available, select a predefined value.

3. Click outside of the filter dialog (or press Esc) to close the dialog.
   ▼ indicates that a filter is applied to the column.

The table shows the matching items.

# 2 QMC resources overview

All resources that are available in the QMC are described briefly in the following table.

| 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.<br>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. |
| **Content libraries** | A content library is a storage that enables the Qlik Sense users to add shared contents to their apps.<br>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.<br>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.<br>*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:<br>• Sheets<br>• Stories<br>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**.<br>An app can be published to only one stream. To publish an app to another stream, the app must first be duplicated and then published to the other stream.<br>*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 two types of tasks:<br>• Reload<br>• User synchronization<br>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:<br>• Scheduled<br>• Task event |
| **Users** | Users are imported from a user directory via a user directory connector in the QMC. |
| **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** | The License Enabler File (LEF) defines the terms of your license and the access types that you can allocate to users. There are two license types: one that is user-based and one that is token-based.<br>• User-based license: you can allocate professional access and analyzer access. The LEF determines the distribution of the two access types.<br>• Token-based license: you can allocate user access and login access. The LEF determines the number of tokens that you can allocate to the two access types.<br>An access type allows users to access streams and apps within a Qlik Sense site. |
| **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 LDAP, Microsoft Active Directory, ApacheDS, ODBC, Access (via ODBC), Excel (via ODBC), SQL (via ODBC), and Teradata (via ODBC).<br>*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. You can use professional access rules or analyzer access rules (user-based license) or user access rules or login access rules (token-based license) to allocate access. Alternatively, a local user can first log on to be recognized as a user, and then be allocated tokens.*<br>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.<br>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.<br>*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.*<br>*In a multi-node installation, you manage the whole Qlik Sense 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 master, slave, 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 define the nodes' access rights to resources. |
| **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. |

## 2.1 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 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 app. |
| **Owner** | The owner of the app. |
| **Published** | The date that the app was published. |
| **Migration status** | This field is only relevant when you manually migrate apps that have not been automatically migrated. |
| **Stream** | The stream that the app is published to. |
| **Tags** | The tags that are connected to the app. |
| **Description** | The app description, if any. |
| **File size (MB)** | The file size of the app.<br>*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** | The 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. |
| ▼▲ | 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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |

| | |
|---|---|
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.<br>See: *Searching and filtering in the QMC (page 33)* |
| 🔄 | 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.<br>*In a multi-node site, where the Qlik Sense scheduler service (QSS) on the central node runs as master and the QSSs on the rim nodes run as slaves, 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 master QSS to the slave QSSs. The second time the action is performed, the task will work.* |

| | |
|---|---|
| **More actions** > **Create new reload task** | Create a new reload task. |
| **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 following tables present the available fields and buttons 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.*

### 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.

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

| 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:<br>• **Not approved**: The app object is not approved because it was added to a published app.<br>• **Approved**: The app object is approved because it belonged to the app when the app was published. |
| **Published** | The status of the app object:<br>• **Not published**: The app object is not published to a stream.<br>• **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. |
| **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.

| 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. |
| **Task session timeout (minutes)** | The time limit for task session timeout. |
| **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 reload 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. Select **Apps** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the app that you want to upload images to and click **Edit**.
3. On the **App edit** page, under **Associated items**, select **App contents**.
4. Click ⊕ **Upload**.
   A file selection dialog is displayed.
5. 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.

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

## 2.2 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.*

| | |
|---|---|
| **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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>ⓘ *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.<br>See: *Searching and filtering in the QMC (page 33)* |
| 🔄 | 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. |

|  |  |
|---|---|
| ⊕ **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 following tables present the available fields and buttons 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.*

### 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 contains the properties for the contents in the content library.

| 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** | 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. |

### 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.

| 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 page is displayed.

## 2.3 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.

*If the **Data connections** overview contains a connection called DM, that connection is for Qlik DataMarket internal use.*

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 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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.<br>See: *Searching and filtering in the QMC (page 33)* |
| ⟳ | 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 following tables present the available fields and buttons 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.

### 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.

| **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 security rule edit page is displayed.

## 2.4 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.

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.*

| | |
|---|---|
| **Name** | Name of the analytic connection. Must be unique. 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). |
| **Certificate file path** | The full path to the certificate. 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.<br>*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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>ⓘ *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.<br>See: *Searching and filtering in the QMC (page 33)* |
| 🔄 | 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. |

## 2.5 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.*

| | |
|---|---|
| **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:<br>• **Not approved**: The app object is not approved because it was added to a published app.<br>• **Approved**: The app object is approved because it belonged to the app when the app was published. |
| **Published** | The status of the app object:<br>• **Not published**: The app object is not published to a stream.<br>• **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. |
| **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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.<br>See: *Searching and filtering in the QMC (page 33)* |
| 🔄 | 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 following tables present the available fields and buttons for the associated items. 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.

## 2.6 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. To publish an app to another stream, the app must first be duplicated and then published to the other stream.

*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.*

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 Qlik Sense Cloud. |
| **Last successfully finished sync** | The date and time of the last successfully finished sync to Qlik Sense Cloud. |
| **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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>ⓘ *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.<br>See: *Searching and filtering in the QMC (page 33)* |
| ⟳ | 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 following tables present the available fields and buttons 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.*

### 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.

| 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.

| 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.

## 2.7 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 two types of tasks:

- Reload
- User synchronization

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.*

| | |
|---|---|
| **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:<br>- Reload (for app)<br>- User synchronization (for user directory connector) |
| **Enabled** | Status values: **Yes** or **No**. |
| **Status** | The status of the task:<br>••• Never started<br>⟳ Triggered<br>⟳ Started<br>⌛ Queued<br>⟳ Abort initiated<br>⟳ Aborting<br>☒ Aborted<br>✓ Success<br>✗ Failed<br>••• Skipped<br>⟳ Retrying<br>✗ Error<br>••• Reset<br>Click ⓘ to open a summary of the latest reload or user synchronization tasks.<br>See: *Task status information (page 64)* |
| **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:<br>- **On task event trigger**: The task execution is initiated by the completion of another task.<br>- **On multiple triggers**: The task has more than one trigger applied.<br>- The date and time for the next execution of the task is displayed if the task has a scheduled trigger applied.<br>- 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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>ⓘ *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.<br>See: *Searching and filtering in the QMC (page 33)* |
| ⟳ | Refresh the page. |
| **Edit** | Edit the selected task. |
| **Delete** | Delete the selected tasks. |
| **Start** | Start the selected tasks. |
| **Stop** | Stop the selected tasks. |
| ⊕ **Create new** | Create a new reload task. |

| | |
|---|---|
| **More actions > Enable** | Enable the selected tasks. |
| **More actions > Disable** | Disable the selected tasks. |
| **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.*

## Reload task: associated items

The following associated items are available for reload 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.

| 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. |

| Property | Description |
|---|---|
| **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 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. |
| **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.<br>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.

# 2.8 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.*

| | |
|---|---|
| **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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.<br>See: *Searching and filtering in the QMC (page 33)* |
| ⟳ | 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

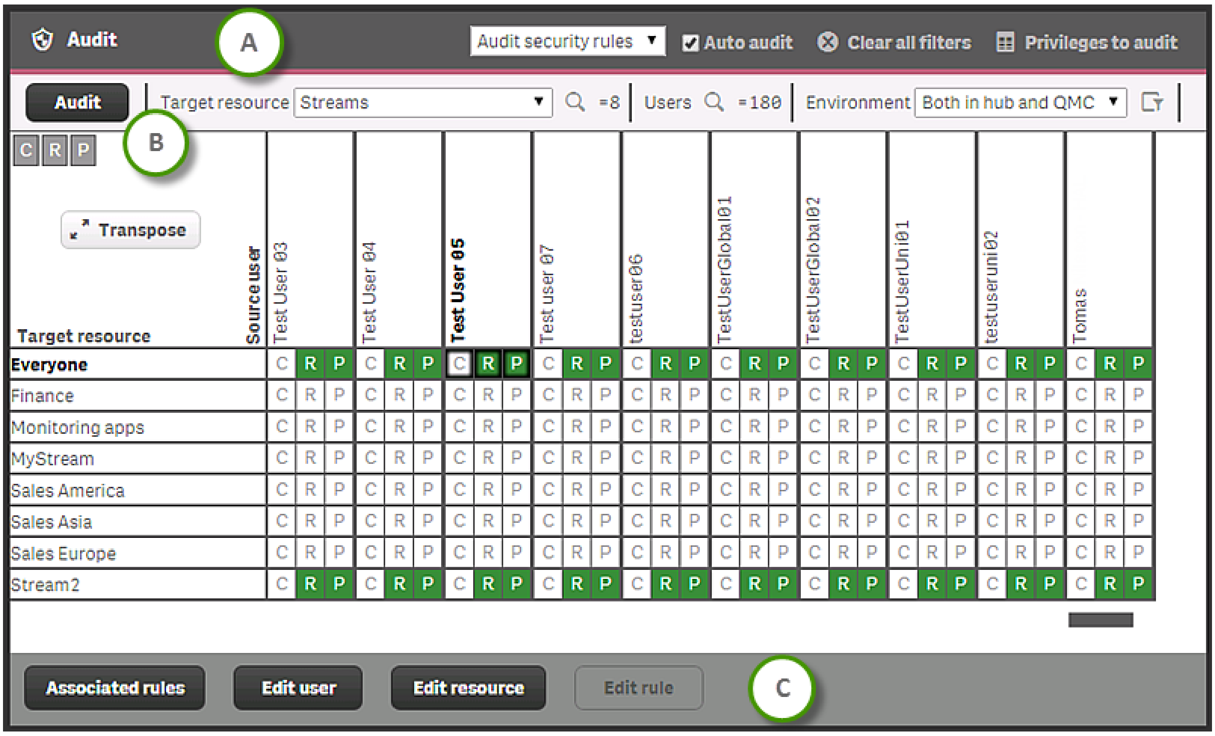
**Owned items** is available from **Associated items** when you edit users. The overview contains a list of the resources owned by the selected users.

| 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.

## 2.9 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.



| Target resource \ Source user | Test User 03 | Test User 04 | Test User 05 | Test user 07 | testuser06 | TestUserGlobal01 | TestUserGlobal02 | TestUserUni01 | testuseruni02 | Tomas |
|---|---|---|---|---|---|---|---|---|---|---|
| Everyone | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P |
| Finance | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P |
| Monitoring apps | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P |
| MyStream | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P |
| Sales America | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P |
| Sales Asia | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P |
| Sales Europe | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P |
| Stream2 | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P | C R P |

*Audit page with a query on* ***Streams***

<table>
<tr><th colspan="2">Audit overview</th></tr>
<tr><td>A (Heading bar)</td><td>

**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.

<table>
<tr><th>Action</th><th>Description</th></tr>
<tr><td><b>C</b>: <b>Create</b></td><td>Create resource</td></tr>
<tr><td><b>R</b>: <b>Read</b></td><td>Read resource</td></tr>
<tr><td><b>U</b>: <b>Update</b></td><td>Update resource</td></tr>
<tr><td><b>D</b>: <b>Delete</b></td><td>Delete resource</td></tr>
<tr><td><b>E</b>: <b>Export</b></td><td>Export an app</td></tr>
<tr><td><b>A</b>: <b>Export data</b></td><td>Export app data</td></tr>
<tr><td><b>T</b>: <b>Duplicate</b></td><td>Duplicate an app</td></tr>
<tr><td><b>M</b>: <b>Access offline</b></td><td>Access apps offline</td></tr>
<tr><td><b>P</b>: <b>Publish</b></td><td>Publish a resource to a stream</td></tr>
<tr><td><b>O</b>: <b>Change owner</b></td><td>Change the owner of a resource</td></tr>
<tr><td><b>B</b>: <b>Load balancing</b></td><td>Control to which nodes that apps are load balanced</td></tr>
<tr><td><b>L</b>: <b>Login access</b></td><td>Login access to a resource</td></tr>
</table>

</td></tr>
</table>

| **Audit overview** | |
|---|---|
| B (Audit bar) | **Audit**: Click **Audit** when you have selected target resource, users, and environment.<br>**Target resource**: Select the resource to audit. Resources include the following:<br>- Analytic connections<br>- Apps<br>- Content libraries<br>- Data connections<br>- App objects<br>- Streams<br>- Reload tasks<br>- User synchronization tasks<br>- Users<br>- Security rules<br>- Extensions<br>- User directory connectors<br>- Nodes<br>- Login access (only for license rule audit)<br>License rules audit is always on login access.<br>**Users**: Click 🔍 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.<br>See: *Searching and filtering in the QMC (page 33)*<br>**Environment**: Select the context for the audit.<br>⧩ : Simulate user environment.<br>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.<br>**Example:**<br>`OS=Windows;`<br>`IP=10.88.3.35;`<br>`Browser= Firefox;` |

| Audit overview | |
| --- | --- |
| C (Action bar) | **Associated rules**: Click to show the security rules that give access to the user/target combination.<br>**Edit user**: Click to edit the selected user.<br>**Edit resource**: Click to edit the selected resource.<br>**Edit rule**: Click to edit the selected rule. (Only available when an associated rule has been selected.)<br>**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.<br>*If you do not have editing rights, the **Edit user** and **Edit resource** buttons are replaced by **View user** and **View resource** buttons.* |

*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.

See: *Editing security rules (page 474)*, *Editing load balancing rules (page 418)* and *Editing a license rule (page 267)*

## 2.10 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.*

| | |
|---|---|
| **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.<br>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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |

| | |
|---|---|
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.<br>See: *Searching and filtering in the QMC (page 33)* |
| 🔄 | 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.

| **Action** | **Description** |
|---|---|
| Create | Create resource. |
| Read | Read resource. |
| Update | Update resource. |

| Action | Description |
|---|---|
| Delete | Delete resource. |
| Export | Export an app from Qlik Sense Enterprise into a qvf file. |
| Publish | Publish a resource to a stream. |
| 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:<br>"Export as image" for visualizations.<br>"Export as PDF" for visualizations.<br>"Export data" for visualizations.<br>"Export sheet" in the menu.<br>"Export story" in storytelling.<br>*You cannot grant access to only a subset of these actions.*<br>*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 installed in Qlik Sense (page 425).* |
| 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)))]
```

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

| 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**.<br>You can also use predefined functions for conditions to return property values. |
| resourcetypevalue | You must provide at least one resource type value. |
| property | The property name for the resource condition. See *Properties (page 74)* 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

| Property | Description | Example |
|---|---|---|
| resource.@<customproperty> | Custom property associated with the resource. In the examples, @Department is the custom property name. | `resource.@Department = Finance`.<br>`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

| Property | Description | Example |
|---|---|---|
| user.email<br>owner.email | Email of the user.<br>Email of the owner. | `user.email="user@domain.com"`<br>`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. | See: *Security rules example: Access to stream by IP address (page 491)* |

| | | |
|---|---|---|
| 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<br>owner.group | Group that the user belongs to.<br>Group that the owner belongs to. | user.group=resource.app.stream.@AdminGroup<br>owner.group=@Developers |
| user.userdirectory<br>owner.userdirectory | User directory that the user belongs to.<br>User directory that the owner belongs to. | user.userdirectory="Employees"<br>owner.userdirectory="Employees" |
| user.userId<br>owner.userId | ID of the user.<br>ID of the owner. | user.userId="<userID>"<br>owner.userId="<ownerID>" |
| user.roles<br>owner.roles | Roles of the user.<br>Roles of the owner. | user.roles="AuditAdmin"<br>owner.roles="SystemAdmin" |

## Resource app

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

## Resource app.object

| 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:<br>• app_appscript<br>• dimension<br>• embeddedsnapshot<br>• genericvariableentry<br>• hiddenbookmark<br>• masterobject<br>• measure<br>• sheet<br>• snapshot<br>• story<br>• bookmark | `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

| 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

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

## Resource SystemRule

| Property | Description | Example |
|---|---|---|
| Category | System rule category.<br>Possible values:<br>• Security<br>• License<br>• 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.<br>Possible values:<br>• BothQlikSenseAndQMC<br>• QlikSenseOnly<br>• QMCOnly | `resource.rulecontext="BothQlikSenseAndQMC"` |
| Type | Type of rule.<br>Possible values:<br>• Default<br>• Read only<br>• Custom | `resource.type!="custom"` |

## Resource ContentLibrary

| Property | Description | Example |
|---|---|---|

| | | |
|---|---|---|
| Type | Possible values:<br>• media | `resource.type="media"` |

## Resource ServerNodeConfiguration

| 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

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

## Resource UserSyncTask

| 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

| 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:

| Example | Result |
|---|---|
| **Resource filter:** App*<br>**Conditions:**`resource.resourcetype="App" and (resource.name like "*")` | The rule will apply to all apps.<br>*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*<br>**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**<br>= `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_*`<br>`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**=`*`<br>and Conditions field empty | This rule will apply to all resources and all users. |
| user.name="MyUserName" | The rule will apply to the user with the user name MyUserName.<br>*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.* |

| Example | Result |
|---|---|
| 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<br>resource.name="My*" and<br>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 **Advanced** 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

| 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**.<br>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.<br>Cannot be used in conjunction with '**_***' option. |

| Argument | Description |
|---|---|
| _* | 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.<br>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.<br>Cannot be used in conjunction with the '*' option. |

## Properties

| Property | Security rule will be applied to |
|---|---|
| App | Apps |
| App.Object | Objects<br>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:

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

| Example | Result |
|---|---|
| `App*, Streams*, App.Object*`<br>`resource.resourcetype="App.Object" and`<br>`(((resource.objectType="sheet")))` | The rule will apply to apps, streams and sheets.<br>*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:<br>**Resource*** `App*`<br>**Conditions*** `resource.resourcetype="App" and ( )`<br>*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.* |

## 2.11 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.*

| | |
|---|---|
| **Name** | The name of the custom property, defined from the QMC. |
| **Resource types** | The resource types that the custom property is available for. |
| **ID** | The customer property ID. |
| **Created** | The date and time when the custom property was created. |
| **Last modified** | The 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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.*

## 2.12 License management

The License Enabler File (LEF) defines the terms of your license and the access types that you can allocate to users. There are two license types: one that is user-based and one that is token-based.

- User-based license: you can allocate professional access and analyzer access. The LEF determines the distribution of the two access types.

- Token-based license: you can allocate user access and login access. The LEF determines the number of tokens that you can allocate to the two access types.

An access type allows users to access streams and apps within a Qlik Sense site.

- 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 **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.
- The **Qlik DataMarket** page is where you activate or apply changes to the Qlik DataMarket subscription.

## Professional access allocations

You allocate professional access 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.

There is a direct relationship between the access type (professional access) and the user. If you deallocate professional 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 professional access is released immediately. You can reinstate quarantined professional access, to the same user, within seven days.

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.*

| | |
|---|---|
| **Name** | Name of the user with an allocated (or quarantined) professional access.<br>**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. |
| **Status** | Status of the professional access:<br>**Allocated** means that professional access is allocated to the identified user and the user can access the hub and apps.<br>**Quarantined** means the following:<br>• The user cannot access streams and apps on the hub.<br>• Professional access was previously allocated to the user and thereafter deallocated.<br>• During the quarantine period, professional access can be reinstated to the original user. |
| **Last used** | Date and time when the user accessed the hub. |
| **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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |

| | |
|---|---|
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.<br>See: *Searching and filtering in the QMC (page 33)* |
| 🔄 | 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.*

| | |
|---|---|
| **Name** | Name of the professional access rule. |
| **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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>ⓘ *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.<br>See: *Searching and filtering in the QMC (page 33)* |
| ⟳ | Refresh the page. |
| **Edit** | Edit the selected professional access rule. |
| **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

You allocate analyzer access 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 stories based on data in apps. The user can also create bookmarks, print objects, stories, and sheets, and export data from an object to Excel.

There is a direct relationship between the access type (analyzer access) and the user. If you deallocate analyzer access from a user, the access type is put in quarantine, given that 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 **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.*

| | |
|---|---|
| **Name** | Name of the user with an allocated (or quarantined) analyzer access.<br>**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. |

| | |
|---|---|
| **Status** | Status of the analyzer access:<br>**Allocated** means that analyzer access is allocated to the identified user and the user can access the hub and apps.<br>**Quarantined** means the following:<br>• The user cannot access streams and apps on the hub.<br>• Analyzer access was previously allocated to the user and thereafter deallocated.<br>• During the quarantine period, analyzer access can be reinstated to the original user. |
| **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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>ⓘ *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.<br>See: *Searching and filtering in the QMC (page 33)* |

| | |
|---|---|
| ↻ | 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.*

| | |
|---|---|
| **Name** | Name of the analyzer access rule. |
| **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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.<br>See: *Searching and filtering in the QMC (page 33)* |
| ↻ | Refresh the page. |
| **Edit** | Edit the selected analyzer access rule. |
| **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.*

## 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.*

| | |
|---|---|
| **Name** | The name of the user with an allocated (or quarantined) user access.<br>**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:<br>**Allocated** means that user access is allocated to the identified user and the user can access the hub and apps.<br>**Quarantined** means the following:<br>• The user cannot access streams and apps on the hub.<br>• User access was previously allocated to the user and thereafter deallocated.<br>• The token is not available for new allocation until the end of the quarantine period (seven days).<br>• 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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>ⓘ *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.<br>See: *Searching and filtering in the QMC (page 33)* |
| 🔄 | 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.*

| | |
|---|---|
| **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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.<br>See: *Searching and filtering in the QMC (page 33)* |
| 🔄 | Refresh the page. |
| **Edit** | Edit the selected user access rule. |
| **Delete** | Delete the selected user access rules. |
| ⊕ **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 rule: 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.

# 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 (▦) to add fields.

| | |
|---|---|
| **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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.<br>See: *Searching and filtering in the QMC (page 33)* |
| 🔄 | Refresh the page. |
| **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 rule: 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.

| **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. |

| Property name | Description |
|---|---|
| **ID** | The ID of the license rule. |
| **Created** | Date and time when the license rule was created. |
| **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.

The tokens are the only purchasable Qlik Sense license. 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.

| 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. |

## 2.13 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.*

| | |
|---|---|
| **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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.<br>See: *Searching and filtering in the QMC (page 33)* |
| ⟳ | Refresh the page. |
| **Edit** | Edit the selected extensions. |
| **Delete** | Delete the selected extensions. |

| | |
|---|---|
| ⊕ **Import** | Import a new extension.<br>⚠ *Do not import extensions with the same name as a native object, it is not supported.* |
| **Export** | Export an extension.<br>ⓘ *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 following tables present the available fields and buttons 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.

### 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.

| 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.

## 2.14 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.*

| | |
|---|---|
| **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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.<br>See: *Searching and filtering in the QMC (page 33)* |
| ⟳ | 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.*

## 2.15 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 are published to streams from the QMC. Generated on-demand apps can also be published from the QMC.

*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 | Description |
|---|---|
| **Enable on-demand app service** | Enables and disables the On-demand app service. The service is disabled by default.<br>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. |
| **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.<br>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.<br>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 engine, the load on that Qlik 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.<br>The On-demand app service keeps data about navigation links and about requests to generate and reload on-demand apps.<br>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.<br>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.<br>See: *Anonymous authentication (page 389)*<br>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.<br>⚠ *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".*<br>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.<br>The time is measured from the last data load.<br>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.<br>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.<br>*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.* |

## 2.16 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 LDAP, Microsoft 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. You can use professional access rules or analyzer access rules (user-based license) or user access rules or login access rules (token-based license) to allocate access. Alternatively, a local user can first log on to be recognized as a user, and then be allocated tokens.*

*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".*

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.

| | |
|---|---|
| **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:<br>- Entered manually for ODBC and LDAP.<br>- Generated from the connector's properties for Active Directory.<br>*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, 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.<br>*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:<br>- **Idle**: When no synchronization is performed.<br>- **External fetch**: The first phase of the synchronization, when fetching the data from the directory service.<br>- **Database store**: The second phase of the synchronization, when storing the data in the QRS.<br>*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 successfully finished sync** | The date and time when synchronization of user data last finished successfully. |
| **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.<br>• 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.<br>• 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**, or **Generic LDAP** if you only want to synchronize a selection of users.<br>ⓘ *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** | By whom the user directory connector 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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>ⓘ *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.<br>See: *Searching and filtering in the QMC (page 33)* |
| 🔄 | Refresh the page.<br>*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.

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

## User sync settings

| 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.<br>- 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**, or **Generic LDAP** if you only want to synchronize a selection of users.<br>ⓘ *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**<br>ⓘ *Not entered manually for Active Directory.* | 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. | |
| **Path** | The URI used to connect to the directory server. To support SSL, specify the protocol as LDAPS instead. (Currently LDAPS is only supported for AD). | 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.

| 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.<br>*If the user synchronization is unsuccessful, try setting the value to '0' (zero).* | 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.<br>*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.*<br>This property is only visible for Generic LDAP and Active directory search, (Active Directory always uses optimization). | Not selected |

## Directory entry attributes

*The directory entry attributes are case-sensitive.*

| 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.<br>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.<br>See also the **Group membership** setting, above. | member |

## Tags

| Property | Description |
|---|---|
| **Tags** | *If no tags are available, this property group is empty.*<br>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.

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

## User sync settings

| 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.<br>• 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**, or **Generic LDAP** if you only want to synchronize a selection of users.<br>*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.

| 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.

| 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.<br>*If the user synchronization is unsuccessful, try setting the value to '0' (zero).* | 2000 |

### Tags

| Property | Description |
|---|---|
| **Tags** | *If no tags are available, this property group is empty.*<br>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.

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

## User sync settings

| 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.<br>- 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**, or **Generic LDAP** if you only want to synchronize a selection of users.<br>*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**<br>*Not entered manually for Active Directory.* | 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. | |
| **Path** | The URI used to connect to the directory server. To support SSL, specify the protocol as LDAPS instead. (Currently LDAPS is only supported for AD). | 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.

| 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.<br>*If the user synchronization is unsuccessful, try setting the value to '0' (zero).* | 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.<br>*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.*<br>This property is only visible for Generic LDAP and Active directory search, (Active Directory always uses optimization). | Not selected |

## Directory entry attributes

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

*The directory entry attributes are case-sensitive.*

| 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.<br>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.<br>See also the **Group membership** setting, above. | member |

## Tags

| Property | Description |
|---|---|
| **Tags** | *If no tags are available, this property group is empty.*<br>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.

> *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".*

The following property groups are available for ODBC UDC.

### Identification

All fields are mandatory and must not be empty.

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

### User sync settings

| 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.<br>• 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**, or **Generic LDAP** if you only want to synchronize a selection of users.<br>*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

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

| Property | Description | Defau lt 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*.<br>*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*.<br>*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:<br>• A full connection string, for example: *Driver={SQL Server Native Client 11.0};Server=localhost;Database=Users;Trusted_Connection=yes;*<br>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.<br>2. *Server* must point to the server that you want to connect to.<br>3. *Database* must point to the database where the tables are.<br>4. *Trusted_Connection=yes* may be required, depending on the setup. In this example it is required.<br>• A pointer to an established System DSN, for example, *dsn=MyDSN;*<br>*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.<br>**Example:**<br>Assume that you have a connection string as follows:<br>*Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;Uid=Admin;Pwd=verySecretAdminPassword;*<br>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:<br>Save the first part:<br>*Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;*<br>in the **Visible connection string** field, and the second part:<br>*Uid=Admin;Pwd=verySecretAdminPassword;*<br>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.<br>*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

| Property | Description |
|---|---|
| **Tags** | *If no tags are available, this property group is empty.*<br>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.

| 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. |

# 2.17 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.)*

## 2.18 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.*

| | |
|---|---|
| **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:<br>• **(x) of (y) services are running**<br>The number of services (x) that are running compared to the number of enabled services (y) on the node.<br>• **(x) of (y) services are stopped**<br>The number of services (x) that are stopped compared to the number of enabled services (y) on the node.<br>• **(z) has stopped**<br>The name of the service (z) that has stopped (if only one service has stopped).<br>*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**. |
| **Engine** | Status values: **Yes** or **No**.<br>**Yes**: The Qlik Sense engine service (QES) is active. |
| **Proxy** | Status values: **Yes** or **No**.<br>**Yes**: The Qlik Sense proxy service (QPS) is active. |
| **Printing** | Status values: **Yes** or **No**.<br>**Yes**: The Qlik Sense printing service (QPR) is active. |
| **Scheduler** | Status values: **Yes** or **No**.<br>**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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>ⓘ *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.<br>See: *Searching and filtering in the QMC (page 33)* |
| ↻ | 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.

## 2.19 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.*

| | |
|---|---|
| **Node** | The name of the engine node. |
| **Status** | One of the following statuses is displayed:<br>- **Running**<br>The service is running as per normal.<br>- **Stopped**<br>The service has stopped.<br>- **Disabled**<br>The service has been disabled.<br>*Click ℹ in the* ***Status*** *column for more detailed information on the status.*<br>See: *Checking the status of Qlik Sense services (page 299).* |
| **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. |
| **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.<br>*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.<br>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 ( 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.<br>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.<br>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.<br>⚠ *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. |
| **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 .<br>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.<br>A negative value disables the limit.<br>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.<br>A negative value or 0 disables the limit.<br>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.<br>A negative value or 0 disables the limit.<br>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.<br>A negative value or 0 disables the limit.<br>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.<br>A negative value or 0 disables the limit. |
| **Reload time limit (seconds)** | Limits the CPU time that a reload request can use.<br>A negative value or 0 disables the limit. |
| **Create search index during reload** | Status values: **Yes** or **No**.<br>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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |

| | |
|---|---|
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.<br>See: *Searching and filtering in the QMC (page 33)* |
| 🔄 | 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.*

## 2.20 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.*

| | |
|---|---|
| **Node** | The name of the printing node. |

| | |
|---|---|
| **Status** | One of the following statuses is displayed:<br>• **Running**<br>The service is running as per normal.<br>• **Stopped**<br>The service has stopped.<br>• **Disabled**<br>The service has been disabled.<br>*Click ⓘ in the **Status** column for more detailed information on the status.*<br>See: *Checking the status of Qlik Sense services (page 299).* |
| **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.*

## 2.21 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.*

| | |
|---|---|
| **Node** | The name of the proxy node. |
| **Status** | One of the following statuses is displayed:<br>• **Running**<br>The service is running as per normal.<br>• **Stopped**<br>The service has stopped.<br>• **Disabled**<br>The service has been disabled.<br>*Click ⓘ in the **Status** column for more detailed information on the status.*<br>See: *Checking the status of Qlik Sense services (page 299).* |
| **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.<br>*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**.<br>**Yes**: Unencrypted communication is allowed. This means that both https (secure communication) and (http) unencrypted communication is allowed. |
| **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.<br>*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**.<br>**Yes**: Kerberos authentication is enabled. |

| | |
|---|---|
| **REST API listen port** | The listen port for the proxy API.<br>*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.<br>*When editing a proxy certificate as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.* |
| **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.<br>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.<br>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.<br>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.<br>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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>ⓘ *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.<br>See: *Searching and filtering in the QMC (page 33)* |
| ⟳ | 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.

| Property | Description |
|---|---|
| **Description** | The description of the virtual proxy. |
| **Prefix** | The path name in the proxy's URI that defines each additional path. Example:<br>*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.<br>*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. |

## 2.22 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.*

| | |
|---|---|
| **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. |
| **Is default virtual proxy** | Status values: **Yes** or **No**. |
| **Authentication method** | • **Ticket**: a ticket is used for authentication.<br>• **Header authentication static user directory**: allows static header authentication, where the user directory is set in the QMC.<br>• **Header authentication dynamic user directory**: allows dynamic header authentication, where the user directory is fetched from the header.<br>• SAML: SAML2 is used for authentication.<br>• JWT: JSON Web Token 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 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:<br>• **No anonymous user**<br>• **Allow anonymous user**<br>• **Always anonymous user** |
| **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:<br>`company.com` |

| | |
|---|---|
| **Additional response headers** | Headers added to all HTTP responses back to the client. Example:<br>`Header1: value1`<br>`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**.<br>**Yes**: The following information about the client environment is sent in the security header: OS, device, browser, and IP.<br>**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 attribute 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'. |
| **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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>ⓘ *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.<br>See: *Searching and filtering in the QMC (page 33)* |
| ⟳ | 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.

| | |
|---|---|
| **Node** | The proxy name. |
| **Status** | One of the following statuses is displayed:<br>• **Running**<br>The service is running as per normal.<br>• **Stopped**<br>The service has stopped.<br>• **Disabled**<br>The service has been disabled.<br>*Click ⓘ in the **Status** column for more detailed information on the status.*<br>See: *Checking the status of Qlik Sense services (page 299)*. |
| **Service listen port HTTPS (default)** | The secure listen port for the proxy, which by default manages all Qlik Sense communication.<br>*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**.<br>**Yes**: Unencrypted communication is allowed. This means that both https (secure communication) and (http) unencrypted communication is allowed. |
| **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.<br>*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**.<br>**Yes**: Kerberos authentication is enabled. |
| **REST API listen port** | The listen port for the proxy API.<br>*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.<br>*When editing a proxy certificate as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.* |
| **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.<br>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.<br>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.<br>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.<br>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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Edit** | Edit the selected proxy. |
| **Unlink** | Unlink a proxy service from the selected proxy.<br>ⓘ *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.*

## 2.23 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 master, slave, 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** | The name of the scheduler node. |
| **Status** | One of the following statuses is displayed:<br>- **Running** The service is running as per normal.<br>- **Stopped** The service has stopped.<br>- **Disabled** The service has been disabled.<br>*Click ⓘ in the **Status** column for more detailed information on the status.*<br>See: *Checking the status of Qlik Sense services (page 299).* |
| **Tags** | The tags that are connected to the scheduler. |
| **Type** | - **Master**: sends the task to a slave QSS within the site.<br>- **Slave**: receives the task from the master QSS and executes the task.<br>- **Master and slave**: when the master QSS also acts a slave 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.<br>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.<br>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.<br>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.<br>Each level from **Fatal** to **Debug** includes more information than the previous level. |
| **Security log level** | Security-related messages are saved to this logger.<br>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.<br>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.<br>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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>ⓘ *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.<br>See: *Searching and filtering in the QMC (page 33)* |
| ↻ | 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.*

## 2.24 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** | The name of the repository node. |
| **Status** | One of the following statuses is displayed:<br>- **Running** The service is running as per normal.<br>- **Stopped** The service has stopped.<br>- **Disabled** The service has been disabled.<br>*Click ⓘ in the **Status** column for more detailed information on the status.*<br>See: *Checking the status of Qlik Sense services (page 299).* |
| **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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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. |
| ⏷ | 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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |

| | |
|---|---|
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.<br>See: *Searching and filtering in the QMC (page 33)* |
| ⟳ | 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.*

## 2.25 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.*

| | |
|---|---|
| **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. |
| **Disabled** | Status values: **Yes** or **No**. |

| | |
|---|---|
| **Context** | The rule can be set for either **QMC**, **Hub**, or **Both**. |
| **Type** | The 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** | The tags that are connected to the load balancing rule. |
| **Conditions** | The conditions of the load balancing rule. |
| **ID** | The ID of the load balancing rule. |
| **Created** | The date and time when the load balancing rule was created. |
| **Last modified** | The 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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Actions** | Options for clearing filter and search, selecting and deselecting all rows, and toggling wrapping.<br>*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.<br>See: *Searching and filtering in the QMC (page 33)* |
| 🔄 | 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)

| Property | Description |
|---|---|
| App | 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 | 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**.<br>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.<br>See: *Resource filter (Advanced view) (page 149)* |
| property | The property name for the resource condition, for available names.<br>See: *Properties (page 150)* |
| propertyvalue | The value of the selected property name. |

### Properties

| 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. |
| 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:**

| Example | Result |
|---|---|
| `resource.resourcetype="App" and (resource.name like "*")` | The rule will apply to all apps.<br>*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**=`*`<br>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**.

## 2.26 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.

## 2.27 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.

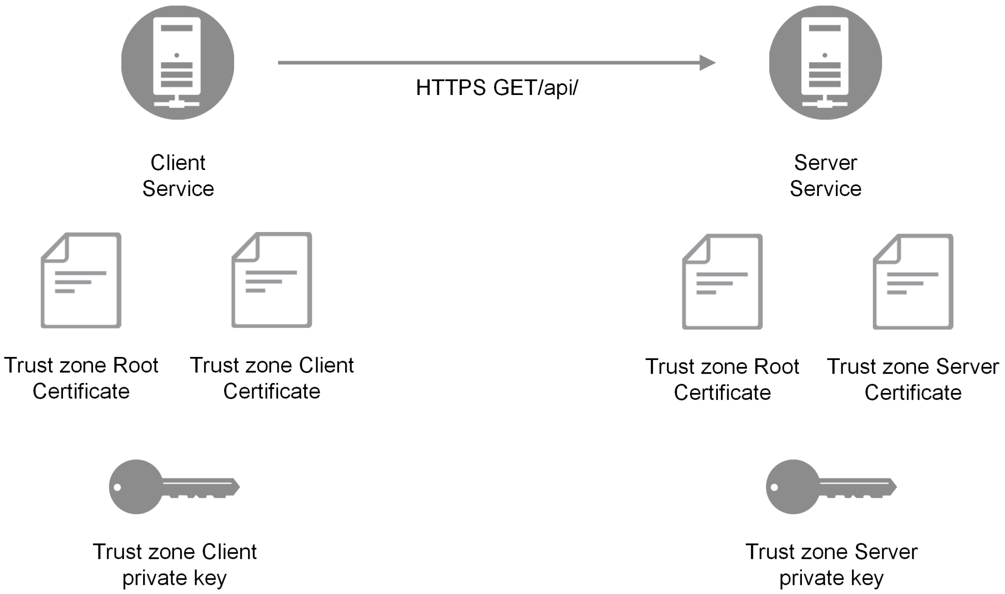
Windows certificate store location: *Local Computer* > *Personal* > *Certificates*.

### 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.

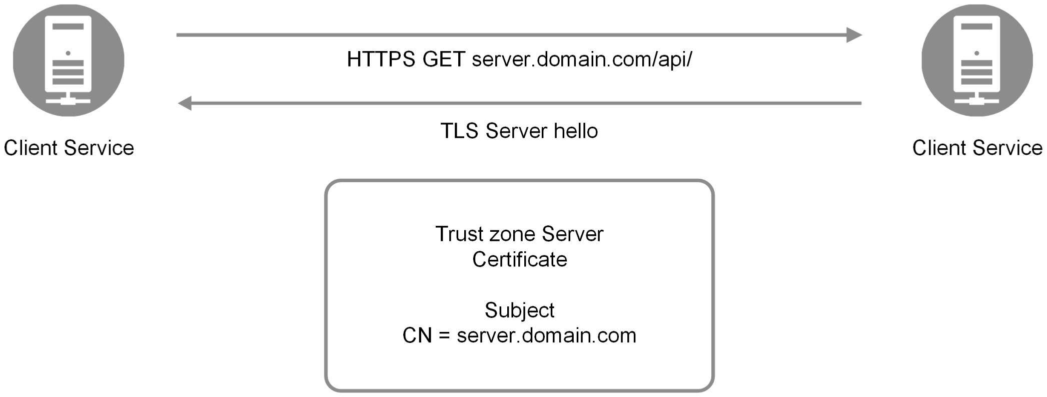
Windows certificate store location: *Local service user* > *Personal Certificates*.

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.


HTTPS GET/api/
Client Service
Server Service
Trust zone Root Certificate
Trust zone Client Certificate
Trust zone Root Certificate
Trust zone Server Certificate
Trust zone Client private key
Trust zone Server private key

*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*

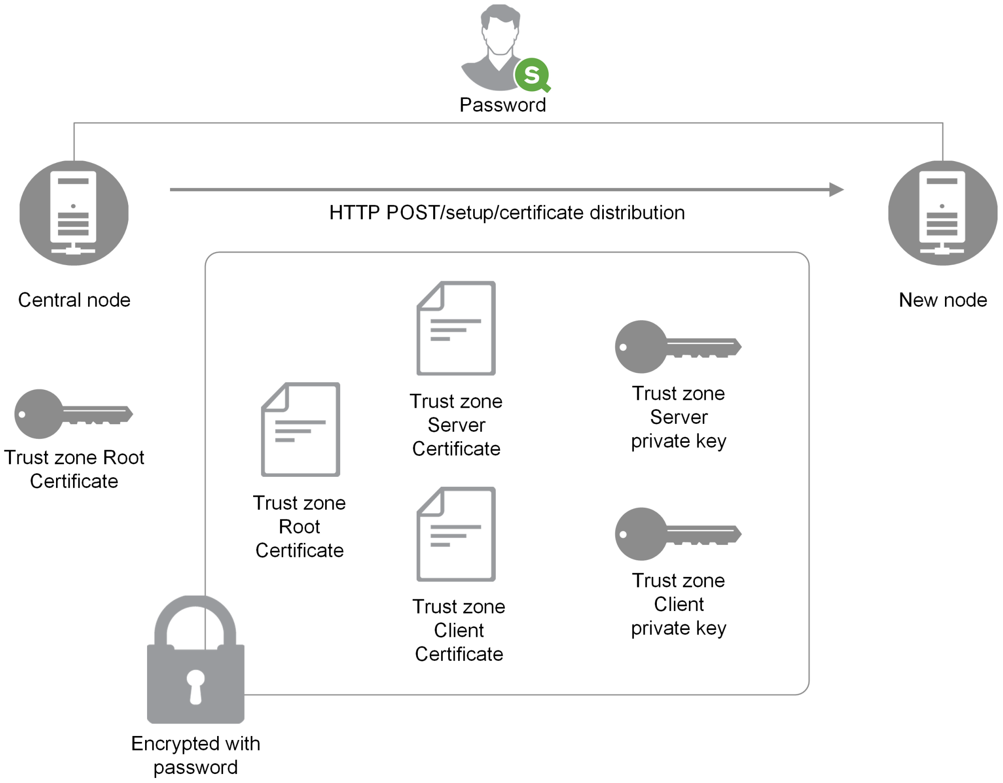
The common name of the server certificate is entered by the administrator during the node registration process in the QMC.

## 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.


Password
HTTP POST/setup/certificate distribution
Central node
New node
Trust zone Root Certificate
Trust zone Root Certificate
Trust zone Server Certificate
Trust zone Server private key
Trust zone Client Certificate
Trust zone Client private key
Encrypted with password

*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.

# 3 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

## 3.1 Managing licenses

### Licenses

The License Enabler File (LEF) defines the terms of your license and the access types that you can allocate to users. There are two license types: one that is user-based and one that is token-based.

- User-based license: you can allocate professional access and analyzer access. The LEF determines the distribution of the two access types.
- Token-based license: you can allocate user access and login access. The LEF determines the number of tokens that you can allocate to the two access types.

An access type allows users to access streams and apps within a Qlik Sense site.

### User-based licenses

User-based licenses grant a predefined number of professional and analyzer access allocations. The distribution of the access types is determined by the LEF.

#### Professional access

You allocate professional access 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. There is a direct relationship between the access type (professional access) and the user. If you deallocate professional 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 professional access is released immediately. You can reinstate quarantined professional access, to the same user, within seven days.

### Summary professional access:

- Assigned to an identified user.
- Daily access to analyze or create content.
- Unlimited access to streams, apps, and other resources.
- Maximum number of parallel sessions is five.

### Analyzer access

You allocate analyzer access 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 stories based on data in apps. The user can also create bookmarks, print objects, stories, and sheets, and export data from an object to Excel. There is a direct relationship between the access type (analyzer access) and the user. If you deallocate analyzer access from a user, the access type is put in quarantine, given that 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.

### Summary analyzer access:

- Assigned to an identified user.
- Daily access to analyze (but not create, edit, or publish), sheets and apps in the hub.
- Can create bookmarks.
- Can print objects, stories, and sheets.
- Can export data from an object to Excel.
- Maximum number of parallel sessions is five.

## 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

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.

### Login access

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 from the License Enabler File (LEF). This makes you the root administrator (RootAdmin) for the Qlik Sense site.

Do the following:

1. Fill out the mandatory 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.

| Property name | Description |
|---|---|
| **Owner name** | The user name of the Qlik Sense product owner. |

| Property name | Description |
|---|---|
| **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. |

2. 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.*

3. Click **Apply** in the action bar to apply and save your changes.
   **Successfully licensed** is displayed.
4. Click **Close**.

You have now activated the license. Next you need to allocate professional access or user access to yourself.

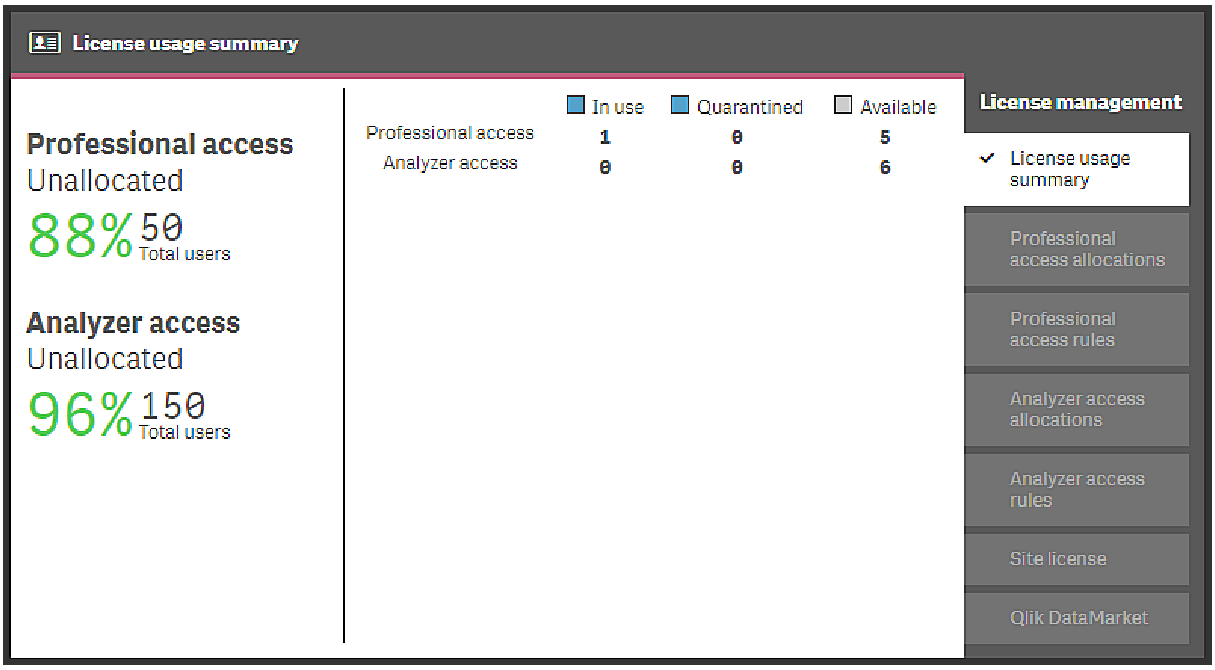
> *You give users access to Qlik Sense by managing the access types: professional or analyzer access (user-based license) or user access or login access (token-based license), according to which consumption model you prefer for accessing Qlik Sense.*

## 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.



License usage summary

**Professional access**
Unallocated
88% 50 Total users

**Analyzer access**
Unallocated
96% 150 Total users

| | 🟦 In use | 🟦 Quarantined | □ Available |
|---|---|---|---|
| Professional access | 1 | 0 | 5 |
| Analyzer access | 0 | 0 | 6 |

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:

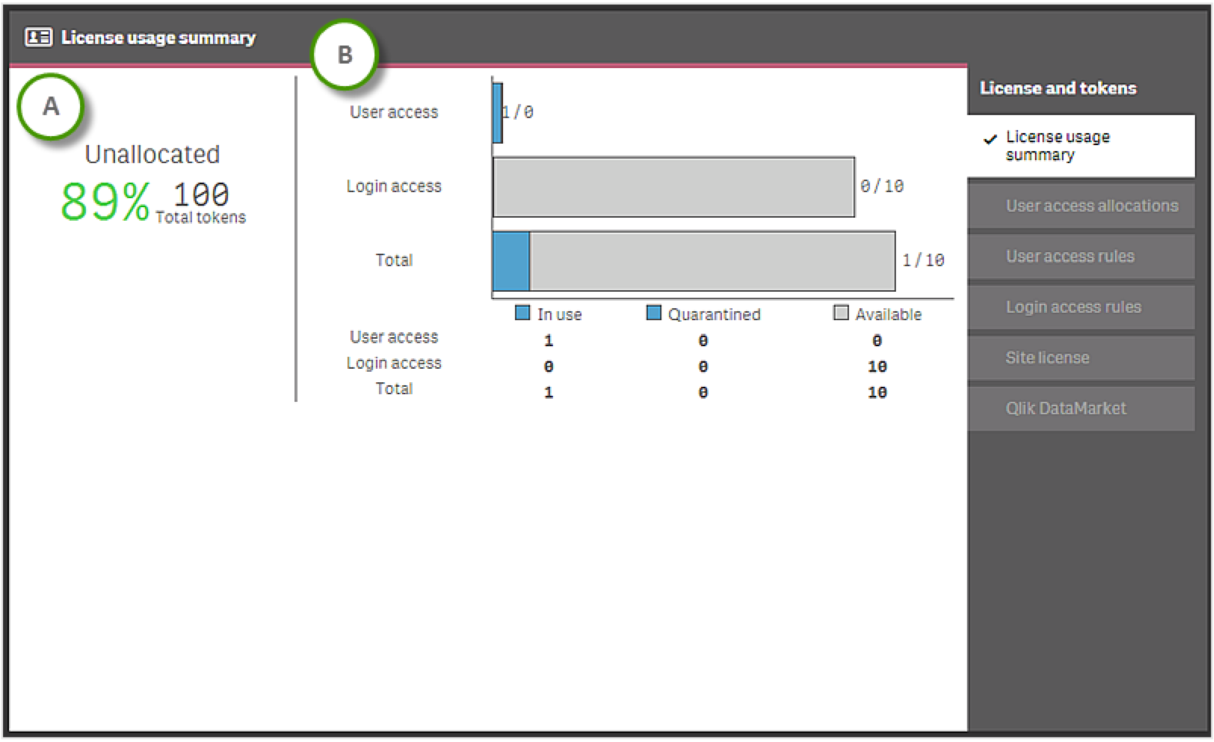
- **Professional access**: the number of professional access allocations to identified users.
- **Analyzer access**: the number of analyzer access allocations to identified users.

Status

- **In use**: the number of access allocations that are currently in use.
- **Quarantined**: 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.



| | ■ In use | ■ Quarantined | □ Available |
|---|---|---|---|
| User access | 1 | 0 | 0 |
| Login access | 0 | 0 | 10 |
| Total | 1 | 0 | 10 |

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.

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.

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. 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.

   | **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.*

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.*

## Activating the Qlik DataMarket license

Before you can use the Qlik DataMarket database, you need to accept the terms and conditions and choose a subscription.

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 **Qlik DataMarket** in the panel to the right.
3. Read the **Terms and conditions** and select **I accept the terms and conditions**.
4. Select one of the subscription options: **Free** or **Licensed subscription**. The option **Free** gives you access to a limited data set. The option **Licensed subscription** requires a license and a License Enabler File (LEF), and gives you access to a larger data set than the free version.
   a. If you select **Free**, you only need to click **Apply** to activate the license.
   b. If you select **Licensed subscription**, continue with the following steps.
5. Fill out the fields. The property group **Site license** contains properties related to the license for Qlik DataMarket. All fields are mandatory.

| Property name | Description |
|---|---|
| **Owner name** | The user name of the Qlik DataMarketproduct owner. |
| **Owner organization** | The name of the organization that the Qlik DataMarket product owner is a member of. |
| **Serial number** | The serial number assigned to the Qlik DataMarket software. |
| **Control number** | The control number assigned to the Qlik DataMarket software. |
| **LEF access** | The LEF file assigned to the Qlik DataMarket software. |

6. 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.

*__Failed to get LEF from server__ is displayed if the serial number or control number is incorrect.*

7. Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.
   **Successfully updated** is displayed.

## Changing the Qlik DataMarket license

After you have activated the Qlik DataMarket license the first time, you can change subscription type and update the license properties.

To change to **Free** subscription, you only need to select **Free** and click **Apply**.

To change to **Licensed subscription**, or to update the license details, you need to enter the license details and add the License Enabler File (LEF).

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 **Qlik DataMarket** in the panel to the right.
3. Fill out the mandatory fields.

   The property group **Site license** contains properties related to the license for Qlik DataMarket. All fields are mandatory.

   | Property name | Description |
   |---|---|
   | **Owner name** | The user name of the Qlik DataMarketproduct owner. |
   | **Owner organization** | The name of the organization that the Qlik DataMarket product owner is a member of. |
   | **Serial number** | The serial number assigned to the Qlik DataMarket software. |
   | **Control number** | The control number assigned to the Qlik DataMarket software. |
   | **LEF access** | The LEF file assigned to the Qlik DataMarket 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.

   ***Failed to get LEF from server*** *is displayed if the serial number or control number is incorrect.*

   Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

## 3.2 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.

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.

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.

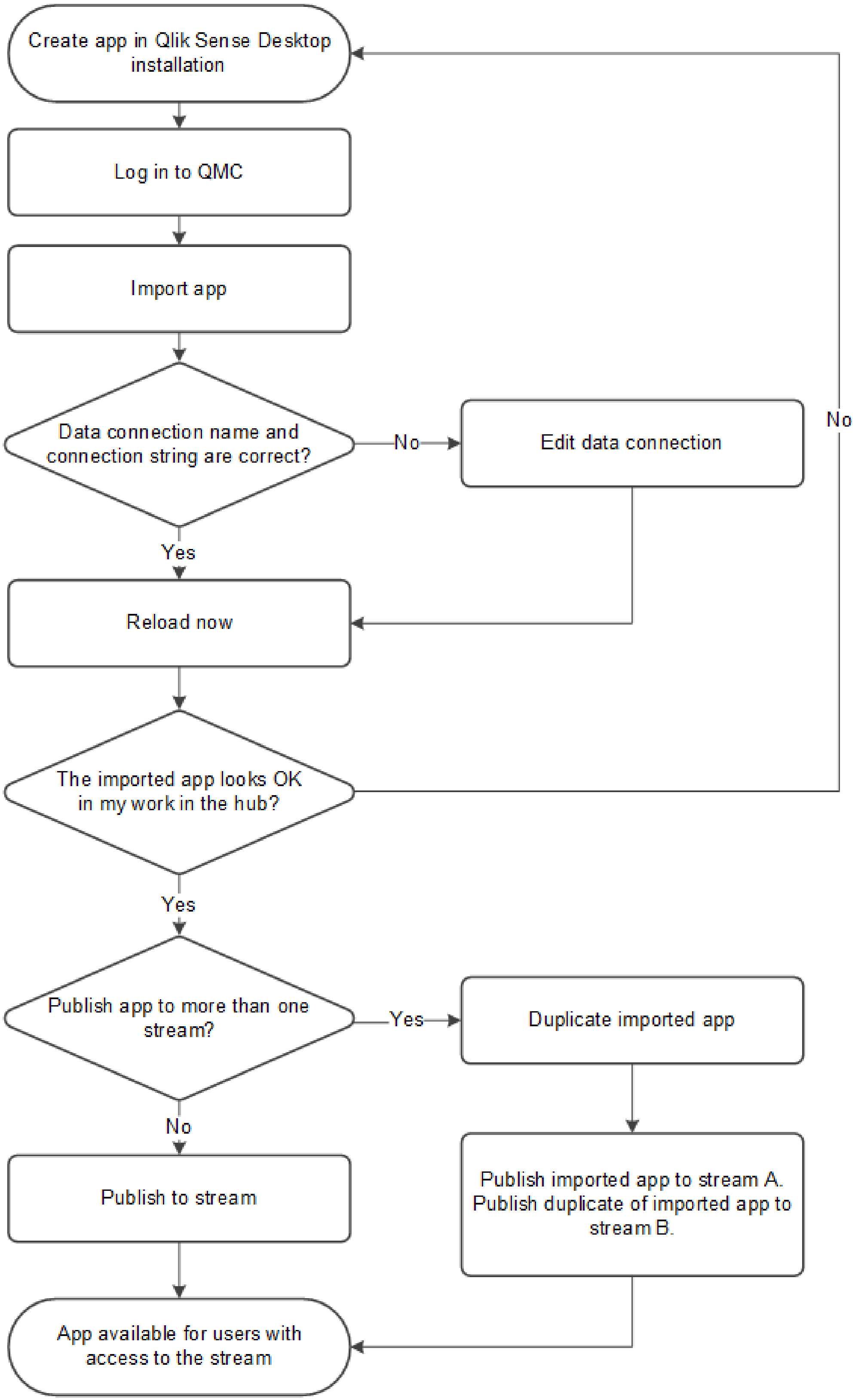
*You can duplicate an app if you have create and read access to the app and read access to the* ***Apps*** *section in the QMC. However, for security reasons, the script will only be duplicated if you also have read rights to the script. Access to the script enables editing or removal of section access, 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.*

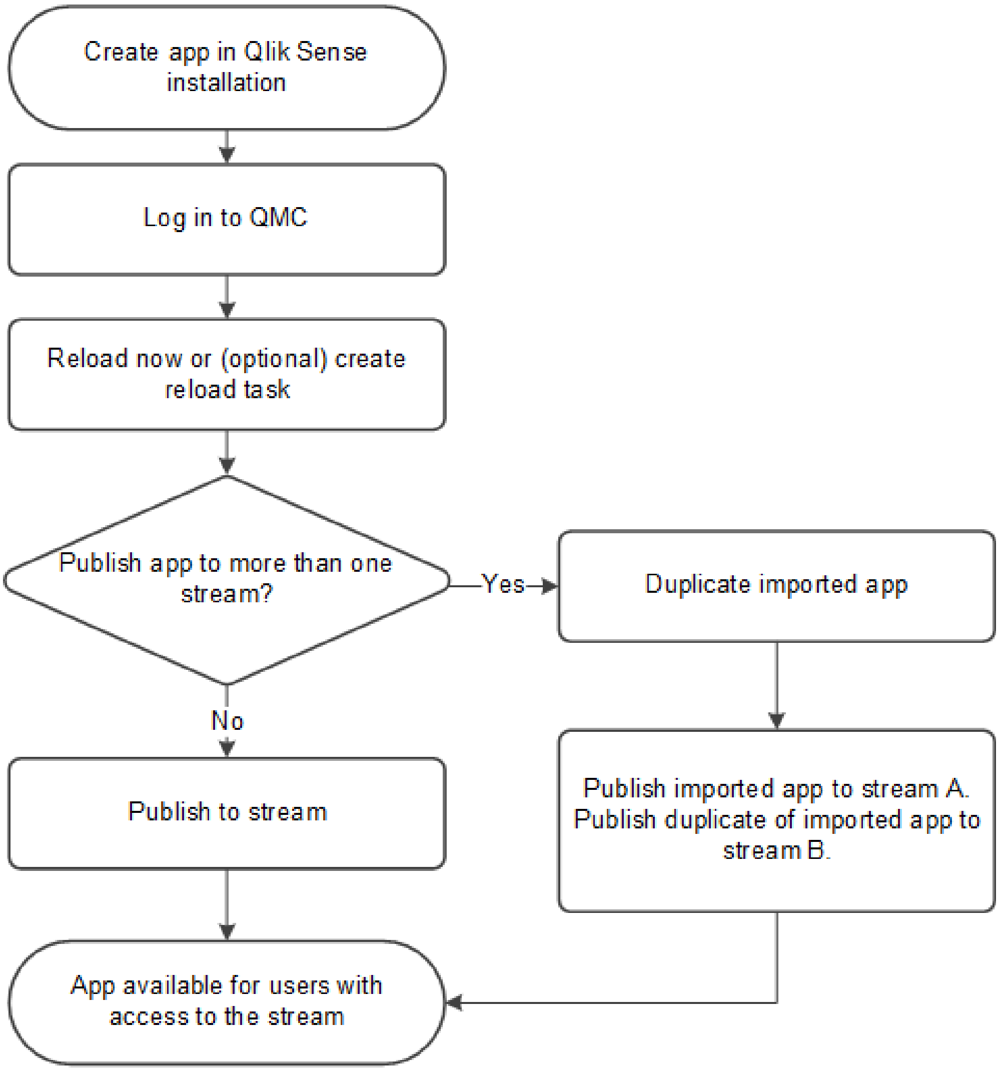
## Workflow: Apps developed on a Qlik Sense Desktop installation

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:


Create app in Qlik Sense Desktop installation
Log in to QMC
Import app
Data connection name and connection string are correct?
No
Edit data connection
Yes
Reload now
The imported app looks OK in my work in the hub?
No
Yes
Publish app to more than one stream?
Yes
Duplicate imported app
No
Publish to stream
Publish imported app to stream A. Publish duplicate of imported app to stream B.
App available for users with access to the stream

## 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:


Create app in Qlik Sense installation
Log in to QMC
Reload now or (optional) create reload task
Publish app to more than one stream?
Yes
Duplicate imported app
No
Publish to stream
Publish imported app to stream A. Publish duplicate of imported app to stream B.
App available for users with access to the stream

## Importing apps

You can import an app if your browser supports HTML5 upload.

Do the following:

1. Select **Apps** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Click ⊕ **Import** in the action bar.
   The **Import app** dialog opens.
3. Select a file to import.
4. 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.*

5. 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.

## Migrating apps

Migrating apps means moving apps from an older version of Qlik Sense to a newer version.

You are most likely to need to migrate an app in the following circumstances:

- When upgrading Qlik Sense.
- When importing an old app.

Apps are migrated automatically, both during an upgrade of Qlik Sense and when importing old apps. If the migration is successful, no manual steps are required. Migrated apps are available in the hub.

You can migrate apps from version 1.0 of Qlik Sense and newer, to more recent versions of Qlik Sense.

## Apps that have not been migrated

When apps have not been migrated, the **Apps** tab on the QMC start page, shows the number of unmigrated apps. The number does not necessarily indicate that a migration has failed, it may also be that there are apps that have not yet been migrated.

With unmigrated apps, the apps overview page has an extra column, **Migration status**.

The following five status values can be displayed when migrating an app:

- Successful
- Ongoing
- Pending
- Migration failed
- Unknown (Displayed when there are apps with the status Pending or Ongoing, and the administrator restarts the Qlik Sense repository service (QRS), before the migration of these apps has been completed.)

Any status, except Successful, will add to the number displayed on the apps tab on the QMC start page. If all apps are successfully migrated, the migrate button and migration status column are not displayed on the apps overview page.

*When upgrading Qlik Sense to a later version, **Migration status** for all apps will be set to Unknown on the first start of the (QRS).*

## Migrating apps manually

If some apps have failed to migrate automatically, you can try migrating them manually.

Do the following:

1. Navigate to the apps overview page.
2. Select the apps with the status **Migration failed** or **Unknown**.
3. In the action bar at the bottom, click **Migrate**.
   The migration is started. If other apps are being migrated, the selected apps will have the status **Pending**.

The apps are migrated.

## Editing apps

You can edit apps that you have update rights to.

Do the following:

1. Select **Apps** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the apps that you want to edit.
   You can also select apps from stream associations.
3. 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.
4. Edit the properties.
   **Identification**

| 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. |

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

| Property | Description |
|---|---|
| **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.
   **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. Select **Apps** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the apps that you want to delete.
3. Click **Delete** in the action bar.A **Delete** dialog is displayed.
4. 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 app in the owner's **Work** folder gets 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.

Do the following:

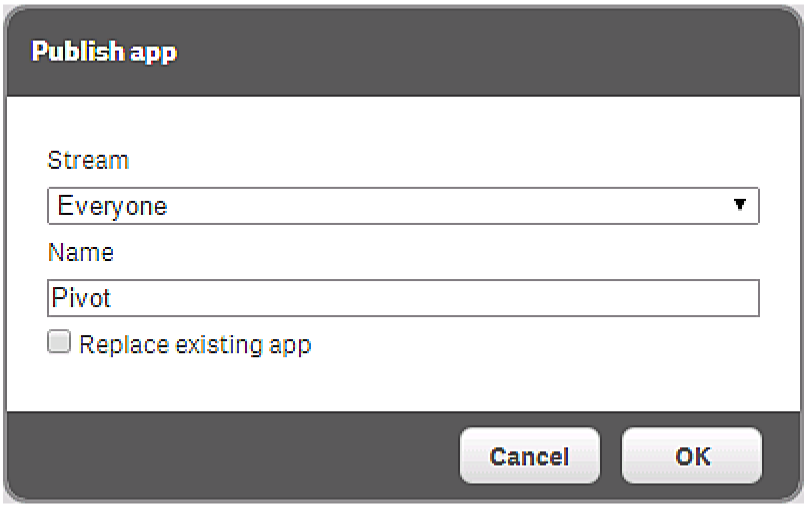
1. Select **Apps** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the apps that you want to publish.
   The number next to **Publish** indicates the number of apps in your selection that you are allowed to publish.
3. Click **Publish** in the action bar.

   > *The **Publish** button is not displayed if you do not have access to any streams.*

   A dialog window opens.
4. 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.
5. Optional: You can replace an already published app. This is only possible if you have selected a single

app.

a. Select **Replace existing app**.



Publish app

Stream

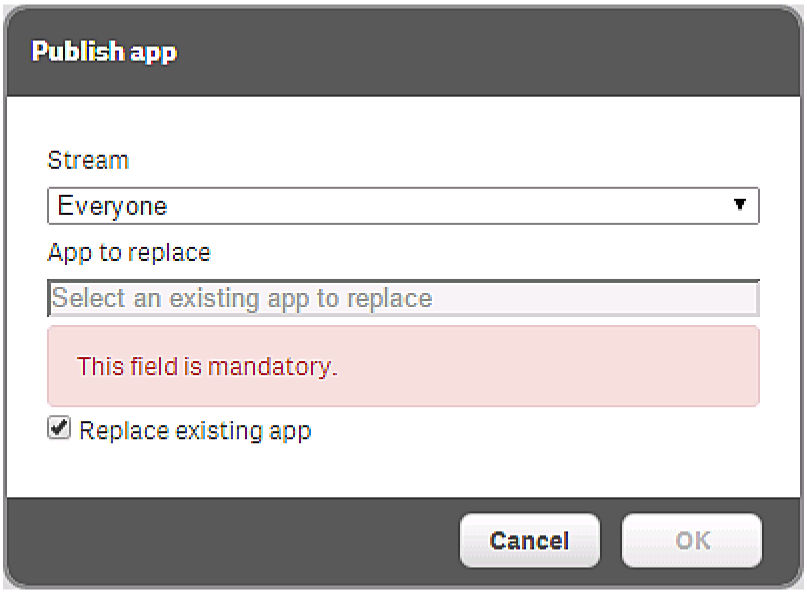
Everyone

Name

Pivot

□ Replace existing app

b. Click the **App to replace** box.



Publish app

Stream

Everyone

App to replace

Select an existing app to replace

This field is mandatory.

☑ Replace existing app

A dialog opens.

c. Double-click the published app you want to replace.
The app is added to the **App to replace** field.

6. 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, create a duplicate of the published app, edit the duplicate and publish 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.

Do the following:

1. Select **Apps** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. 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.

## Replacing apps

You can choose to replace a published app when you publish an app. 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 app in the owner's **Work** folder gets a stream icon to indicate that it has been published.

### 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, 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.*

> *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. Select **Apps** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the app that you want to export.
3. Click **More actions** in the action bar.
   A pop-up menu opens.
4. Click **Export** in the pop-up menu.
   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.

> *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. Select **Apps** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. 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.*

3. 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

Do the following:

1. Select **Apps** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. 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 ⊕ **Create new** in the action bar on the tasks page.

Either way the **Edit reload task** page is displayed.

3. 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.

| 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**

| Property | Description | Default value |
|---|---|---|
| **Enabled** | The task is enabled when selected. | Selected |
| **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 master scheduler and the task is performed by one of the nodes. If the session times out, the master 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)**

| 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.<br>*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.<br>**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.<br>**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.<br>**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.<br>**Example:**<br>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.<br>If you select **Observe daylight saving time**, a trigger set to start at 10:00 will always start at 10.00.<br>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.<br>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:<br>• Start time: **(hh:mm)**<br>• Start date: **(YYYY-MM-DD)** |

| Property | Description |
|---|---|
| **Schedule** | Frequency of the trigger:<br>• **Once**.<br>• **Hourly**. Time period between executions of the trigger. Edit **Repeat after each** by typing the values for:<br>  • **hour(s)** (default is 1)<br>  • **minute(s)** (default is 0)<br>• **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.<br>• **Weekly**. Time period between executions of the trigger:<br>  • Type a value for **Every week(s)** (default is 1).<br>  • 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.<br>• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.<br>*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.* |
| **End** | End time and date:<br>• End time: **(hh:mm)**<br>• End date: **(YYYY-MM-DD)**<br>Select **Infinite** to create a trigger with no end date. |

**Triggers (Task event)**

| Property | Description |
|---|---|
| **Trigger name** | Name of the trigger. Mandatory. |
| **Type** | Trigger type. |
| **Enabled** | Status of the trigger. When selected, the trigger is active. |

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td><b>Time constraint</b></td><td>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.<br>See: <i>Creating a task chain (page 287)</i></td></tr>
<tr><td colspan="2"><b>Tasks</b></td></tr>
<tr><td></td><td>Do the following:<ol><li>Click ⊕ <b>Add task</b> to add a tasks that will function as a trigger condition.<br>A <b>Status</b> list and an empty <b>Task</b> field is added.</li><li>Click the empty field to add a task.<br>A task selection dialog is opened and displays a list of tasks with the following columns: <b>Name</b>, <b>App</b> connected to the task, and <b>Tags</b>, which is the task name.</li><li>Double-click the task to use as a trigger condition.<br>The task is added to the trigger and the dialog is closed.</li><li>In the <b>Status</b> list, select whether the trigger condition is fulfilled on <b>TaskSuccessful</b> or <b>TaskFail</b>.</li></ol><i>A task with trigger condition <b>Task failed</b> is started not only when the preceding task finishes with status Failed, but also with status Aborted, Skipped, or Error (when the error occurs before reload).</i><br>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.</td></tr>
</table>

*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**

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

**Custom properties**

| Property | Description |
|---|---|
| **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. |

4. 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. Select **Apps** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the apps that you want to edit tasks for and click **Edit** in the action bar.
3. Select **Tasks** under **Associated items**.
4. Select the tasks that you want to edit and click **Edit** in the action bar.
   The **Reload task edit** page is displayed.
5. 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.

| 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**

| Property | Description | Default value |
|---|---|---|
| **Enabled** | The task is enabled when selected. | Selected |
| **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 master scheduler and the task is performed by one of the nodes. If the session times out, the master 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)

| 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.<br>*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.<br>**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.<br>**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.<br>**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.<br>**Example:**<br>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.<br>If you select **Observe daylight saving time**, a trigger set to start at 10:00 will always start at 10.00.<br>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.<br>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:<br>• Start time: **(hh:mm)**<br>• Start date: **(YYYY-MM-DD)** |

| Property | Description |
|---|---|
| **Schedule** | Frequency of the trigger:<br>- **Once**.<br>- **Hourly**. Time period between executions of the trigger. Edit **Repeat after each** by typing the values for:<br>  - **hour(s)** (default is 1)<br>  - **minute(s)** (default is 0)<br>- **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.<br>- **Weekly**. Time period between executions of the trigger:<br>  - Type a value for **Every week(s)** (default is 1).<br>  - 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.<br>- **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.<br>*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.* |
| **End** | End time and date:<br>- End time: **(hh:mm)**<br>- End date: **(YYYY-MM-DD)**<br>Select **Infinite** to create a trigger with no end date. |

**Triggers** (Task event)

| Property | Description |
|---|---|
| **Trigger name** | Name of the trigger. Mandatory. |
| **Type** | Trigger type. |
| **Enabled** | Status of the trigger. When selected, the trigger is active. |

| Property | Description |
|---|---|
| **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.<br>See: *Creating a task chain (page 287)* |
| **Tasks** | |
| | Do the following:<br>1. Click ⊕ **Add task** to add a tasks that will function as a trigger condition.<br>A **Status** list and an empty **Task** field is added.<br>2. Click the empty field to add a task.<br>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.<br>3. Double-click the task to use as a trigger condition.<br>The task is added to the trigger and the dialog is closed.<br>4. In the **Status** list, select whether the trigger condition is fulfilled on **TaskSuccessful** or **TaskFail**.<br>*A task with trigger condition **Task failed** is started not only when the preceding task finishes with status Failed, but also with status Aborted, Skipped, or Error (when the error occurs before reload).*<br>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**

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

**Custom properties**

| Property | Description |
|---|---|
| **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 to apply and save your changes.
   **Successfully updated** is displayed at the bottom of the page.

# 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. Select **Tasks** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the user sync task that you want to create a trigger for and click **Edit**.
3. Under **Associated items**, select **Triggers**.
4. Click **Create associated trigger**.
   The **Trigger - Start on schedule** window is opened.
5. Fill in the trigger name and the start time and date.
6. For **Schedule**, select **Monthly**.
7. 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.*

8. 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. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the reload task that you want to create a trigger for and click **Edit**.
3. In the **Triggers** heading bar, click **Actions**.
   A popup is displayed with different trigger options.
4. Select **Create new task event trigger**.
   The **Trigger - Start on task event** window is opened.
5. Fill in the trigger name and the time constraint.
6. Click **Add task**.
7. Click the **Task** field and select the task that the trigger is dependent on.
8. 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**.
9. Click **OK**.
   The new trigger is added to the triggers list.
10. 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. Select **Apps** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the apps that you want to delete tasks from and click **Edit** in the action bar.
3. Select **Tasks** under **Associated items**.
   The **App association items** page with the **Reload tasks** overview is displayed.
4. Select the tasks to delete and click **Delete** in the action bar.
   A **Delete** dialog is displayed.
5. 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. Select **Apps** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the apps that you want to start tasks for and click **Edit** in the action bar.
3. Select **Tasks** under **Associated items**.
   The **App associated items** page is displayed.
4. 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. Select **Apps** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the apps that you want to stop tasks for and click **Edit** in the action bar.
3. Select **Tasks** under **Associated items**.
   The **App associations** page with the **Tasks** overview is displayed.
4. 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. Select **Apps** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. 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.
3. 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**.
4. 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. Select **Content libraries** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Click ⊕ **Create new** in the action bar.
3. Edit the properties.

   > *You can display or hide property groups using the panel to the far right.*

   **Identification**

| 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**

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

**Custom properties**

| Property | Description |
|---|---|
| **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.

4. Click **Apply** in the action bar to create and save the content library.
   The **Create security rule** dialog opens.
5. Edit the security rule for administrative access of the content library:
   a. Edit the **Identification** properties:

| | |
|---|---|
| **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 and examples |
|---|---|
| = | This operator is not case sensitive and returns True if the compared expressions are exactly equal.<br>**Example:**<br>`user.name = ”a*”`<br>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.<br>**Example:**<br>`user.name = ”a*”`<br>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.<br>**Example:**<br>`user.name=resource.name`<br>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. Select **Content libraries** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the library you want to edit.
3. Click **Edit** in the action bar.
4. Edit the properties.
   **Identification**

| 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**

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

**Custom properties**

| Property | Description |
|---|---|
| **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.
   **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. Select **Content libraries** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the content libraries that you want to delete.
3. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
4. 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. The maximum file size is half of the free disk space.

You can choose to upload objects from the content libraries overview page or from the content library **Associated items**.
Do the following:

1. 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:* ⧩

2. 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.
3. Click **Browse**.
   A browse window opens.
4. 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.
5. 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. Select **Content libraries** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the content library that you want to delete objects from and click **Edit**.
   The content library edit page opens.
3. Select **Contents** under **Associated items**.
   The contents overview is displayed.
4. Select the files that you want to delete.
5. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
6. 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. Select **Content libraries** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the content library that you want to create rules for and click **Edit**.
   The content library edit page opens.
3. Select **Security rules** under **Associated items**.
   The security rules overview is displayed.
4. Click ⊕ **Create associated rule** in the action bar.
   The **Create security rule** dialog opens.
5. Edit the security rule for administrative access of the content library:
   a. Edit the **Identification** properties:

| | |
|---|---|
| **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 and examples |
|---|---|
| = | This operator is not case sensitive and returns True if the compared expressions are exactly equal.<br>**Example:**<br>`user.name = ”a*”`<br>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.<br>**Example:**<br>`user.name = ”a*”`<br>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.<br>**Example:**<br>`user.name=resource.name`<br>All resources with the same name as the user are targeted by the rule. |

6. 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. Select **App objects** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the app objects you want to edit.
3. 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.

4. Edit the properties.

> *You can display or hide property groups using the panel to the far right.*

**Identification**

| Property | Description |
|---|---|
| **Name** | The name of the app object. Mandatory. |
| **Owner** | The owner of the app object. |

**Tags**

| 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. |

5. 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. Select **App objects** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the app objects that you want to delete.
3. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
4. Click **OK**.

# 3.3 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 selection and template apps from the Qlik Sense hub, if you have the appropriate access rights. Selection and template apps are published to streams from the Qlik Management Console, which is a part of Qlik Sense. Generated on-demand apps can also be published from the QMC.

To publish an on-demand app that is generated in a Qlik Sense Desktop installation, you must first import it, by using 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.

## 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 | Description |
|---|---|
| **Enable on-demand app service** | Enables and disables the On-demand app service. The service is disabled by default.<br>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. |
| **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.<br>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.<br>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 engine, the load on that Qlik 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.<br>The On-demand app service keeps data about navigation links and about requests to generate and reload on-demand apps.<br>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.<br>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.<br>See: *Anonymous authentication (page 389)*<br>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.<br>⚠ *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".*<br>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.<br>The time is measured from the last data load.<br>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.<br>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.<br>⚠ *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. However, 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. 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.

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.

# 3.4 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. To publish an app to another stream, the app must first be duplicated and then published to the other stream.

> *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.*

## Creating streams

You create a stream to let users read and/or publish apps, sheets, and stories. What privileges a user has is determined by the security rules for each stream.

Do the following:

1. Select **Streams** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Click ⊕ **Create new** in the action bar.
3. Edit the properties.

   **Identification**

   | 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**

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

   **Custom properties**

   | Property | Description |
   |---|---|
   | **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. |

4. Click **Apply** in the action bar to create and save the stream.
   The **Create security rule** dialog opens.
5. Create security rules for the stream and click **Apply**.

*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. 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.
2. Click **Edit** in the action bar.
3. Edit the properties.

   **Identification**

   | 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**

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

   **Custom properties**

   | Property | Description |
   |---|---|
   | **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. |

4. 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. Select **Streams** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the streams that you want to delete.
3. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
4. Click **OK**.

## Creating access rights for streams

You create security rules to give access rights to the streams.

Do the following:

1. Select **Streams** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the stream you want to create rules for and click **Edit**.
   The stream edit page opens.
3. Select **Security rules** under **Associated items**.
   The system rules overview is displayed.
4. Click ⊕ **Create associated rule** in the action bar.
   The **Create security rule** dialog opens.
5. Edit the security rule for administrative access of the stream:
   a. Edit the **Identification** properties:

| | |
|---|---|
| **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 and examples |
|---|---|
| = | This operator is not case sensitive and returns True if the compared expressions are exactly equal.<br>**Example:**<br>`user.name = ”a*”`<br>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.<br>**Example:**<br>`user.name like ”a*”`<br>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.<br>**Example:**<br>`user.name != resource.name`<br>All resources that do not have the same name as the user are targeted by the rule. |

6. Optionally, edit the **Advanced** properties and create the **Conditions** for the rule:
   - Add a condition.
   - Use the **Context** list to specify where the rule applies.
7. 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**.*

# 3.5 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.*

## 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.

## 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. Select **Data connections** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the data connections that you want to edit.

   *If you select several data connections, you cannot view, edit or add security rules.*

3. Click **Edit** in the action bar.
4. Edit the properties.
   You can display or hide property groups using the panel to the far right.

   **Identification**

| 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. |

| Property | Description |
|---|---|
| **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.<br>*The password is saved encrypted.* |

**Tags**

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

**Custom properties**

| Property | Description |
|---|---|
| **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.
   **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. Select **Data connections** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the data connections that you want to delete.
3. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
4. Click **OK**.

## Creating access rights for data connections

You create security rules to give access rights to the data connections. Do the following:

1. Select **Data connections** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the data connection that you want to create rules for and click **Edit**.
   The data connection edit page opens.
3. Select **Security rules** under **Associated items**.
4. Click ⊕ **Create associated rule** in the action bar.
   The **Create security rule** dialog opens.
5. Edit the security rule for administrative access of the data connection:
   a. Edit the **Identification** properties:

| | |
|---|---|
| **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 and examples** |
|---|---|
| = | This operator is not case sensitive and returns True if the compared expressions are exactly equal.<br>**Example:**<br>`user.name = ”a*”`<br>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.<br>**Example:**<br>`user.name like ”a*”`<br>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.<br>**Example:**<br>`user.name != resource.name`<br>All resources that do not have the same name as the user are targeted by the rule. |

6. 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.

*Do not import extensions with the same name as a native object, it is not supported.*

Do the following:

1. Select **Extensions** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Click ⊕ **Import** in the action bar.
3. 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.
4. Click **Open** in the file explorer window.
5. Click **Import**.

*Extensions are saved to \\QlikShare\StaticContent\Extensions. The maximum file size is half of the free disk space. If the import of an extension fails, check the log files at %ProgramData%Qlik/Sense/Log/Repository/System.*

### Extension names

If the name of an extension already exists (or occurs more than once in the zip file), the zip file is not uploaded.

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. Select **Extensions** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the extensions that you want to edit.
3. Click **Edit** in the action bar.
4. Edit the properties.

**Identification**

| 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.<br>*This property is only visible when editing an extension.* |

**Tags**

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

**Custom properties**

| Property | Description |
|---|---|
| **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. You can also edit the fields under **Associated items**.

   **Associated items**

   | 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. |

6. 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. Select **Extensions** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the extensions that you want to delete.
3. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
4. 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. Select **Analytic connections** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Click ⊕ **Create new** in the action bar.
3. Edit the properties.

**Identification**

| Property | Description |
|---|---|
| **Name** | Name of the analytic connection. Must be unique. 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. 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.<br>*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**

| Property | Description |
|---|---|
| **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. |

4. 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. Select **Analytic connections** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the analytic connections that you want to edit and click **Edit** in the action bar.
3. Edit the properties.

| Property | Description |
|---|---|
| **Name** | Name of the analytic connection. Must be unique. 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. 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.<br>*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**

| Property | Description |
|---|---|
| **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. |

4. Click **Apply** in the action bar to save the analytic connection.
5. **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.

# 3.6 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:

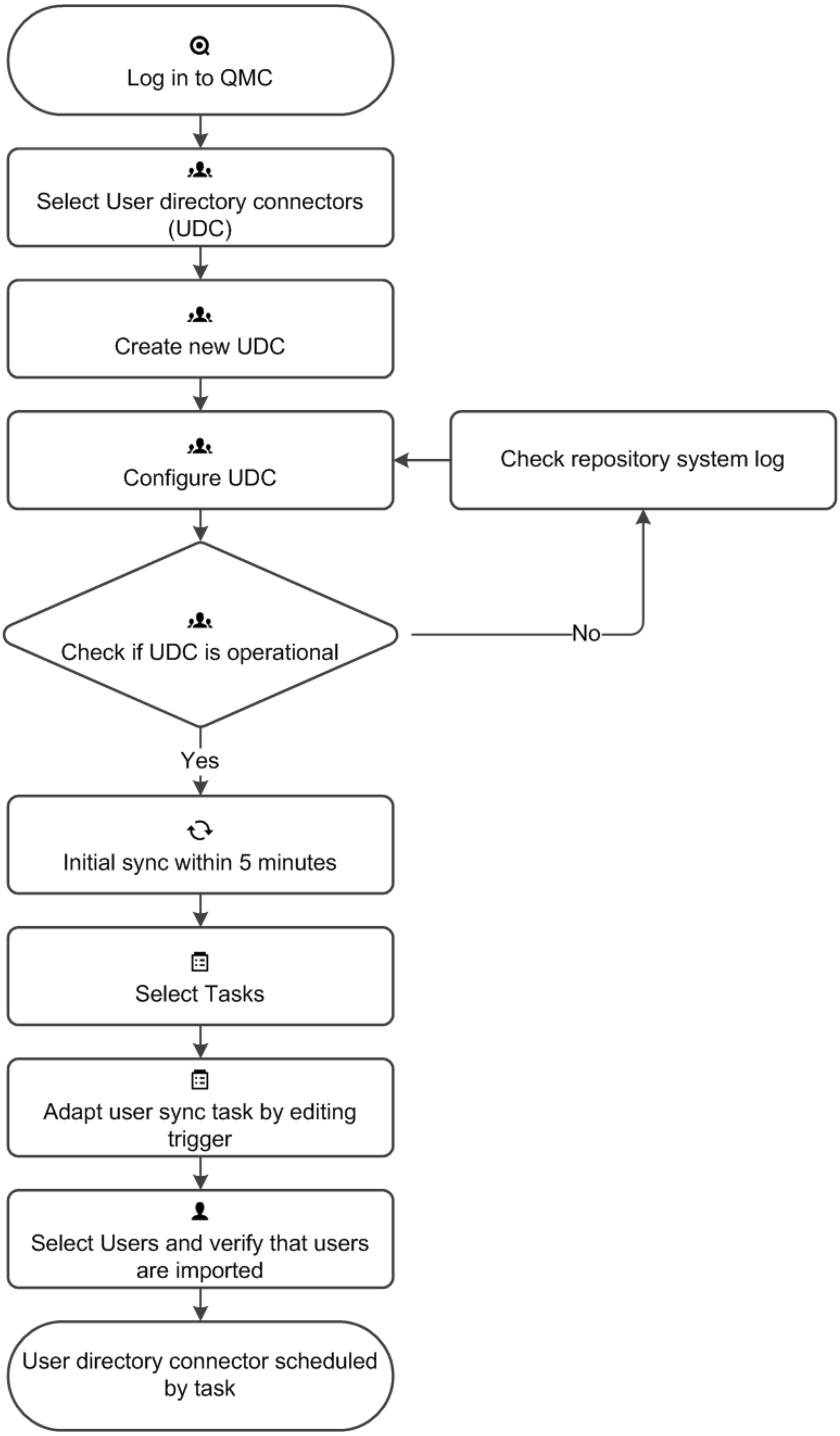
- Creating new user directory connectors
- Synchronizing with user directories
- Managing access types
- Changing ownership of resources
- Removing resources owned by users
- Connecting administrative roles to a user
- Inactivating users
- Deleting users

## 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.


Log in to QMC
Select User directory connectors (UDC)
Create new UDC
Configure UDC
Check repository system log
Check if UDC is operational
No
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

   | | |
   |---|---|
   | 1 | userid,name |
   | 2 | JoD,John Doe |

   Table2

   | | |
   |---|---|
   | 1 | userid,type,value |
   | 2 | JoD,email,jod@gmail.com |

3. 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.

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

   **User sync settings**

| 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.<br>- When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service.<br>ⓘ *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:<br>• A full connection string, for example: *Driver={Microsoft Access Text Driver (*.txt, *.csv)};Extensions=asc,csv,tab,txt;Dbq=%ProgramData%\Qlik\Sense\temp*<br>○ *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.<br>○ *Dbq*: Path to the folder where the csv files are stored.<br>• A pointer to an established System DSN, for example, *dsn=MyDSN;*<br>*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.<br>*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*

4. Click **Apply** to apply your changes.
5. 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).

## 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

   | | |
   |---|---|
   | 1 | ID,userid,name |
   | 2 | 1,JoD,John Doe |

   Table2: SQL attributes

   | | |
   |---|---|
   | 1 | userid,type,value |
   | 2 | JoD,email,jod@gmail.com |

   *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. 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.

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

   **User sync settings**

| 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.<br>• When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service.<br>*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, for example, *UsersTable*.<br>*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, for example, *AttributesTable*.<br>*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:<br>• A full connection string, for example: *Driver={SQL Server Native Client 11.0};Server=localhost;Database=Users;Trusted_Connection=yes;*<br>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.<br>2. *Server* must point to the server that you want to connect to.<br>3. *Database* must point to the database where the tables are.<br>4. *Trusted_Connection=yes* may be required, depending on the setup. In this example it is required.<br>• A pointer to an established System DSN, for example, *dsn=MyDSN;*<br>*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.<br>*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;*

4. Click **Apply** to apply your changes.
5. 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).

## ODBC example (Access)

Each data source has a different configuration and the following is an example (txt) of adding an ODBC user directory connector.

> *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*.

   > *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

   | |
   |---|
   | userid,name |
   | JoD,John Doe |

   Attributes

   | |
   |---|
   | userid,type,value |
   | JoD,email,jod@gmail.com |

3. 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.

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

   **User sync settings**

| 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.<br>• When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service.<br>*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 text file containing the users. Include the file extension in the table name, for example: *File.txt/File.csv*. | - |
| **Attributes table name** | The text file containing the user attributes. Include the file extension in the table name, for example: *File.txt/File.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:<br>• A full connection string, for example: *Driver={Microsoft Access Text Driver (*.txt, *.csv)};Extensions=asc,csv,tab,txt;Dbq=%ProgramData%\Qlik\Sense\temp*<br>*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=%ProgramData%\Qlik\Sense\temp, to be able to use txt and csv files.*<br>◦ *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.<br>◦ *DBQ*: Path to the folder where the txt files are stored.<br>• A pointer to an established System DSN, for example, *dsn=MyDSN;*<br>*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.<br>*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**: *Users.txt*
**Attributes table name**: *Attributes.txt*
**Visible connections string**: *Driver={Microsoft Access Text Driver (*.txt, *.csv)};Extensions=asc,csv,tab,txt;DBQ=%ProgramData%\Qlik\Sense\temp*

4. Click **Apply** to apply your changes.
5. 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) users. For large user directories, we recommend that you always select **Sync user data for existing users** in the **User sync settings** property group.*

Do the following:

1. Select **User directory connectors** on the QMC start page or from the **Start▼** drop-down menu to display the overview.

2. Click ⊕ **Create new** in the action bar.
   The dialog with available user directory connector types is displayed.
3. Select the type for the new user directory connector and also the source. The following types are available:
   - Generic LDAP
   - Active Directory
   - ApacheDS
   - ODBC
   - Access (through ODBC)
   - Excel (through ODBC)
   - SQL (through ODBC)
   - Teradata (through 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. You can use professional access rules or analyzer access rules (user-based license) or user access rules or login access rules (token-based license) to allocate access. Alternatively, a local user can first log on to be recognized as a user, and then be allocated tokens.*

4. Edit the properties.

   **Identification**

   All fields are mandatory and must not be empty.

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

**User sync settings**

| 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.<br>• 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**, or **Generic LDAP** if you only want to synchronize a selection of users.<br>*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, Active Directory, and ApacheDS)

| Property | Description | Default value |
|---|---|---|
| **User directory name**<br>*Not entered manually for Active Directory.* | 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. | |

| Property | Description | Default value |
|---|---|---|
| **Path** | The URI used to connect to the directory server. To support SSL, specify the protocol as LDAPS instead. (Currently LDAPS is only supported for AD). | 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**.*

| 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*.<br>*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*.<br>*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:<br>- A full connection string, for example: *Driver={SQL Server Native Client 11.0};Server=localhost;Database=Users;Trusted_Connection=yes;*<br>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.<br>2. *Server* must point to the server that you want to connect to.<br>3. *Database* must point to the database where the tables are.<br>4. *Trusted_Connection=yes* may be required, depending on the setup. In this example it is required.<br>- A pointer to an established System DSN, for example, *dsn=MyDSN;*<br>*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.<br>**Example:**<br>Assume that you have a connection string as follows:<br>*Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;Uid=Admin;Pwd=verySecretAdminPassword;*<br>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:<br>Save the first part:<br>*Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;*<br>in the **Visible connection string** field, and the second part:<br>*Uid=Admin;Pwd=verySecretAdminPassword;*<br>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.<br>*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.

| 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.<br>*If the user synchronization is unsuccessful, try setting the value to '0' (zero).* | 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.<br>*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.*<br>This property is only visible for Generic LDAP and Active directory search, (Active Directory always uses optimization). | Not selected |

*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)

*The directory entry attributes are case-sensitive.*

| 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.<br>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.<br>See also the **Group membership** setting, above. | member |

**Directory entry attributes** (ApacheDS)

*The directory entry attributes are case-sensitive.*

| 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 |

| Property | Description | Default value |
|---|---|---|
| **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.<br>See also the **Group membership** setting, above. | member |

**Tags**

| Property | Description |
|---|---|
| **Tags** | *If no tags are available, this property group is empty.*<br>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 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. Select **User directory connectors** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the user directory connector that you want to edit and click **Edit** in the action bar.
   The edit page opens.
3. Edit the properties.

   **Identification**

   All fields are mandatory and must not be empty.

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

   **User sync settings**

   | 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.<br>• 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**, or **Generic LDAP** if you only want to synchronize a selection of users.<br>*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, Active Directory, and ApacheDS)

| Property | Description | Default value |
|---|---|---|
| **User directory name**<br>*Not entered manually for Active Directory.* | 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. | |
| **Path** | The URI used to connect to the directory server. To support SSL, specify the protocol as LDAPS instead. (Currently LDAPS is only supported for AD). | 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**.*

| 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. Include the file extension in the table name, for example: *Table.csv*.<br>*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*.<br>*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:<br>- A full connection string, for example: *Driver={SQL Server Native Client 11.0};Server=localhost;Database=Users;Trusted_Connection=yes;*<br>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.<br>2. *Server* must point to the server that you want to connect to.<br>3. *Database* must point to the database where the tables are.<br>4. *Trusted_Connection=yes* may be required, depending on the setup. In this example it is required.<br>- A pointer to an established System DSN, for example, *dsn=MyDSN;*<br>*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.<br>**Example:**<br>Assume that you have a connection string as follows:<br>*Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;Uid=Admin;Pwd=verySecretAdminPassword;*<br>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:<br>Save the first part:<br>*Driver={Microsoft Access Driver (.mdb)};Dbq=C:\mydatabase.mdb;*<br>in the **Visible connection string** field, and the second part:<br>*Uid=Admin;Pwd=verySecretAdminPassword;*<br>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.<br>*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.

| 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.<br>*If the user synchronization is unsuccessful, try setting the value to '0' (zero).* | 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.<br>*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.*<br>This property is only visible for Generic LDAP and Active directory search, (Active Directory always uses optimization). | Not selected |

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).

**Directory entry attributes** (Generic LDAP)

*The directory entry attributes are case-sensitive.*

| 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.<br>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.<br>See also the **Group membership** setting, above. | member |

**Directory entry attributes** (ApacheDS)

*The directory entry attributes are case-sensitive.*

| 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 |

| Property | Description | Default value |
|---|---|---|
| **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.<br>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.<br>See also the **Group membership** setting, above. | member |

**Tags**

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

Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

4. 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. Select **User directory connectors** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
3. 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:

- only the user directory connector
- the user directory connector and all the users that are imported from the user directory

Do the following:

1. Select **User directory connectors** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

   *You cannot delete more than one user directory connector at a time.*

2. Select the user directory connector that you want to delete.
3. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
4. 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).
5. Click **OK**.

## Synchronizing with user directories

You can synchronize the user data from the user directories.

Do the following:

1. Select **User directory connectors** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. 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.*

3. 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**, or **Generic 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.*

4. Go back to the overview by clicking on **User directory connectors** in the top left corner.
5. Select the user directory that you want to synchronize.
6. 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**
7. When **Idle** is displayed, verify that **Last successfully finished sync** date and time is updated.

> *If the status is displayed as **Idle** and **Last started sync** is more recent than **Last successfully finished sync**, the synchronization has failed.*

> *If the user synchronization is unsuccessful, set the property **Page size of search** to no value (empty). This can solve the problem.*

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. Select **License management** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select **Professional access allocations** in the panel to the right.
3. Click ⊕ **Allocate** in the action bar.
   The **Users** dialog opens.
4. Select users in the list and click **Allocate**.

   > ⓘ ***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. Select **License management** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select **Professional access allocations** in the panel to the right.
3. Select the users whose access you want to deallocate and click **Deallocate** in the action bar.
   A confirmation dialog is displayed..
4. 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.

Select **License management** on the QMC start page or from the **Start▼** drop-down menu to display the overview.

2. Select **Professional access allocations** in the panel to the right.
3. 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. Select **License management** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select **Professional access rules** in the panel to the right.
3. Click ⊕ **Create new** in the action bar.
4. Edit the properties.

**Identification**

| **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**

| **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** |
|---|---|
| = | This operator is not case sensitive and returns True if the compared expressions are exactly equal.<br>**Example:**<br>`user.name = ”a*”`<br>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.<br>**Example:**<br>`user.name like ”a*”`<br>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.<br>**Example:**<br>`user.name != resource.name`<br>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**

| | |
|---|---|
| **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**

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

5. 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. Select **License management** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.

2. Select **Professional access rules** in the panel to the right.
3. Select the rule you want to edit.
4. Click **Edit** in the action bar.
5. Edit the properties.

**Identification**

| 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**

| 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 |
|---|---|
| = | This operator is not case sensitive and returns True if the compared expressions are exactly equal.<br>**Example:**<br>`user.name = ”a*”`<br>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.<br>**Example:**<br>`user.name like ”a*”`<br>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.<br>**Example:**<br>`user.name != resource.name`<br>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**

| 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**

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

**Users**

| Property name | Description |
|---|---|
| **Name** | Name of the user. |
| **Permitted action** | Action that the user is allowed to perform. |

6. 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 user access

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 access allocations** in the panel to the right.
3. Click ⊕ **Allocate** in the action bar.
   The **Users** dialog opens.
4. 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. Select **License management** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select **Analyzer access allocations** in the panel to the right.
3. Select the users whose access you want to deallocate and click **Deallocate** in the action bar.
   A confirmation dialog is displayed..
4. 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. Select **License management** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select **Analyzer access allocations** in the panel to the right.
3. 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. Select **License management** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select **Analyzer access rules** in the panel to the right.

3. Click ⊕ **Create new** in the action bar.
4. Edit the properties.

**Identification**

| 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**

| 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 |
|---|---|
| = | This operator is not case sensitive and returns True if the compared expressions are exactly equal.<br>**Example:**<br>`user.name = ”a*”`<br>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.<br>**Example:**<br>`user.name like ”a*”`<br>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.<br>**Example:**<br>`user.name != resource.name`<br>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**

| | |
|---|---|
| **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**

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

5. 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. Select **License management** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select **Analyzer access rules** in the panel to the right.
3. Select the rule you want to edit.
4. Click **Edit** in the action bar.
5. Edit the properties.

**Identification**

| 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**

| 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 |
|---|---|
| = | This operator is not case sensitive and returns True if the compared expressions are exactly equal.<br>**Example:**<br>`user.name = ”a*”`<br>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.<br>**Example:**<br>`user.name like ”a*”`<br>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.<br>**Example:**<br>`user.name != resource.name`<br>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**

| 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**

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

**Users**

| Property name | Description |
|---|---|
| **Name** | Name of the user. |
| **Permitted action** | Action that the user is allowed to perform. |

6. Click **Apply** to save the updates.
   **Successfully added** is displayed at the bottom of the page.

## 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. Select **License management** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select **User access allocations** in the panel to the right.
3. Click ⊕ **Allocate** in the action bar.
   The **Users** dialog opens.
4. 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.
2. Select **User access allocations** in the panel to the right.
3. Select the users whose access you want to deallocate and click **Deallocate** in the action bar.
   A confirmation dialog is displayed..
4. 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.
2. Select **User access allocations** in the panel to the right.
3. 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 a user access rule

A user access rule defines which users that have access to the available tokens.

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 **User access rules** in the panel to the right.
3. Click ⊕ **Create new** in the action bar.
4. Edit the properties.

**Identification**

| 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**

| 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 |
|---|---|

| | |
|---|---|
| = | This operator is not case sensitive and returns True if the compared expressions are exactly equal.<br>**Example:**<br>`user.name = ”a*”`<br>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.<br>**Example:**<br>`user.name like ”a*”`<br>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.<br>**Example:**<br>`user.name != resource.name`<br>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**

| | |
|---|---|
| **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**

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

5. 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. Select **License management** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select **User access rules** in the panel to the right.
3. Select the rule you want to edit.
4. Click **Edit** in the action bar.
5. Edit the properties.

**Identification**

| **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**

| **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** |
|---|---|
| = | This operator is not case sensitive and returns True if the compared expressions are exactly equal.<br>**Example:**<br>`user.name = ”a*”`<br>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.<br>**Example:**<br>`user.name like ”a*”`<br>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.<br>**Example:**<br>`user.name != resource.name`<br>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**

| 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**

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

**Users**

| Property name | Description |
|---|---|
| **Name** | The name of the user. |
| **Permitted action** | The action that the user is allowed to perform. |

6. 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. Select **License management** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select **User access rules** in the panel to the right.
3. Select the rules that you want to delete.
4. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
5. 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. Select **License management** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select **Login access rules** in the panel to the right.
3. Click ⊕ **Create new** in the action bar.
4. Edit the properties.

   **Identification**

| Property name | Description |
|---|---|
| **Name** | The name of the login access (group). |

**Tokens**

| Property name | Description |
|---|---|
| **Allocated tokens** | The number of allocated tokens that the login access group can use. |

5. 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 266)*.

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. Select **License management** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select **Login access rules** in the panel to the right.
3. Select the login access rule you want to edit and click **Edit** in the action bar.
4. Edit the properties.

   **Identification**

   | Property name | Description |
   |---|---|
   | **Name** | The name of the login access (group). |

   You can change the name for the login access:

   **Tokens**

   | Property name | Description |
   |---|---|
   | **Allocated tokens** | The number of allocated 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.
5. 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**

See: *Editing a license rule (page 267)*

6. Click **Apply**.
7. 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. Select **License management** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select **Login access rules** in the panel to the right to display the overview.
3. Select the login access rules that you want to delete.
4. Click **Delete** in the action bar.A **Delete** dialog is displayed.
5. 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.

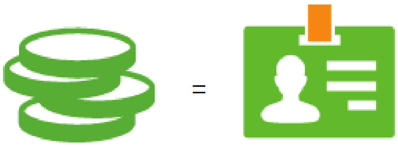
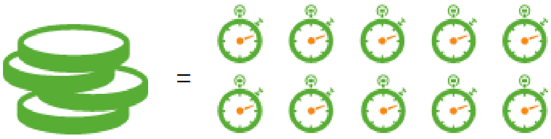
## Login access: Token consumption example

Qlik Sense licensing is based on a token model. You buy tokens and can allocate and reallocate these 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.

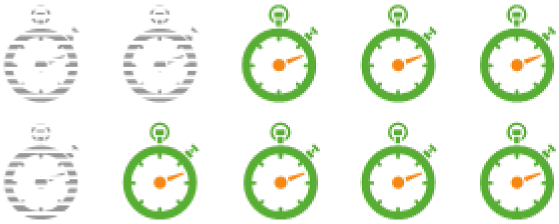
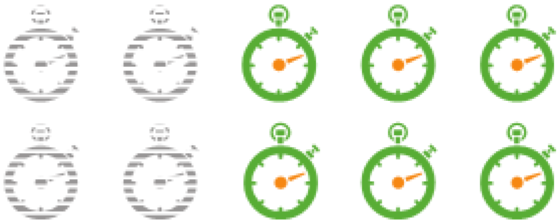
| Token allocation | Access pass description |
|---|---|
| 1 token = 1 user access pass | Assigned to a unique and identified named user with unlimited use of Qlik |

| | |
|---|---|
|  | Sense as authorized by your organization's security policies and rules. |
| 1 token = 10 login access passes<br> | 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.

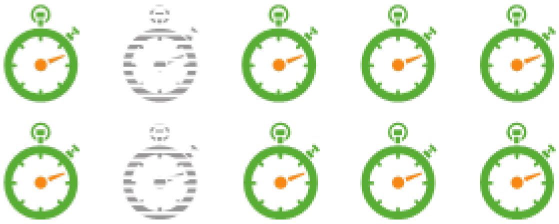
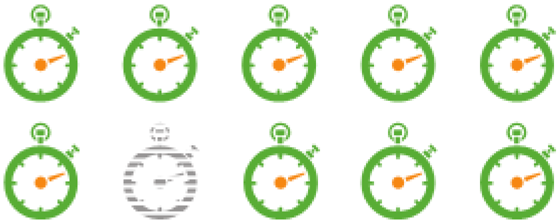
| Day # | Login access pass consumption | Description |
|---|---|---|
| Day 0 | | Let's assume that you allocate one token to a group. This gives the group 10 available login access passes. |
| Day 1 | | A user assigned to that group logs into Qlik Sense, which immediately consumes one login access pass. |
| 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:<br>- The user logs out.<br>- The user closes the browser (not just the |

| | | |
|---|---|---|
| | | tab).<br>• 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.

| 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. Select **License management** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select **Login access rules** in the panel to the right.
3. Select a login access rule and click **Edit**.
   To create a new login access rule, see: *Creating login access rules (page 260)*.
4. Under **Associated items**, select **License rules**.
5. Click **Create associated rule**.
6. Edit the license rule as needed:
   a. **Identification**

| | |
|---|---|
| **Disabled** | Select to disable the rule. The rule is enabled by default. |
| **Name** | The name of the login access rule. Mandatory. |
| **Description** | Enter a description of the rule. |

   b. **Basic**

| | |
|---|---|
| **Resource filter** | If you change the resource filter, the rule may not work as intended. |

*The option **Allow access** is automatically selected.*

| **Operator** | **Descriptions and examples** |
|---|---|
| = | This operator is not case sensitive and returns True if the compared expressions are exactly equal.<br>**Example:**<br>`user.name = ”a*”`<br>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.<br>**Example:**<br>`user.name like ”a*”`<br>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.<br>**Example:**<br>`user.name != resource.name`<br>All resources that do not have the same name as the user are targeted by the rule. |

c. **Advanced**

| | |
|---|---|
| **Conditions** | 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.
   **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. Select **License management** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select **Login access rules** in the panel to the right.
3. Select a login access rule and click **Edit**.
4. Under **Associated items**, select **License rules**.
5. Select a license rule and click **Edit**.
   Edit the license rule as needed:

a. **Identification**

| | |
|---|---|
| **Disabled** | Select to disable the rule. The rule is enabled by default. |
| **Name** | The name of the login access rule. Mandatory. |
| **Description** | Enter a description of the rule. |

b. **Basic**

| | |
|---|---|
| **Resource filter** | If you change the resource filter, the rule may not work as intended. |

ⓘ *The option **Allow access** is automatically selected.*

| Operator | Descriptions and examples |
|---|---|
| = | This operator is not case sensitive and returns True if the compared expressions are exactly equal.<br>**Example:**<br>`user.name = ”a*”`<br>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.<br>**Example:**<br>`user.name like ”a*”`<br>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.<br>**Example:**<br>`user.name != resource.name`<br>All resources that do not have the same name as the user are targeted by the rule. |

c. **Advanced**

| | |
|---|---|
| **Conditions** | Define the resource, user, or combined conditions that the rule should apply to. |

6. Optionally, edit the **Advanced** properties and create the **Conditions** for the rule.

7. 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. Select **User directory connectors** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the user directory connector that you want to start tasks for and click **Edit** in the action bar.

   > *The panel to the far left lists your selections.*

3. Select **Tasks** under **Associated items**.
   The **User synchronization tasks** overview is displayed.
4. 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. Select **User directory connectors** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the user directory connector that you want to edit tasks for and click **Edit** in the action bar.
3. 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.
4. Edit the properties.

   **Identification**

   All fields are mandatory and must not be empty.

| 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**

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

5. 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. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the task you want to add a trigger on and click **Edit** in the action bar at the bottom of the page.
3. Select **Triggers** under **Associated items**.
   The **Triggers** overview is displayed.
4. Click ⊕ **Create associated trigger** in the action bar.
   The **Trigger - Start on schedule** dialog is displayed.
5. Edit the fields in the dialog to set the trigger conditions.

| 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.<br>*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.<br>**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.<br>**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.<br>**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.<br>**Example:**<br>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.<br>If you select **Observe daylight saving time**, a trigger set to start at 10:00 will always start at 10.00.<br>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.<br>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:<br>• Start time: **(hh:mm)**<br>• Start date: **(YYYY-MM-DD)** |

| Property | Description |
|---|---|
| **Schedule** | Frequency of the trigger:<br>- **Once**.<br>- **Hourly**. Time period between executions of the trigger. Edit **Repeat after each** by typing the values for:<br>  - **hour(s)** (default is 1)<br>  - **minute(s)** (default is 0)<br>- **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.<br>- **Weekly**. Time period between executions of the trigger:<br>  - Type a value for **Every week(s)** (default is 1).<br>  - 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.<br>- **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.<br>*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.* |
| **End** | End time and date:<br>- End time: **(hh:mm)**<br>- End date: **(YYYY-MM-DD)**<br>Select **Infinite** to create a trigger with no end date. |

6. 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. Select **Tasks** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the task you want to edit a trigger on and click **Edit** in the action bar at the bottom of the page.
3. Select **Triggers** at **Associated items**.

The **Triggers** overview is displayed.

4. 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.
5. Edit the fields in the dialog to change the trigger conditions.

| 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.<br>*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.<br>**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.<br>**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.<br>**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.<br>**Example:**<br>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.<br>If you select **Observe daylight saving time**, a trigger set to start at 10:00 will always start at 10.00.<br>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.<br>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:<br>• Start time: **(hh:mm)**<br>• Start date: **(YYYY-MM-DD)** |
| **Schedule** | Frequency of the trigger:<br>• **Once**.<br>• **Hourly**. Time period between executions of the trigger. Edit **Repeat after each** by typing the values for:<br>  • **hour(s)** (default is 1)<br>  • **minute(s)** (default is 0)<br>• **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.<br>• **Weekly**. Time period between executions of the trigger:<br>  • Type a value for **Every week(s)** (default is 1).<br>  • 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.<br>• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.<br>*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.* |
| **End** | End time and date:<br>• End time: **(hh:mm)**<br>• End date: **(YYYY-MM-DD)**<br>Select **Infinite** to create a trigger with no end date. |

6. 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. Select **User directory connectors** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the user directory connector that you want to start a task for and click **Edit** in the action bar.
3. Select **Tasks** under **Associated items**.
   The **User synchronization tasks** overview is displayed.
4. 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 only the user sync task.

See: *Deleting user directory connectors and users (page 244)*

## Editing users

You can edit users that you have update rights to.

Do the following:

1. 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:*

2. Select the users that you want to edit.
3. Click **Edit** in the action bar.
4. Edit the properties.

   **Identification**

| **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.<br>*You can add new, non-existent admin roles, but they will not be valid until they have been properly defined.* |

**Tags**

| Property | Description |
|---|---|
| **Tags** | *If no tags are available, this property group is empty.*<br>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.

| 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. |

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.

## 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. Select **Users** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the users that you want to inactivate.
3. Click **Edit** in the action bar.
   The **User edit** page opens.
4. Select **Blocked**.
5. 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, such as custom properties, regarding the user 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. Select **Users** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the users that you want to delete.

   *You can filter a column by using the filtering option:* ⏷

3. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
4. 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 if needed, or assigned other admin roles with other 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. Select **Users** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the users that you want to disconnect or change admin roles for.
3. Click **Edit** in the action bar.
   The **User edit** page opens.
4. Select **Identification** under **Properties**.
5. 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.*

6. Click **Apply** in the action bar to apply and save your changes.

## 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. 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:* ⏷

2. Select the user whose items you want to view.
3. Click **Edit** in the action bar.
   The **User edit** page opens.
4. 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. 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:* ⏷

2. Select the user whose items you want to edit.
3. Click **Edit** in the action bar.
   The **User edit** page opens.
4. Click the **Owned items** under **Associated items**.
   The **User associated items** overview opens.
5. Select the item that you want to edit.
6. Click **Edit** in the action bar.
   The edit page for the selected item type opens.
7. Edit the properties.
8. 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. Select **Users** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the user whose items you want to view.
3. Click **Delete** in the action bar.
   The **User edit** page opens.
4. Click the **Owned items** under **Associated items**.
   The **User associated items** overview opens.
5. Select the items that you want to delete.
6. 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.
7. 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 following sections.

### 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.

See: *Default administration roles (page 384)*

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.

See: *Security rules example: Creating custom admin roles (page 479)*

### 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.

See: *Security rules example: Applying Qlik Sense access rights for user types (page 484)*

# 3.7 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 two types of tasks:

- Reload
- User synchronization

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.

## 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

1. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Click ⊕ **Create new** in the action bar.
   The **Reload task edit** page is displayed.
3. 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.

| 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**

| Property | Description | Default value |
|---|---|---|
| **Enabled** | The task is enabled when selected. | Selected |
| **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 master scheduler and the task is performed by one of the nodes. If the session times out, the master 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)**

| 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.<br>*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.<br>**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.<br>**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.<br>**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.<br>**Example:**<br>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.<br>If you select **Observe daylight saving time**, a trigger set to start at 10:00 will always start at 10.00.<br>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.<br>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:<br>• Start time: **(hh:mm)**<br>• Start date: **(YYYY-MM-DD)** |

| Property | Description |
|---|---|
| **Schedule** | Frequency of the trigger:<br>• **Once**.<br>• **Hourly**. Time period between executions of the trigger. Edit **Repeat after each** by typing the values for:<br>  ◦ **hour(s)** (default is 1)<br>  ◦ **minute(s)** (default is 0)<br>• **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.<br>• **Weekly**. Time period between executions of the trigger:<br>  ◦ Type a value for **Every week(s)** (default is 1).<br>  ◦ 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.<br>• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.<br>*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.* |
| **End** | End time and date:<br>• End time: **(hh:mm)**<br>• End date: **(YYYY-MM-DD)**<br>Select **Infinite** to create a trigger with no end date. |

**Triggers (Task event)**

| Property | Description |
|---|---|
| **Trigger name** | Name of the trigger. Mandatory. |
| **Type** | Trigger type. |
| **Enabled** | Status of the trigger. When selected, the trigger is active. |

| Property | Description |
|---|---|
| **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.<br>See: *Creating a task chain (page 287)* |
| **Tasks** | |
| | Do the following:<br>1. Click ⊕ **Add task** to add a tasks that will function as a trigger condition.<br>A **Status** list and an empty **Task** field is added.<br>2. Click the empty field to add a task.<br>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.<br>3. Double-click the task to use as a trigger condition.<br>The task is added to the trigger and the dialog is closed.<br>4. In the **Status** list, select whether the trigger condition is fulfilled on **TaskSuccessful** or **TaskFail**.<br>*A task with trigger condition **Task failed** is started not only when the preceding task finishes with status Failed, but also with status Aborted, Skipped, or Error (when the error occurs before reload).*<br>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**

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

**Custom properties**

| Property | Description |
|---|---|
| **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.

4. **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:

- 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. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
   b. Click ⊕ **Create new** in the action bar.
   The **Reload task edit** page is displayed.
   c. Type *Task 1* in the **Name** field.
   d. 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.
   e. Leave the **Execution** properties as is.
   f. 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.
   g. 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**.
      The trigger is added to the **Triggers** table.
   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**.
    - b. Create the task.
    - c. 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.

> ⓘ *A task can trigger itself in a circular task chain.*

Do the following:

1. 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:* ⏷

2. 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
     ⟳ Triggered
     ⟳ Started
     ⌛ Queued
     ⟳ Abort initiated
     ⟳ Aborting
     ☒ Aborted
     ✓ Success
     ✗ Failed
     ••• Skipped
     ⟳ Retrying
     ✗ Error
     ••• Reset
   - 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. Select **Tasks** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the task that you want to edit.
3. Click **Edit** in the action bar at the bottom of the page.
4. 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.*

   **Reload task properties**

   **Identification**

   All fields are mandatory and must not be empty.

| 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**

| Property | Description | Default value |
|---|---|---|
| **Enabled** | The task is enabled when selected. | Selected |

| 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 master scheduler and the task is performed by one of the nodes. If the session times out, the master 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)

| 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.<br>*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.<br>**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.<br>**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.<br>**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.<br>**Example:**<br>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.<br>If you select **Observe daylight saving time**, a trigger set to start at 10:00 will always start at 10.00.<br>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.<br>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:<br>• Start time: **(hh:mm)**<br>• Start date: **(YYYY-MM-DD)** |

| Property | Description |
|---|---|
| **Schedule** | Frequency of the trigger:<br>• **Once**.<br>• **Hourly**. Time period between executions of the trigger. Edit **Repeat after each** by typing the values for:<br>  • **hour(s)** (default is 1)<br>  • **minute(s)** (default is 0)<br>• **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.<br>• **Weekly**. Time period between executions of the trigger:<br>  • Type a value for **Every week(s)** (default is 1).<br>  • 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.<br>• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.<br>*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.* |
| **End** | End time and date:<br>• End time: **(hh:mm)**<br>• End date: **(YYYY-MM-DD)**<br>Select **Infinite** to create a trigger with no end date. |

**Triggers** (Task event)

| Property | Description |
|---|---|
| **Trigger name** | Name of the trigger. Mandatory. |
| **Type** | Trigger type. |
| **Enabled** | Status of the trigger. When selected, the trigger is active. |

| Property | Description |
|---|---|
| **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.<br>See: *Creating a task chain (page 287)* |
| **Tasks** | |
| | Do the following:<br>1. Click ⊕ **Add task** to add a tasks that will function as a trigger condition.<br>A **Status** list and an empty **Task** field is added.<br>2. Click the empty field to add a task.<br>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.<br>3. Double-click the task to use as a trigger condition.<br>The task is added to the trigger and the dialog is closed.<br>4. In the **Status** list, select whether the trigger condition is fulfilled on **TaskSuccessful** or **TaskFail**.<br>*A task with trigger condition **Task failed** is started not only when the preceding task finishes with status Failed, but also with status Aborted, Skipped, or Error (when the error occurs before reload).*<br>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**

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

Custom properties

| Property | Description |
|---|---|
| **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.

| 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 |

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

| Property | Description |
|---|---|
| **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 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. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the tasks that you want to delete.

   *You can filter a column by using the filtering option:* ⏷

3. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
4. 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. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the tasks that you want to enable.
3. 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.
4. 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. Select **Tasks** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the tasks that you want to enable.
3. 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.
4. 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. 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:* ⏷

2. 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.
3. 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. 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:* ▼

2. Select the tasks that you want to stop. The number displayed next to **Stop**, indicates the number of items to stop.
3. 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.

# 3.8 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. 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 299)* 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.*

2. Click ℹ on a service to get detailed information on the status, for example the time stamp.
   The **Service status** window opens.
3. 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 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. |
| (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 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 white 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.
   See: *Configuring the node (page 300)*

   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. Select **Repositories** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the repositories that you want to edit.
3. 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.

4. Edit the properties.

   **Identification**

   All fields are mandatory and must not be empty.

| 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.

| Property | Description | Default value |
|---|---|---|
| **Audit activity log level** | Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Basic**: a limited set of entries | Basic |
| **Audit security log level** | Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Basic**: a limited set of entries | Basic |
| **Service log level** | Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Error**: only error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries | Info |

**Tracing**

| | | |
|---|---|---|
| **Application log level** | All the application messages for the repository service are saved to this logger.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **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.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **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.<br>Use the drop-down to set the verbosity of the logger:<br>• **Info**: fatal, error, warning, and information entries<br>• **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.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **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.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **Debug**: same as info, but also including debug entries | Info |

| | | |
|---|---|---|
| **Security log level** | All the certificates messages are saved to this logger.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **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.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **Debug**: same as info, but also including debug entries | Info |

| | | |
|---|---|---|
| **System log level** | All the standard repository messages are saved to this logger.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **Debug**: same as info, but also including debug entries | Info |

| | | |
|---|---|---|
| **User management log level** | All user sync messages are saved to this logger.<br>**Example:**<br>Error: User import failure or why a user directory connector setting is incorrect.<br>Warning: Potential error in data source, for example a circular dependence in Active Directory groups.<br>Info: Engine start and progress or user import start and user import results, for example number of users and user groups.<br>Debug: User request string to Active Director/LDAP server or SQL user query to ODBC source.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **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**

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

**Custom properties**

| Property | Description |
|---|---|
| **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.
   **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. Select **Nodes** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Click ⊕ **Create new** in the action bar.
3. Fill out the properties.

**Identification**

All fields are mandatory and must not be empty.

| 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`.<br>ⓘ *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 white list**.*<br>ⓘ *There is support for using an IPv6 address as host name.* |

### Node purpose

| Property | Description |
|---|---|
| **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, and the effects 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.
- Development: this server is intended to allow users to create apps but not serve the normal user traffic for users consuming published apps. In this case, the create and edit capabilities are enabled, but the server will not be considered when load balancing user traffic.
- 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.*

| Property | Description |
|---|---|
| **Failover candidate** | 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.<br>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.<br>*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.

| 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.

| 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**

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

**Custom properties**

| Property | Description |
|---|---|
| **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.

4. 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.*

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**.
6. 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. Select **Nodes** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the node that you want to edit.
3. Click **Edit** in the action bar.
4. Edit the properties.
   **Identification**
   All fields are mandatory and must not be empty.

| Property | Description |
|---|---|
| **Name** | The node name. |

| Property | Description |
|---|---|
| **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`.<br>*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 white list**.*<br>*There is support for using an IPv6 address as host name.* |

**Node purpose**

| Property | Description |
|---|---|
| **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, and the effects 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.
- Development: this server is intended to allow users to create apps but not serve the normal user traffic for users consuming published apps. In this case, the create and edit capabilities are enabled, but the server will not be considered when load balancing user traffic.
- 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.*

| Property | Description |
|---|---|
| **Failover candidate** | 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.<br>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.<br>ⓘ *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.

| 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.

| 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**

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

**Custom properties**

| Property | Description |
|---|---|
| **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.
   **Successfully updated** is displayed at the bottom of the page.

## 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:

- Select **Service cluster** on the QMC start page or from the **Start**▼ drop-down menu to display the service cluster page.

*All of the following settings are read only, except for **Failover timeout (minutes)**.*

**Identification**

| Property | Description |
|---|---|
| **Name** | Service cluster name. |

**Cluster settings**

| 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>*. |

| Property | Description |
|---|---|
| **Apps** | Root subfolder to which all nodes connect to retrieve apps. |
| **Static content root folder** | Root subfolder that contains static content, such as images. |
| **Connector 32 root folder** | Root subfolder for 32-bit Qv connectors. (Reserved for future use.) |
| **Connector 64 root folder** | Root subfolder for 64-bit Qv connectors. (Reserved for future use.) |
| **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.<br>Default value: 10 minutes. This value is editable. |

## Redistributing a certificate

A node that has not received the certificate correctly must be re-registered.

Do the following:

1. Select **Nodes** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. 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.
3. Click **Redistribute**.
   A dialog with **your authorization password** appears when finished.
4. 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. Select **Nodes** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the nodes that you want to delete.
3. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
4. 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. Select **Proxies** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the proxies that you want to edit.
3. Click **Edit** in the action bar.
4. Edit the properties.

   **Identification**

   All fields are mandatory and must not be empty.

| Property | Description | Default value |
|---|---|---|
| **Node** | The proxy name. | Inherits the node name. |

**Ports**

| Property | Description | Default value |
|---|---|---|
| **Service listen port HTTPS (default)** | The secure listen port for the proxy, which by default manages all Qlik Sense communication.<br>*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.*<br>*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.* | 443 |
| **Authentication listen port** | The listen port for the internal authentication module.<br>*When editing this port as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.* | 4244 |

| Property | Description | Default value |
|---|---|---|
| **Kerberos authentication** | Select to enable Kerberos authentication.<br>⚠ *If the Kerberos authentication setup is incorrectly configured, you risk locking yourself out from the QMC.* | Not selected |
| **REST API listen port** | The listen port for the proxy API.<br>ⓘ *When editing this port as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.* | 4243 |

| 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*.<br>⚠ *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.*<br>ℹ *The **Service listen port HTTP** needs to be set when **Allow HTTP** is checked.*<br>ℹ *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

| 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.

| Property | Description | Default value |
|---|---|---|
| **Audit activity log level** | Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Basic**: a limited set of entries | Basic |
| **Audit security log level** | Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Basic**: a limited set of entries | Basic |
| **Service log level** | Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Error**: only error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries | Info |

### TRACING

| | | |
|---|---|---|
| **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.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **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.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **Debug**: same as info, but also including debug entries | Info |
| **Security log level** | All the certificates messages are saved to this logger.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **Debug**: same as info, but also including debug entries | Info |

| | | |
|---|---|---|
| **System log level** | All the standard proxy messages are saved to this logger.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **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**

| 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 as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.<br>*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.*<br>*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.*<br>*Qlik Sense supports certificates that are made to use signing algorithms based on SHA-1 or SHA-256.* |

**Tags**

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

**Custom properties**

| Property | Description |
|---|---|
| **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. Edit the fields under **Associated items**.

**Virtual proxies**

| 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**. |

6. 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.

Do the following:

1. Select **Virtual proxies** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the virtual proxy that you want to add load balancing to.
3. Click **Edit**.
   The virtual proxy properties are shown.
4. In the **Load balancing** property, click ⊕ **Add new server node** to select which server nodes to add load balancing to.
   A dialog opens.
5. Select nodes from the list.
6. 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.

7. Click **OK**.
   **Successfully updated** is displayed at the bottom of the page.

## Configuring load balancing to isolate development nodes

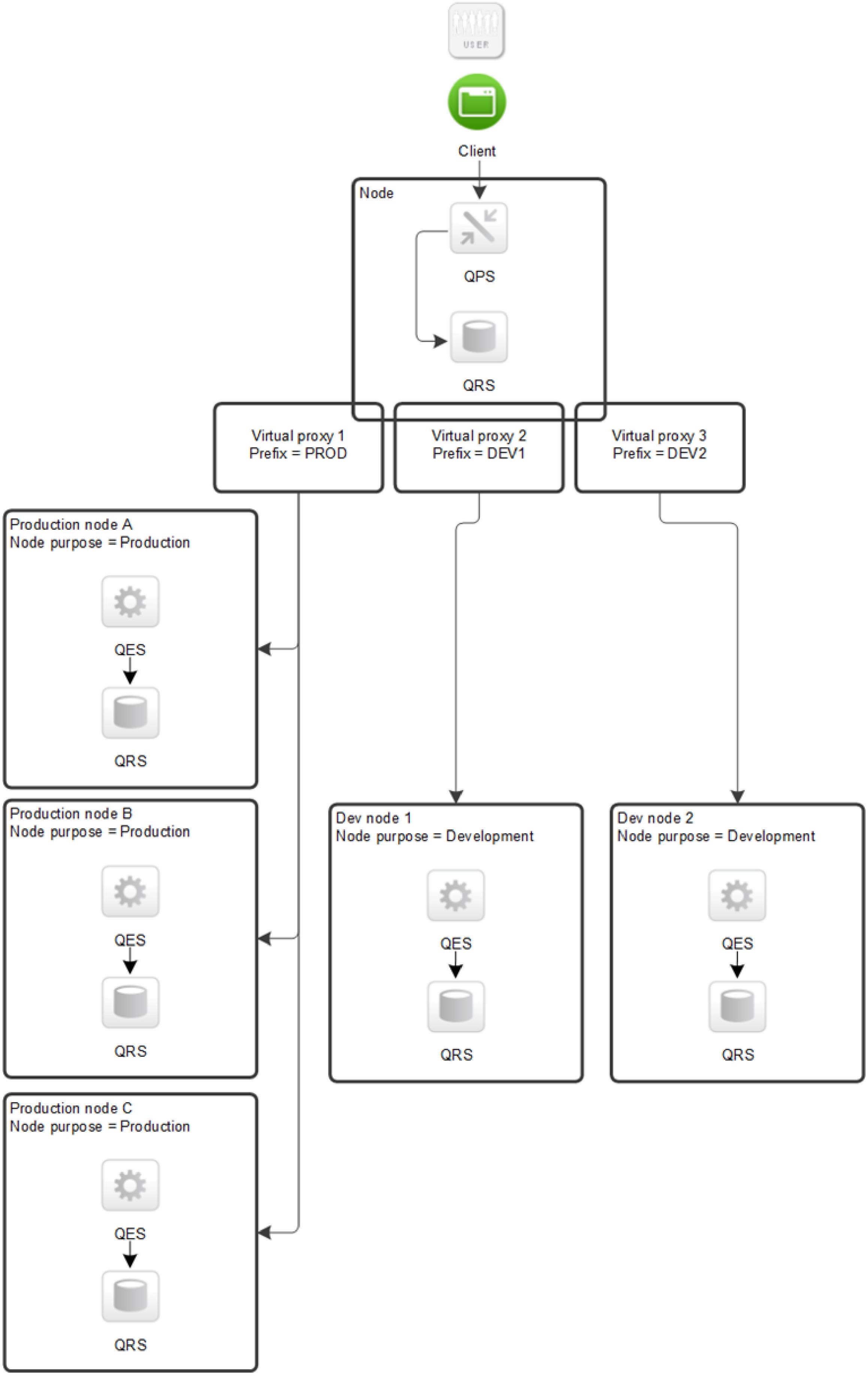
When you install multiple engines and virtual proxies, you must add load balancing to the new nodes and virtual proxies. It is only on the central node that load balancing is automatically added. You can configure a proxy so that it only talks to its local engine or to a subset of the engines, which 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.



USER
Client
Node
QPS
QRS
Virtual proxy 1
Prefix = PROD
Virtual proxy 2
Prefix = DEV1
Virtual proxy 3
Prefix = DEV2
Production node A
Node purpose = Production
QES
QRS
Production node B
Node purpose = Production
QES
QRS
Production node C
Node purpose = Production
QES
QRS
Dev node 1
Node purpose = Development
QES
QRS
Dev node 2
Node purpose = Development
QES
QRS

*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. Select **Virtual proxies** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the virtual proxies that you want to edit.
3. Click **Edit**.
   The virtual proxy properties are shown.
4. In the **Load balancing** property, click ✖ next to the node you want to delete load balancing from.
5. Click **Apply** in the action bar to save your changes.
   A confirmation dialog is displayed..
6. 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.

> *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 350)*

Do the following:

1. Select **Virtual proxies** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Click **Create new**. You cannot add a virtual proxy to more than one proxy at a time.
3. Edit the properties in the **Virtual proxy edit** window.

   **Identification**

   All fields are mandatory and must not be empty.

| 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.<br>Example:<br>*https://[node]/[prefix]/*<br>Note the following:<br>• 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.<br>• 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<br>• You can use slashes (/), but the prefix cannot begin nor end with a slash. | 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.<br>*It can be useful to include the value of the **Prefix** property above as a suffix in the cookie name.* | Blank |

**Authentication**

| Property | Description | Default value |
|---|---|---|
| **Anonymous access mode** | How to handle anonymous access:<br>• **No anonymous user**<br>• **Allow anonymous user**<br>• **Always anonymous user** | No anonymous user |
| **Authentication method** | • **Ticket**: a ticket is used for authentication.<br>• **Header authentication static user directory**: allows static header authentication, where the user directory is set in the QMC.<br>• **Header authentication dynamic user directory**: allows dynamic header authentication, where the user directory is fetched from the header.<br>• SAML: SAML2 is used for authentication.<br>• JWT: JSON Web Token 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).<br>*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 |

| 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.<br>**Example setting and matching header:**<br>`$ud\\$id` – matches USERDIRECTORY\userid (backslashes must be escaped with an additional \)<br>`$id@$ud` – matches userid@USERDIRECTORY ($id and $ud can be in any order)<br>`$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 |
| **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.<br>The server name does not have to be the same as the machine name, but in most cases it is.<br>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.<br>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.<br>Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property). | Blank |

| Property | Description | Default value |
|---|---|---|
| **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.<br>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.<br>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.<br>See: *I do not know the name of a mandatory SAML attribute (page 511)* | 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'.<br>See: *I do not know the name of a mandatory SAML attribute (page 511)* | Blank |
| **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'. | |

| 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.<br>`-----BEGIN CERTIFICATE-----`<br>`MIIDYTCCAkmgAwIBAgIJAM/oG48ciCGeMA0GCSqGSIb3DQEBCwUAMECxED`<br>`AOBgNV`<br>`BAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubmUxHjAcBgkqhkiG9w`<br>`0BCQEW`<br>`D2pkZUBjb21wYW55LmNvbTAeFw0xNzAzMjAxMjMxNDhaFw0yNzAzMTgxMj`<br>`MxNDha`<br>`MECxEDAOBgNVBAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubmUxHj`<br>`AcBgkq`<br>`hkiG9w0BCQEWD2pkZUBjb21wYW55LmNvbTCCASIwDQYJKoZIhvcNAQEBBQ`<br>`ADggEP`<br>`ADCCAQoCggEBALIaab/y0u/kVIZnUsRVJ9vaZ2coiB3dVl/PCa40fyZdOI`<br>`K5CvbA`<br>`d0mJhuM7m/L4PldKmWh7nsPVC6SHAwgVwXASPHZQ6qha9ENChI2NfvqY4h`<br>`XTH//Y`<br>`FYaGLuKHD7pE7Jqt7Bhdh1zbBjrzsr1eU4Owwv9W9DxM4tVx3Xx8AUCNRo`<br>`EWgObz`<br>`Oqw9CfYY7/AWB8Hnr8G22X/l0/i4uJhiIKDVEisZ55hiNTEyqwW/ew0ilI`<br>`7EAngw`<br>`L80D7WXpC2tCCe2V3fgUjQM4Q+0jEZGiARhzRhtaceuTBnnKq3+DnHmW4H`<br>`zBuhZB`<br>`CLMuWaJowkKaSfCQMel6u0/Evxc8i8FkPeMCAwEAAaNQME4wHQYDVR0OBB`<br>`YEFNQ9`<br>`M2Y5WlRCyftHlD2oIk12YHyBMB8GA1UdIwQYMBaAFNQ9M2Y5WlRCyftHlD`<br>`2oIk12`<br>`YHyBMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAHO46YLxtc`<br>`Mcanol`<br>`PUC5nGdyYchZVHkd4F5MIe82mypwFszXGvpxKQXyAIPMkTIGb1wnE/wbCf`<br>`B7moxX`<br>`oFo+NoASER6wtt6FPHNcCiCXHm3B+2at16nOeMLfDefhQq03Q7qjfoa+7w`<br>`oAYole`<br>`C9fTHGAl4TMIPThGSluiVLOLgHFUHpZryI6DdiEutXiH4afXaw0mScG36Z`<br>`1uvHIq`<br>`dPtjb/vDm1b9jvLITe8mZ8c2is1aBCLOdFvNupARxK7U3UD6HzGIh4x7eq`<br>`o6Q9CK`<br>`mKIz25FHrKTkyi1n/0+SAlOGp8PSnWrRZKmHkHbpfY5lpCuIBY9Cu2l1Xe`<br>`q4QW5E`<br>`AqFLKKE=`<br>`-----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 |

**Load balancing**

| Property | Description | Default value |
|---|---|---|
| **Load balancing nodes** | Click **Add new server node** to add load balancing to that node. | Blank |

**Advanced**

| 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.<br>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.<br>Example:<br>`company.com` | Blank (default machine) |
| **Additional response headers** | Headers added to all HTTP responses back to the client.<br>Example:<br>`Header1: value1`<br>`Header2: value2` | Blank |

| Property | Description | Default value |
|---|---|---|
| **Host white list** | 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.<br>To support switching schema when using cross-origin resource sharing (CORS), the host white list must include the schema to avoid requests being blocked by the CORS policy.<br>**Example:**<br>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 white list.<br>*Even if the white list is empty, the name of the machine where Qlik Sense is installed is still considered part of the white list, although not visible.* | Blank |

### Integration

| 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.*

| 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. | - |

See: *Configuring client authentication (page 406)*

### Tags

| Property | Description |
|---|---|
| **Tags** | *If no QMC tags are available, this property group is empty.*<br>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**

| Property | Description |
|---|---|
| **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. |

4. Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.
5. 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 350)*

*For security reasons, some settings in the default virtual proxy are not editable. Incorrect settings could make the system inoperable.*

Do the following:

1. Select **Virtual proxies** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. 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.
3. Edit the properties in the **Virtual proxy edit** window:
   **Identification**
   All fields are mandatory and must not be empty.

| 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.<br>Example:<br>*https://[node]/[prefix]/*<br>Note the following:<br>• 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.<br>• 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<br>• You can use slashes (/), but the prefix cannot begin nor end with a slash. | 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.<br>*It can be useful to include the value of the* ***Prefix*** *property above as a suffix in the cookie name.* | Blank |

**Authentication**

| Property | Description | Default value |
|---|---|---|
| **Anonymous access mode** | How to handle anonymous access:<br>- **No anonymous user**<br>- **Allow anonymous user**<br>- **Always anonymous user** | No anonymous user |
| **Authentication method** | - **Ticket**: a ticket is used for authentication.<br>- **Header authentication static user directory**: allows static header authentication, where the user directory is set in the QMC.<br>- **Header authentication dynamic user directory**: allows dynamic header authentication, where the user directory is fetched from the header.<br>- SAML: SAML2 is used for authentication.<br>- JWT: JSON Web Token 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).<br>*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 |

| 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.<br>**Example setting and matching header:**<br>`$ud\\$id` – matches USERDIRECTORY\userid (backslashes must be escaped with an additional \)<br>`$id@$ud` – matches userid@USERDIRECTORY ($id and $ud can be in any order)<br>`$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 |
| **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.<br>The server name does not have to be the same as the machine name, but in most cases it is.<br>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.<br>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.<br>Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property). | Blank |

| Property | Description | Default value |
|---|---|---|
| **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.<br>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.<br>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.<br>See: *I do not know the name of a mandatory SAML attribute (page 511)* | 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'.<br>See: *I do not know the name of a mandatory SAML attribute (page 511)* | Blank |
| **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'. | |

| 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.<br>-----BEGIN CERTIFICATE-----<br>MIIDYTCCAkmgAwIBAgIJAM/oG48ciCGeMA0GCSqGSIb3DQEBCwUAMEcxEDAOBgNV<br>BAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubmUxHjAcBgkqhkiG9w0BCQEW<br>D2pkZUBjb21wYW55LmNvbTAeFw0xNzAzMjAxMjMxNDhaFw0yNzAzMTgxMjMxNDha<br>MEcxEDAOBgNVBAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubmUxHjAcBgkq<br>hkiG9w0BCQEWD2pkZUBjb21wYW55LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP<br>ADCCAQoCggEBALIaab/y0u/kVIZnUsRVJ9vaZ2coiB3dVl/PCa40fyZdOIK5CvbA<br>d0mJhuM7m/L4PldKmWh7nsPVC6SHAwgVwXASPHZQ6qha9ENChI2NfvqY4hXTH//Y<br>FYaGLuKHD7pE7Jqt7Bhdh1zbBjrzsr1eU4Owwv9W9DxM4tVx3Xx8AUCNRoEWgObz<br>Oqw9CfYY7/AWB8Hnr8G22X/l0/i4uJhiIKDVEisZ55hiNTEyqwW/ew0ilI7EAngw<br>L80D7WXpC2tCCe2V3fgUjQM4Q+0jEZGiARhzRhtaceuTBnnKq3+DnHmW4HzBuhZB<br>CLMuWaJowkKaSfCQMel6u0/Evxc8i8FkPeMCAwEAAaNQME4wHQYDVR0OBBYEFNQ9<br>M2Y5WlRCyftHlD2oIk12YHyBMB8GA1UdIwQYMBaAFNQ9M2Y5WlRCyftHlD2oIk12<br>YHyBMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAHO46YLxtcMcanol<br>PUC5nGdyYchZVHkd4F5MIe82mypwFszXGvpxKQXyAIPMkTIGb1wnE/wbCfB7moxX<br>oFo+NoASER6wtt6FPHNcCiCXHm3B+2at16nOeMLfDefhQq03Q7qjfoa+7woAYole<br>C9fTHGAl4TMIPThGSluiVLOLgHFUHpZryI6DdiEutXiH4afXaw0mScG36Z1uvHIq<br>dPtjb/vDm1b9jvLITe8mZ8c2is1aBCLOdFvNupARxK7U3UD6HzGIh4x7eqo6Q9CK<br>mKIz25FHrKTkyi1n/0+SAlOGp8PSnWrRZKmHkHbpfY5lpCuIBY9Cu2l1Xeq4QW5E<br>AqFLKKE=<br>-----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 |

### Load balancing

| Property | Description | Default value |
|---|---|---|
| **Load balancing nodes** | Click **Add new server node** to add load balancing to that node. | Blank |

### Advanced

| 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.<br>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.<br>Example:<br>`company.com` | Blank (default machine) |
| **Additional response headers** | Headers added to all HTTP responses back to the client.<br>Example:<br>`Header1: value1`<br>`Header2: value2` | Blank |

| Property | Description | Default value |
|---|---|---|
| **Host white list** | 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.<br>To support switching schema when using cross-origin resource sharing (CORS), the host white list must include the schema to avoid requests being blocked by the CORS policy.<br>**Example:**<br>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 white list.<br>*Even if the white list is empty, the name of the machine where Qlik Sense is installed is still considered part of the white list, although not visible.* | Blank |

### Integration

| 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.*

| 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. | - |

See: *Configuring client authentication (page 406)*

### Tags

| Property | Description |
|---|---|
| **Tags** | *If no QMC tags are available, this property group is empty.*<br>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**

| Property | Description |
|---|---|
| **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. |

4. Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.
5. Edit the fields under **Associated items**.

**Proxies**

| | |
|---|---|
| **Node** | The proxy name. |
| **Status** | One of the following statuses is displayed:<br>• **Running**<br>The service is running as per normal.<br>• **Stopped**<br>The service has stopped.<br>• **Disabled**<br>The service has been disabled.<br>*Click ⓘ in the **Status** column for more detailed information on the status.*<br>See: *Checking the status of Qlik Sense services (page 299)*. |
| **Service listen port HTTPS (default)** | The secure listen port for the proxy, which by default manages all Qlik Sense communication.<br>*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**.<br>**Yes**: Unencrypted communication is allowed. This means that both https (secure communication) and (http) unencrypted communication is allowed. |
| **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.<br>*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**.<br>**Yes**: Kerberos authentication is enabled. |
| **REST API listen port** | The listen port for the proxy API.<br>*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.<br>*When editing a proxy certificate as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.* |
| **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.<br>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.<br>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.<br>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.<br>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.<br>To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.<br>You can combine filtering with searching.<br>See: *Searching and filtering in the QMC (page 33)* |
| **Edit** | Edit the selected proxy. |

| | |
|---|---|
| **Unlink** | Unlink a proxy service from the selected proxy.<br>*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. |

6. 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. Select **Virtual proxies** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the virtual proxy that you want to link to a proxy.
3. Click **Edit** in the action bar.
4. To the right on the **Virtual proxy edit** page, under **Associated items**, click **Proxies**.
   The **Associated proxies** page is opened.
5. In the action bar, click ⊕ **Link**.
   The **Select proxy services** page is opened.
6. 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.
7. 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. Select **Virtual proxies** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the virtual proxy you want to delete. You cannot delete virtual proxies for more than one proxy at a time.
3. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
4. Click **OK**.

## Editing schedulers

You can edit schedulers that you have update rights to.

Do the following:

1. Select **Schedulers** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the schedulers that you want to edit.
3. 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.
4. 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.

   | 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.

   | Property | Description | Default value |
   |---|---|---|
   | **Audit activity log level** | Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Basic**: a limited set of entries | Basic |

| Property | Description | Default value |
|---|---|---|
| **Service log level** | Use the drop-down to set the verbosity of the logger:<br>- **Off**: no entries<br>- **Error**: only error entries<br>- **Warning**: same as error, but also including warning entries<br>- **Info**: same as warning, but also including information entries | Info |

**Tracing**

| | | |
|---|---|---|
| **Application log level** | All the application messages for the scheduler service are saved to this logger.<br>Use the drop-down to set the verbosity of the logger:<br>- **Off**: no entries<br>- **Fatal**: only fatal entries<br>- **Error**: same as fatal, but also including error entries<br>- **Warning**: same as error, but also including warning entries<br>- **Info**: same as warning, but also including information entries<br>- **Debug**: same as info, but also including debug entries | Info |

| | | |
|---|---|---|
| **Audit log level** | More detailed, user based, messages are saved to this logger.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **Debug**: same as info, but also including debug entries | Info |
| **Performance log level** | All the performance messages are saved to this logger.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **Debug**: same as info, but also including debug entries | Info |

| | | |
|---|---|---|
| **Security log level** | All the certificates messages are saved to this logger.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **Debug**: same as info, but also including debug entries | Info |
| **System log level** | All the standard scheduler messages are saved to this logger.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **Debug**: same as info, but also including debug entries | Info |

| | | |
|---|---|---|
| **Task execution log level** | All the task execution messages are saved to this logger.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **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>.*

**Advanced**

| Property | Description | Default value |
|---|---|---|
| **Type** | If enabled by the property above, the QSS type is set to:<br>• Master: sends the task to a slave QSS within the site.<br>• Slave: receives the task from the master QSS and executes the task.<br>• Master and slave: when the master QSS also acts a slave QSS, on a single node site. | Slave (except for on a central node; Master) |
| **Max concurrent reloads** | The maximum number of reloads that the scheduler can perform at the same time. | 4 |

| Property | Description | Default value |
|---|---|---|
| **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**

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

**Custom properties**

| Property | Description |
|---|---|
| **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** 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. Select **Engines** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the engine that you want to edit.
3. Click **Edit** in the action bar.
4. Edit the properties.
   **Identification**

| Property | Description | Default value |
|---|---|---|
| **Node** | The engine name. | Inherits the node name. |

**Apps**

| 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.<br>ⓘ *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**

| 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.<br>Click ⊕ to add more ports. Click ⊗ to remove a port. | 4747 |

| Property | Description | Default value |
|---|---|---|
| **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.<br>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. | 70 |
| **Max memory usage (%)** | The maximum memory capacity used by Qlik Sense. | 90 |
| **Memory usage mode** | Use the drop-down to select one of the following methods:<br>• **Hard max limit**: never use more memory than defined by the property above.<br>• **Ignore max limit**: use as much memory as necessary, regardless of the **Max memory usage (%)** setting.<br>• **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.<br>ⓘ *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) |

| Property | Description | Default value |
|---|---|---|
| **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.<br>*Disabling standard mode can create a security risk by exposing the file system.* | Selected |
| **HTTP callback port** | The callback port used by the Qlik Sense repository service for sending HTTP events to engine. | 4748 |

| Property | Description | Default value |
|---|---|---|
| **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 .<br>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.<br>A negative value disables the limit.<br>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.<br>A negative value or 0 disables the limit.<br>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.<br>A negative value or 0 disables the limit.<br>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.<br>A negative value or 0 disables the limit.<br>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.<br>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.<br>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.

| Property | Description | Default value |
|---|---|---|
| **Audit activity log level** | Use the drop-down to set the verbosity of the logger:<br>- **Off**: no entries<br>- **Basic**: a limited set of entries | Basic |
| **Service log level** | Use the drop-down to set the verbosity of the logger:<br>- **Off**: no entries<br>- **Error**: only error entries<br>- **Warning**: same as error, but also including warning entries<br>- **Info**: same as warning, but also including information entries | Info |

**TRACING**

| | | |
|---|---|---|
| **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.<br>Use the drop-down to set the verbosity of the logger:<br>- **Off**: no entries<br>- **Fatal**: only fatal entries<br>- **Error**: same as fatal, but also including error entries<br>- **Warning**: same as error, but also including warning entries<br>- **Info**: same as warning, but also including information entries<br>- **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.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **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.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **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.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **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.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **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.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **Debug**: same as info, but also including debug entries | Off |
| **Analytic connections log level** | All the analytic connections messages are saved to this logger.<br>Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **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**

| Property | Description |
|---|---|
| **Tags** | Click the text box to display the available tags. Start typing to filter the list. Connected tags are listed under the text box. |

**Custom properties**

| Property | Description |
|---|---|
| **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.*

5. 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. Select **Printing** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the printing services that you want to edit.
3. Click **Edit** in the action bar.
4. 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.

| Property | Description | Default value |
|---|---|---|
| **Node** | The name of the printing service. | Inherits the node name. |

### Logging

| Property | Description | Default value |
|---|---|---|
| **Audit activity log level** | Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Fatal**: only fatal entries<br>• **Error**: same as fatal, but also including error entries<br>• **Warning**: same as error, but also including warning entries<br>• **Info**: same as warning, but also including information entries<br>• **Debug**: same as info, but also including debug entries | Info |
| **Service log level** | Use the drop-down to set the verbosity of the logger:<br>• **Off**: no entries<br>• **Error**: only error entries<br>• **Warning**: same as error, but also including warning entries<br>• **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

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

**Custom properties**

| Property | Description |
|---|---|
| **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.

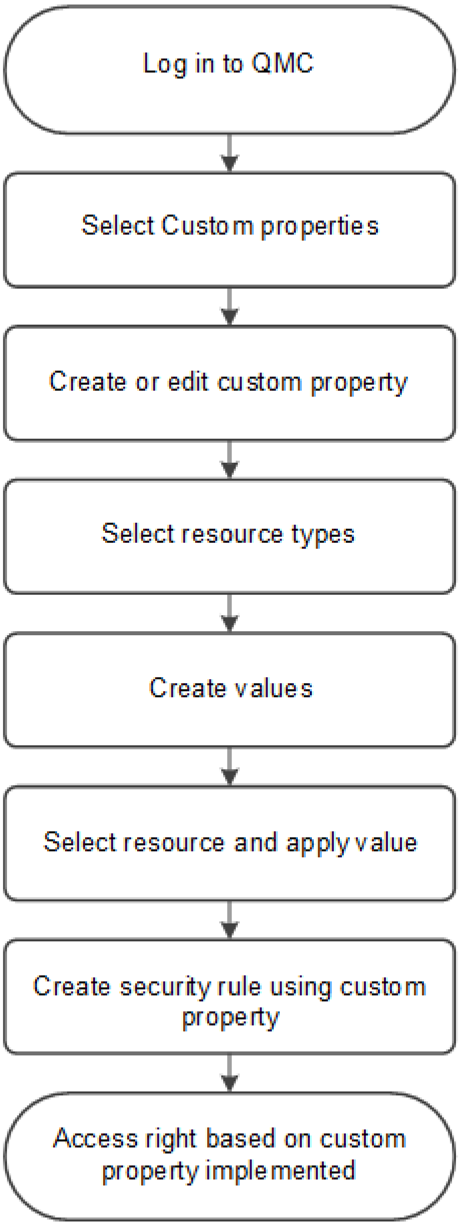
5. Click **Apply** in the action bar to save your changes.
   **Successfully updated** is displayed at the bottom of the page.

## 3.9 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.*

This flow describes using custom properties:


Log in to QMC
Select Custom properties
Create or edit custom property
Select resource types
Create values
Select resource and apply value
Create security rule using custom property
Access right based on custom property implemented

## Creating a custom property

You can create a custom property.

Do the following:

1. Select **Custom properties** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Click ⊕ **Create new** in the action bar.
3. Edit the properties.

### Identification

| 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). |

### Resource types

| Property | Description |
|---|---|
| **Resource types** | Select the resources that you want to make the custom property available for.<br>Custom properties can be applied to the following resources:<br>**Analytic connections**<br>**Apps**<br>**Content libraries**<br>**Data connections**<br>**Engines**<br>**Extensions**<br>**Nodes**<br>**Printing**<br>**Proxies**<br>**Reload tasks**<br>**Repositories**<br>**Schedulers**<br>**Streams**<br>**User synchronization tasks**<br>**Users**<br>**Virtual proxies** |

### Values

| Property | Description |
|---|---|
| **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.

> ⓘ *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 the deletion.

4. 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.

> *You cannot edit properties for several custom properties at the same time.*

Do the following:

1. Select **Custom properties** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select one custom property and click **Edit** in the action bar at the bottom of the page.
3. Edit the properties.

   **Identification**

   | 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). |

   **Resource types**

   | Property | Description |
   |---|---|
   | **Resource types** | Select the resources that you want to make the custom property available for.<br>Custom properties can be applied to the following resources:<br>**Analytic connections**<br>**Apps**<br>**Content libraries**<br>**Data connections**<br>**Engines**<br>**Extensions**<br>**Nodes**<br>**Printing**<br>**Proxies**<br>**Reload tasks**<br>**Repositories**<br>**Schedulers**<br>**Streams**<br>**User synchronization tasks**<br>**Users**<br>**Virtual proxies** |

**Values**

| Property | Description |
|---|---|
| **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.

*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.

4. 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. Select **Custom properties** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the custom properties that you want to delete.
3. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
4. 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. Select a resource on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select one or more resources and click **Edit**.
3. 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.*

4. Click the text box next to the custom property to display a list of available values.
5. Select the values that you want to use.

The values are displayed under the text box.

6. 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.

### Creation of the custom property

Do the following:

1. In the QMC, open **Custom properties**.
2. Click ⊕ **Create new**.
3. Name the customer property *AccessAllResources*.
4. Under **Resource types**, select **Users**.
5. Under **Values**, click ⊕ **Create new** and name the value *ReaderOnly*.
6. 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.*

### Creation of the security rule

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.*

### Application of the custom property 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.

## 3.10 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. Select **Tags** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Click ⊕ **Create new** in the action bar.
3. Type a tag name.

   **Identification**

   | 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.

   | Property | Description |
   |---|---|
   | **Apps** | The resources that the tag is connected to. |
   | **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** | |

4. 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. 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:* ▼

2. Select the items that you want to connect a tag to and click **Edit** in the action bar.
3. Ensure that **Tags** is selected in the **Properties** section.
4. 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.*

5. To filter the list, start typing the tag name.
6. Select a tag.
   The tag is added in blue under the text box.
7. 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. 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:* ▼

2. Select the items you want to remove a tag from and click **Edit** in the action bar.
3. Ensure that **Tags** is selected in the **Properties** section.
4. Under the **Tags** text box, click ⊗ to remove the tag.
5. 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. Select **Tags** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the tags that you want to edit.
3. Click **Edit** in the action bar.
4. Edit the properties.

   **Identification**

   | 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.

   | Property | Description |
   |---|---|
   | **Apps** | The resources that the tag is connected to. |
   | **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** | |

5. 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:

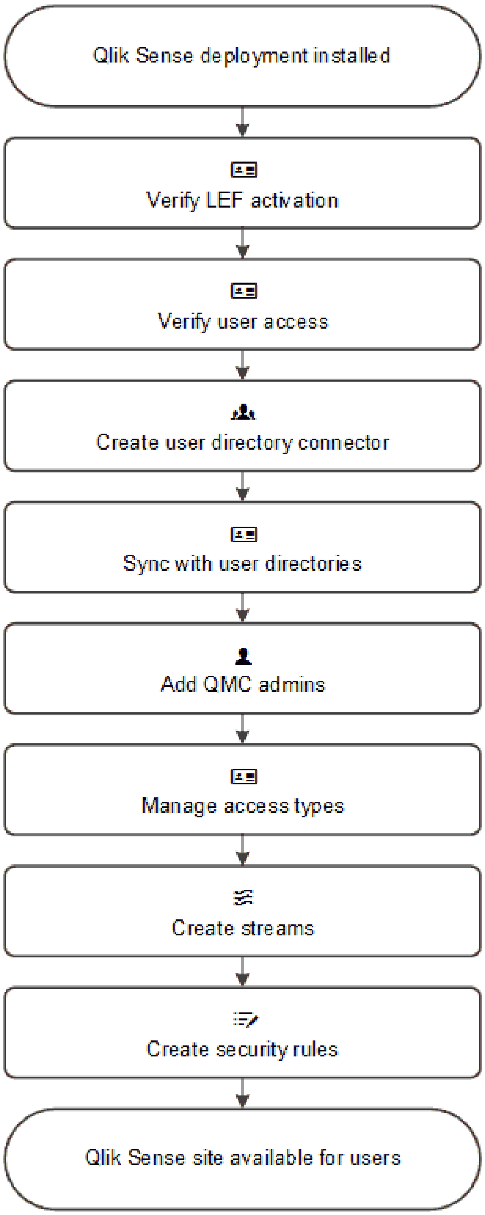
1. Select **Tags** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the tags that you want to delete.

   > *You can filter a column by using the filtering option:* ▼

3. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
4. Click **OK**.

# 4 Configuring Qlik Sense

When Qlik Sense 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 after installation:


Qlik Sense deployment installed
Verify LEF activation
Verify user access
Create user directory connector
Sync with user directories
Add QMC admins
Manage access types
Create streams
Create security rules
Qlik Sense site available for users

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 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****.*

## 4.1 Default configuration

A Qlik Sense installation includes the streams **Everyone** and **Monitoring apps**, and five administrator roles: **RootAdmin**, **AuditAdmin**, **ContentAdmin**, **DeploymentAdmin**, 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:
  - 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.

# 4.2 Configuring security

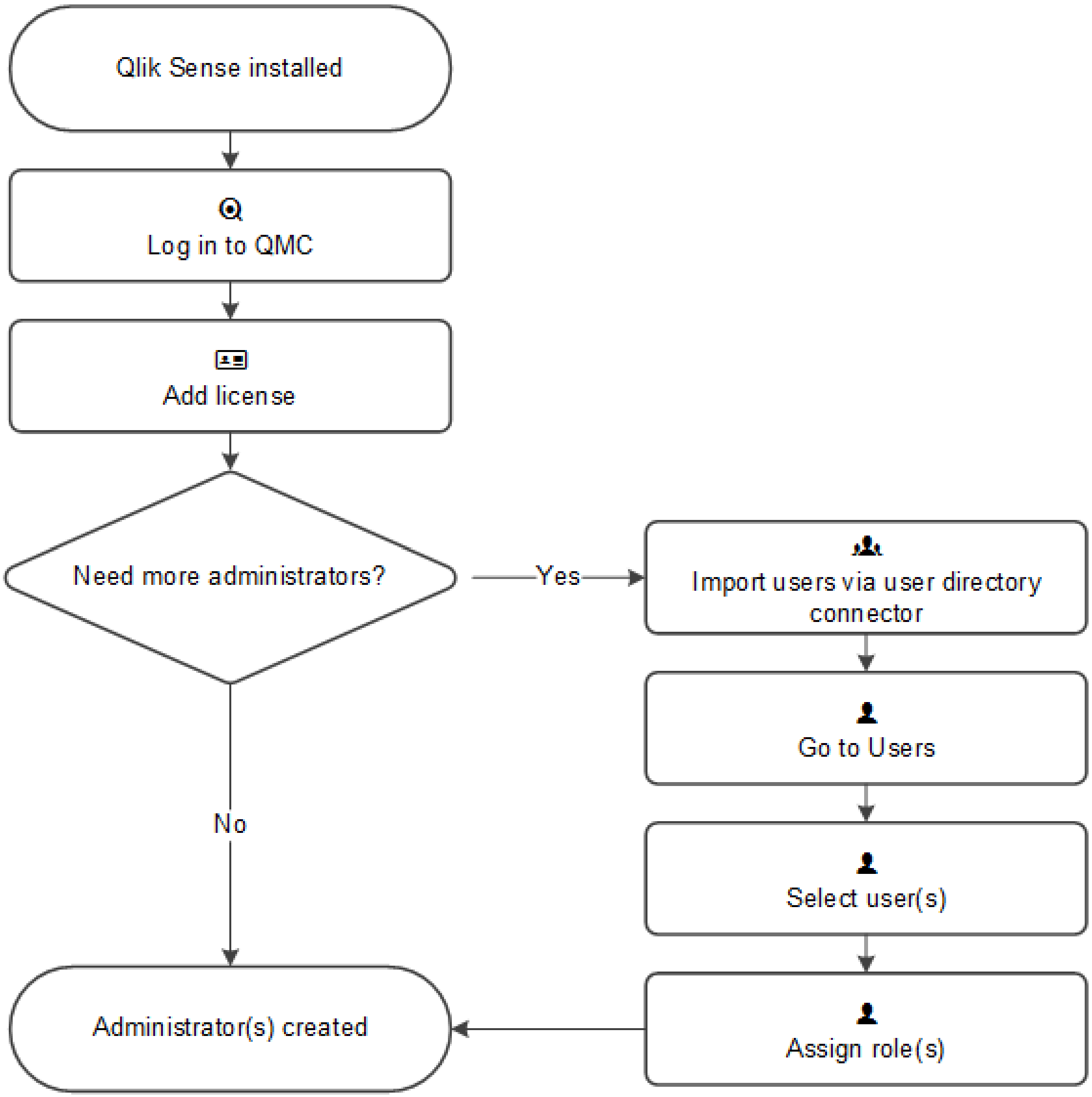
You manage the following Qlik Sense security settings from the QMC:

- 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.

## 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 if needed, or assigned other admin roles with other 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 384)*.

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.*

   *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.

*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.*

*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 384)* table displays an overview of the default QMC administrator roles, which parts of the QMC they can manage, and what administration rights they have.

*As RootAdmin or SecurityAdmin you have the possibility to create new roles to suit your purposes.*

### Administration rights

The *Legend (page 386)* describes the actions presented in this table.

| QMC resource | AuditAdmin | ContentAdmin | DeploymentAdmin | 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 |
| 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 | |
| UserSyncTask_* | R | CRUD | CRUD | CRUD |
| SchemaEvent_* | R | CRUD | CRUD | |
| 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 | SecurityAdmin |
|---|---|---|---|---|
| TermsAcceptance_* | R | R | CRUD | R |
| ServiceStatus_* | R | | CRUD | R |
| ServiceCluster | R | | CRUD | |
| LoadBalancingSelectList | R | | R | |
| *(All in Audit view) | R | | | |

**Legend**

The following table presents the actions that are available for administrators.

| 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: Default administration roles (page 384).*

### Read access rights for default administrators

An "R" indicates that an admin has read access to that QMC section.

| 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 |
| QmcSection_VirtualProxyConfiguration | | | R | R |

| QMC | AuditAdmin | ContentAdmin | DeploymentAdmin | SecurityAdmin |
|---|---|---|---|---|
| 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.ApplicationAccessType | | | R | |
| QmcSection_Token | | | R | |
| QmcSection_UserDirectory | | | R | |
| QmcSection_Certificates | | | R | R |
| QmcSection_ Certificates.Export | | | R | R |
| QmcSection_SyncRule | | | R | |
| QmcSection_ LoadBalancingRules | | | 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.

## 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.*

Do the following:

1. Select **Virtual proxies** on the QMC start page or from the **Start▼** drop-down menu to display the overview.
2. Select the virtual proxy that handles the authentication and click **Edit**.
3. 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.
4. 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 login access rule that allows anonymous users.

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.

## 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. Select **Virtual proxies** on the QMC start page or from the **Start**▼ drop-down menu to display the overview.
2. Select the virtual proxy that handles the authentication and click **Edit**.
3. In the **Authentication** property group, make the necessary selections.
   Depending on what authentication method you select, there are different additional fields.

| Property | Description | Default value |
|---|---|---|
| **Anonymous access mode** | How to handle anonymous access:<br>• **No anonymous user**<br>• **Allow anonymous user**<br>• **Always anonymous user** | No anonymous user |
| **Authentication method** | • **Ticket**: a ticket is used for authentication.<br>• **Header authentication static user directory**: allows static header authentication, where the user directory is set in the QMC.<br>• **Header authentication dynamic user directory**: allows dynamic header authentication, where the user directory is fetched from the header.<br>• SAML: SAML2 is used for authentication.<br>• JWT: JSON Web Token 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).<br>*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 |

| 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.<br>**Example setting and matching header:**<br>`$ud\\$id` – matches USERDIRECTORY\userid (backslashes must be escaped with an additional \)<br>`$id@$ud` – matches userid@USERDIRECTORY ($id and $ud can be in any order)<br>`$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.<br>The server name does not have to be the same as the machine name, but in most cases it is.<br>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.<br>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.<br>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.<br>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.<br>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.<br>See: *I do not know the name of a mandatory SAML attribute (page 511)* | 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'.<br>See: *I do not know the name of a mandatory SAML attribute (page 511)* | 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'. | |

| 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.<br>-----BEGIN CERTIFICATE-----<br>MIIDYTCCAkmgAwIBAgIJAM/oG48ciCGeMA0GCSqGSIb3DQEBCwUAME<br>cxEDAOBgNV<br>BAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubmUxHjAcBgkqhk<br>iG9w0BCQEW<br>D2pkZUBjb21wYW55LmNvbTAeFw0xNzAzMjAxMjMxNDhaFw0yNzAzMT<br>gxMjMxNDha<br>MEcxEDAOBgNVBAoMB0NvbXBhbnkxEzARBgNVBAMMCkpvaG4gRG9ubm<br>UxHjAcBgkq<br>hkiG9w0BCQEWD2pkZUBjb21wYW55LmNvbTCCASIwDQYJKoZIhvcNAQ<br>EBBQADggEP<br>ADCCAQoCggEBALIaab/y0u/kVIZnUsRVJ9vaZ2coiB3dVl/PCa40fy<br>ZdOIK5CvbA<br>d0mJhuM7m/L4PldKmWh7nsPVC6SHAwgVwXASPHZQ6qha9ENChI2Nfv<br>qY4hXTH//Y<br>FYaGLuKHD7pE7Jqt7Bhdh1zbBjrzsr1eU4Owwv9W9DxM4tVx3Xx8AU<br>CNRoEWgObz<br>Oqw9CfYY7/AWB8Hnr8G22X/l0/i4uJhiIKDVEisZ55hiNTEyqwW/ew<br>0ilI7EAngw<br>L80D7WXpC2tCCe2V3fgUjQM4Q+0jEZGiARhzRhtaceuTBnnKq3+DnH<br>mW4HzBuhZB<br>CLMuWaJowkKaSfCQMel6u0/Evxc8i8FkPeMCAwEAAaNQME4wHQYDVR<br>0OBBYEFNQ9<br>M2Y5WlRCyftHlD2oIk12YHyBMB8GA1UdIwQYMBaAFNQ9M2Y5WlRCyf<br>tHlD2oIk12<br>YHyBMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAHO46Y<br>LxtcMcanol<br>PUC5nGdyYchZVHkd4F5MIe82mypwFszXGvpxKQXyAIPMkTIGb1wnE/<br>wbCfB7moxX<br>oFo+NoASER6wtt6FPHNcCiCXHm3B+2at16nOeMLfDefhQq03Q7qjfo<br>a+7woAYole<br>C9fTHGAl4TMIPThGSluiVLOLgHFUHpZryI6DdiEutXiH4afXaw0mSc<br>G36Z1uvHIq<br>dPtjb/vDm1b9jvLITe8mZ8c2is1aBCLOdFvNupARxK7U3UD6HzGIh4<br>x7eqo6Q9CK<br>mKIz25FHrKTkyi1n/0+SAlOGp8PSnWrRZKmHkHbpfY5lpCuIBY9Cu2<br>l1Xeq4QW5E<br>AqFLKKE=<br>-----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 |

4. 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 is used for authentication. 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.

*If RelayState is empty, misspelled, or not part of the host white list, the user will automatically be redirected to the hub.*

*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.

> *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

> *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.
   See: *Creating a virtual proxy (page 329)*

> *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. If your IdP requires a certificate, use the file *server.pem* that is available from *%ProgramData%\Qlik\Sense\Repository\Exported Certificates\.Local Certificates*. For example, to activate single logout in OKTA you must upload a service provider certificate.

### 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.

## 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.

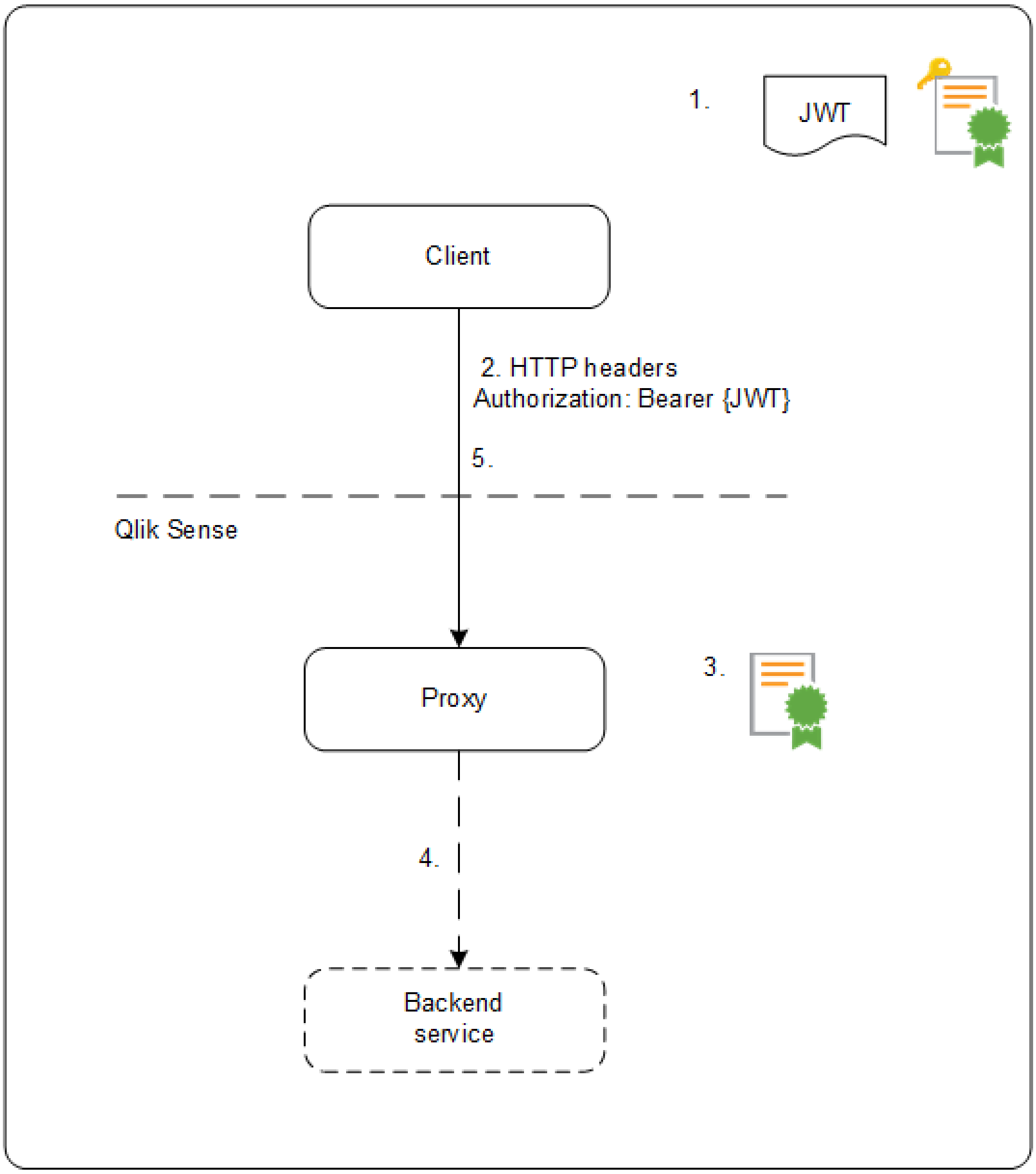
## Supported signature algorithms

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.
   1. If the calls do include a JWT it will be validated, and if it is invalid the user will be rejected access.
   2. 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.
- Only the following signing algorithms are supported:
  - RS256 - RSA signature with SHA256
  - RS384 - RSA signature with SHA384
  - RS512 - RSA signature with SHA512

## 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.

| **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<br>>0: Upper case<br><0: Lower case |
| SSOExternalId | 0 | 0: QlikId (domain\username)<br>1: UPN<br>(username@domain.com)<br>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.

*Only the vendor supplied driver works in this configuration, not the driver in the Qlik Connector Package.*

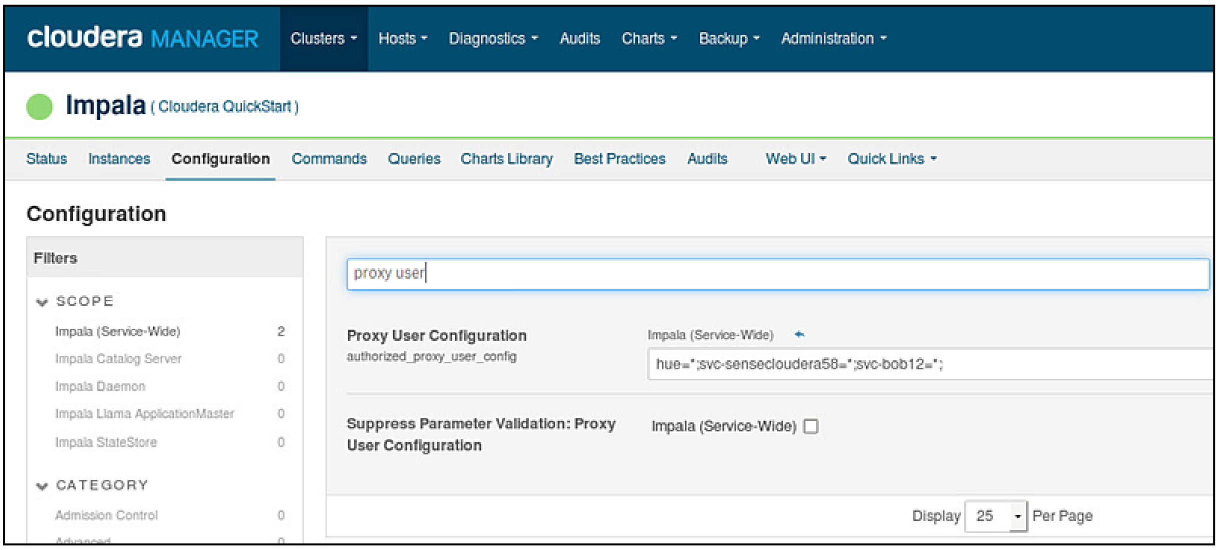
*This configuration is for Cloudera Impala only, Hive requires a different configuration option.*

## 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=*;*



Configuration

proxy user

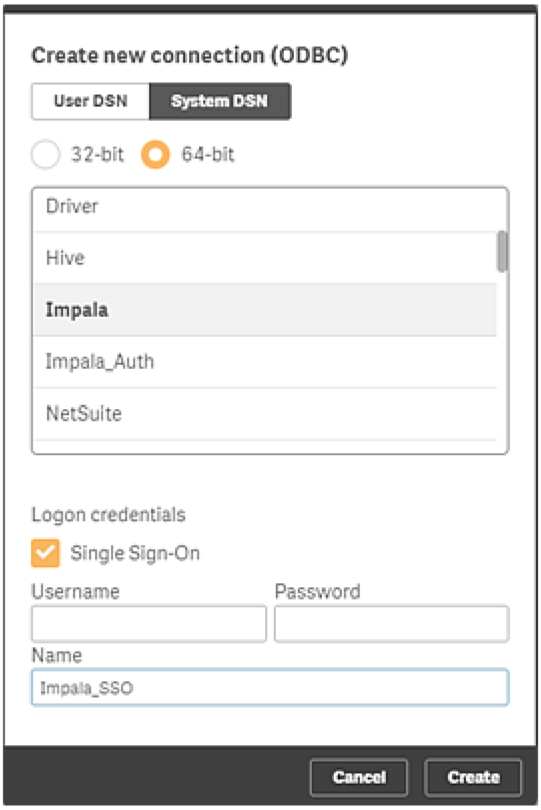
Proxy User Configuration
authorized_proxy_user_config
Impala (Service-Wide)
hue=*;svc-sensecloudera58=*;svc-bob12=*;

Suppress Parameter Validation: Proxy User Configuration
Impala (Service-Wide) ☐

*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 405)*, 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**.



Create new connection (ODBC)

User DSN | **System DSN**

○ 32-bit ● 64-bit

Driver

- Hive
- **Impala**
- Impala_Auth
- NetSuite

Logon credentials

☑ Single Sign-On

Username

Password

Name

Impala_SSO

   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*

| Setting | Default value | Possible values |
|---|---|---|
| **SSODisableLogOn** | 0 | 0: Enables SSO<br>1: Disables SSO |

| | | |
|---|---|---|
| **SSOCasing** | 0 | 0: Case sensitive<br>>0: Upper case<br><0: Lower case |
| **SSOExternalId** | 0 | 0: QlikId (domain\username)<br>1: UPN (username@domain.com)<br>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.

Make sure user access or professional access is allocated to the users.

For more information about access, see *Managing user access (page 255)* and *Managing professional access (page 246)*.

> *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**.

   > *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.*

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.

Starting Qlik Sense Desktop

## 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

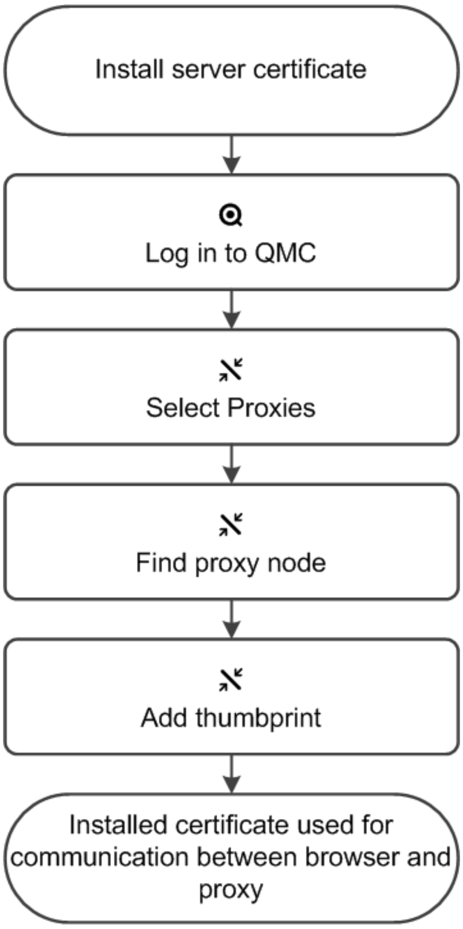
After a standard Qlik Sense installation, the Qlik Sense proxy service (QPS) includes a module that handles the encryption of traffic from the browser to the proxy. The certificate for communication between the web browser and the proxy can be replaced.

*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.*

*When editing a proxy certificate as a user without admin privileges, you need to run the repository in bootstrap mode before the changes take effect.*

*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*.

> *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.*

2. Log into the 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).

*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.*

### 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 Qlik Management Console(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. Select **Certificates** on the QMC start page or from the ▼ menu.
   The **Export** page for **Certificates** is displayed.
2. 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.
3. 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.
4. 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.*

5. Select file format in the **Export file format for certificates** drop-down list.
   The Windows format is .pfx.
6. 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

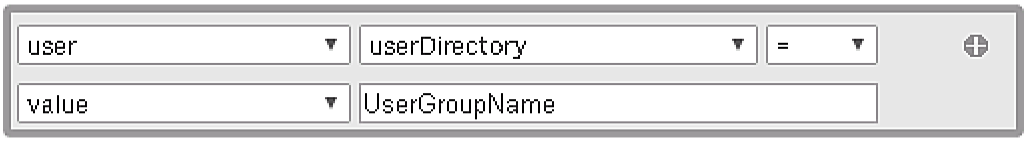
Enable shared content by creating a new security rule in the QMC.

Do the following:

1. In the QMC, open the **Security rules**.
2. Click **Create new** at the bottom of the page.
3. In the **Identification** section, add a name and rule description. You can use the suggestions in the following table.

| Field | Value |
|---|---|
| **Name** | *SharedContentCreate-AllUsersFromUserGroupName* |
| **Description** | *All users from the domain UserGroupName are allowed to create shared content* |

4. In the **Basic** section, type *SharedContent_** as a **Resource filter**.
5. Select the **Create** action and ensure that the **Read** action is cleared.
6. Complete the action rule definition using the values in following image and by replacing *UserGroupName* with the name of your authentication user group.



user ▼ userDirectory ▼ = ▼

value ▼ UserGroupName

7. (Optional) If you want all authenticated users to be allowed to share QlikView content, type *!user.IsAnonymous()* in the **Conditions** box.

8. Click **Apply**.

   The security rule is 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.*

# 4.3 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 master. The master 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. Select **Load balancing rules** on the QMC start page or from the **Start**▼ drop-down menu.
2. 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.
3. Under **Identification**, in the **Create rule from template** drop-down list, select the resource type to create a rule for.

   *In the **Advanced** 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**
4. Under **Identification**, give the rule a name and a description.
5. Click **Disabled** if you do not want to enable the rule at this time.
6. In the **Basic** view, select the type of actions you want to create a rule for.
7. 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 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. |

8. Click **Preview** to view the access rights of your rule in the currently defined audit grid.
9. 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. Select **Load balancing rules** on the QMC start page or from the **Start▼** drop-down menu.
2. Select the rule you want to edit.
3. 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.
4. 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 **Advanced** 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 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. |

| Property name | 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. |

5. Click **Disabled** if you do not want to enable the rule at this time.
6. Click **Preview** to view the access rights of your rule in the currently defined audit grid.
7. 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. Select **Load balancing rules** on the QMC start page or from the **Start**▼ drop-down menu.
2. Select the rules that you want to delete.

   *You can filter a column by using the filtering option:* ⏷

3. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
4. 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.

# 5 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.

## 5.1 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.

See: *Custom properties (page 421)*

### 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 423)*, 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.

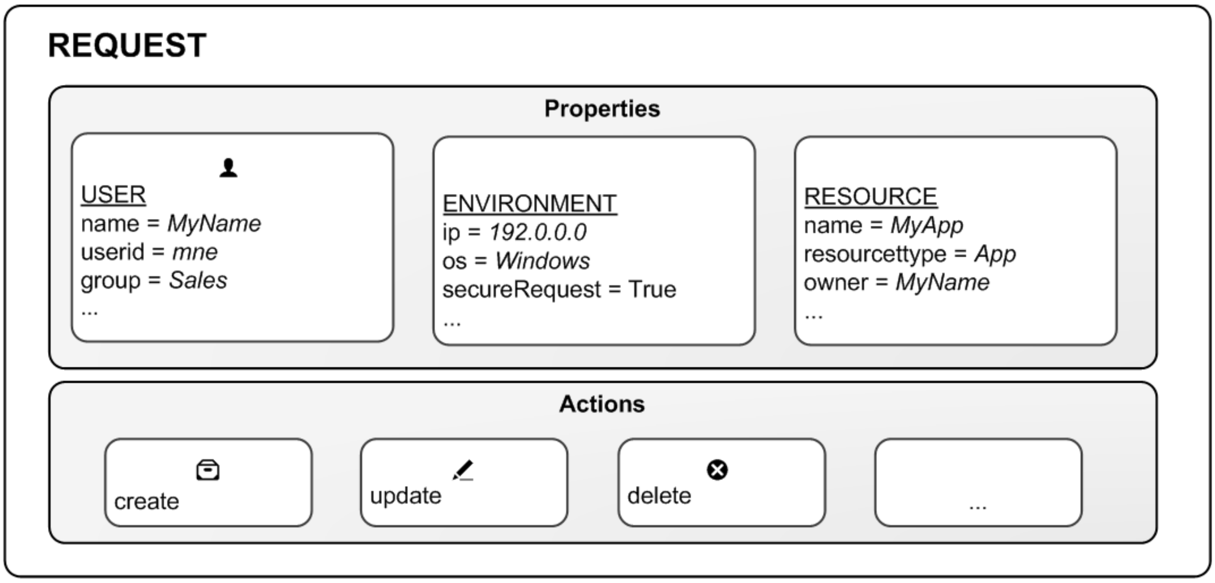
You can see the custom properties in the user condition drop-down list when you create rules. Custom properties have the "@" suffix in the list.

## 5.2 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

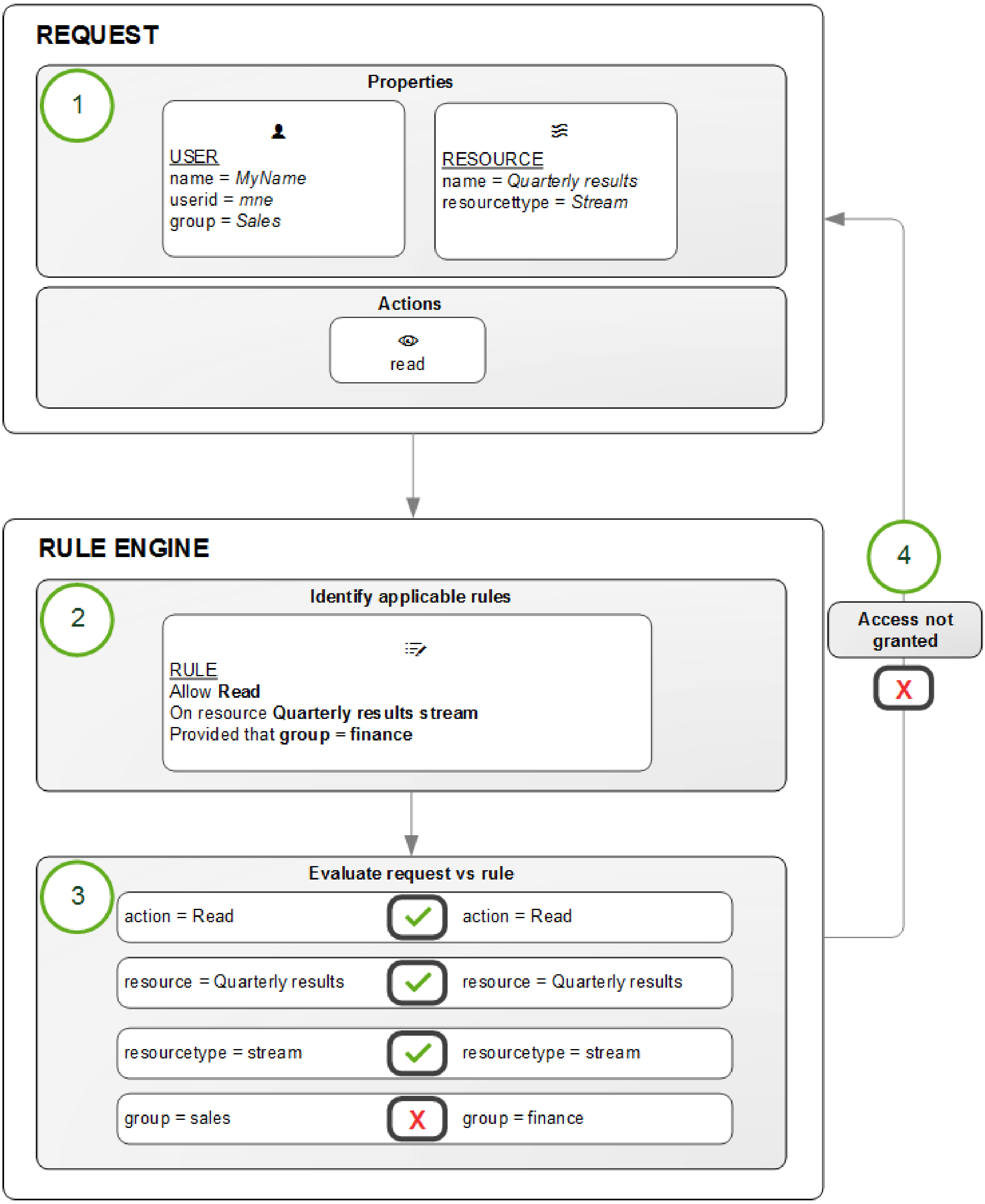
**Example: One property-value pair in conditions:**

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.*

# 5.3 Security rules installed 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. These rules are of two types: Default and Read only. 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, 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

| | |
|---|---|
| **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

| | |
|---|---|
| **Name** | AuditAdminQmcSections |
| **Description** | Audit admin should have read rights to audit related sections |
| **Resource filter** | License_*,TermsAcceptance_*,QmcSection_Tag,QmcSection_Audit |
| **Actions** | Read |
| **Context** | Only in QMC |
| **Type** | Default |
| **Conditions** | ((user.roles="AuditAdmin")) |

## Content library content

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **Name** | ContentAdmin |
| **Description** | Content admin should have rights to manage content related entities |
| **Resource filter** | Stream_*,App*,ReloadTask_*,UserSyncTask_*,SchemaEvent_*,User*,CustomProperty*,Tag_*, DataConnection_*,CompositeEvent_*,Extension_*,ContentLibrary_* |
| **Actions** | Create, Read, Update, Delete, Export, Publish, Change owner |
| **Context** | Only in QMC |
| **Type** | Default |
| **Conditions** | ((user.roles="ContentAdmin")) |

## ContentAdminQmcSections

| | |
|---|---|
| **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_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 |
| **Actions** | Read |
| **Context** | Only in QMC |

| | |
|---|---|
| **Type** | Default |
| **Conditions** | ((user.roles="ContentAdmin")) |

## ContentAdminRulesAccess

| | |
|---|---|
| **Name** | ContentAdminRulesAccess |
| **Description** | Content admin should have rights to manage security rules for streams, data connections, content libraries, and extensions |
| **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}") |

## CreateApp

| | |
|---|---|
| **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

| | |
|---|---|
| **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 |
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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")) |

## DataConnection

| | |
|---|---|
| **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")) |

## Default content library

| | |
|---|---|
| **Name** | Default content library |
| **Description** | Everyone should have read rights to the default content library |
| **Resource filter** | ContentLibrary_<Content library ID> |
| **Actions** | Read |
| **Context** | Both in hub and QMC |
| **Type** | Default |
| **Conditions** | true |

## Default content library

| | |
|---|---|
| **Name** | Default content library |
| **Description** | Everyone should have read rights to the default content library |
| **Resource filter** | ContentLibrary_<Content library ID> |
| **Actions** | Read |
| **Context** | Both in hub and QMC |
| **Type** | Default |
| **Conditions** | true |

## DeleteOdagLinkUsage

| | |
|---|---|
| **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

| | |
|---|---|
| **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_*,UserSyncTask_*,SchemaEvent_*,CompositeEvent_* |
| **Actions** | Create, Read, Update, Delete |
| **Context** | Only in QMC |
| **Type** | Default |
| **Conditions** | ((user.roles="DeploymentAdmin")) |

## DeploymentAdminAppAccess

| | |
|---|---|
| **Name** | DeploymentAdminAppAccess |
| **Description** | Deployment admin should have read and update rights to apps in order to handle sync rules |
| **Resource filter** | App_* |
| **Actions** | Read, Update |
| **Context** | Only in QMC |
| **Type** | Default |
| **Conditions** | ((user.roles="DeploymentAdmin")) |

## DeploymentAdminQmcSections

| | |
|---|---|
| **Name** | DeploymentAdminQmcSections |
| **Description** | Deployment admin should have read rights to deployment related sections |

| | |
|---|---|
| **Resource filter** | License_*,TermsAcceptance_*,ServiceStatus_*,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 |
| **Actions** | Read |
| **Context** | Only in QMC |
| **Type** | Default |
| **Conditions** | ((user.roles="DeploymentAdmin")) |

## DeploymentAdminRulesAccess

| | |
|---|---|
| **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") |

## ExportAppData

| | |
|---|---|
| **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

| | |
|---|---|
| **Name** | Extension |
| **Description** | Everyone should have read rights to extensions |
| **Resource filter** | Extension_* |
| **Actions** | Read |
| **Context** | Both in hub and QMC |
| **Type** | Default |
| **Conditions** | true |

## Extension manage content

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **Name** | File upload connection object |
| **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

| | |
|---|---|
| **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") |

## HubSections

| | |
|---|---|
| **Name** | HubSections |
| **Description** | Everyone should have read rights to all hub sections |
| **Resource filter** | HubSection_* |
| **Actions** | Read |
| **Context** | Both in hub and QMC |
| **Type** | Default |
| **Conditions** | true |

## Installed static content

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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 |
| **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

| | |
|---|---|
| **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 |

## OwnerDistribute

| | |
|---|---|
| **Name** | OwnerDistribute |
| **Description** | The owner of apps and streams should be able to distribute |
| **Resource filter** | App_*, Stream_* |
| **Actions** | Distribute |
| **Context** | Both in hub and QMC |
| **Type** | Default |
| **Conditions** | resource.IsOwned() and resource.owner = user |

## OwnerPublishAppObject

| | |
|---|---|
| **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" |

## OwnerPublishDuplicate

| | |
|---|---|
| **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 |
| **Context** | Both in hub and QMC |
| **Type** | Default |
| **Conditions** | resource.IsOwned() and resource.owner = user |

## OwnerRead

| | |
|---|---|
| **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 |
| **Context** | Both in hub and QMC |
| **Type** | Read only |
| **Conditions** | resource.IsOwned() and resource.owner = user |

## OwnerUpdateApp

| | |
|---|---|
| **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 |

## ReadAnalyticConnectionEveryone

| | |
|---|---|
| **Name** | ReadAppContentFiles |
| **Description** | Non-anonymous users can read an analytic connection |
| **Resource filter** | AnalyticConnection_* |
| **Actions** | Read |
| **Context** | Only in hub |
| **Type** | Read only |
| **Conditions** | !user.IsAnonymous() |

## ReadAppContentFiles

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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") |

## ReadFileReference

| | |
|---|---|
| **Name** | ReadFileReference |
| **Description** | Everyone, except anonymous users, should have read rights to file references |
| **Resource filter** | FileReference_* |
| **Actions** | Read |
| **Context** | Both in hub and QMC |
| **Type** | Read only |
| **Conditions** | !user.IsAnonymous() |

## ReadOdagLinks

| | |
|---|---|
| **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

| | |
|---|---|
| **Name** | ReadOdagLinkUsage |
| **Description** | Non-anonymous users with read access to the selection app can read its OdagLinkUsages |
| **Resource filter** | OdagLinkUsage_* |
| **Actions** | Read |
| **Context** | Only in hub |
| **Type** | Default |
| **Conditions** | !user.IsAnonymous() |

## RootAdmin

| | |
|---|---|
| **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

| | |
|---|---|
| **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_* |
| **Actions** | Create, Read, Update, Delete, Export, Publish, Change owner |
| **Context** | Only in QMC |
| **Type** | Default |
| **Conditions** | ((user.roles="SecurityAdmin")) |

## SecurityAdminQmcSections

| | |
|---|---|
| **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_SystemRule,QmcSection_DataConnection,QmcSection_Tag, QmcSection_Templates,QmcSection_Audit,QmcSection_ProxyService,QmcSection_VirtualProxyConfig, QmcSection_User, QmcSection_CustomPropertyDefinition,QmcSection_Certificates, QmcSection_Certificates.Export,QmcSection_ContentLibrary |
| **Actions** | Read |
| **Context** | Only in QMC |
| **Type** | Default |
| **Conditions** | ((user.roles="SecurityAdmin")) |

## SecurityAdminServerNodeConfiguration

| | |
|---|---|
| **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

| | |
|---|---|
| **Name** | ServiceAccount |
| **Description** | Service accounts should have rights to perform all actions |
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **Name** | StreamMonitoringAppsRead |
| **Description** | Default administrators should have read rights to the default stream called Monitoring apps |
| **Resource filter** | Stream_<stream_ID> |
| **Actions** | Read |
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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

| | |
|---|---|
| **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 |
| **Context** | Both in hub and QMC |
| **Type** | Read only |
| **Conditions** | resource.App.HasPrivilege("update") |

# 5.4 The security rule editor

You can create new security rules in the security rule editor.

Do the following:

1. Select **Security rules** on the QMC start page or from the **Start**▼ drop-down menu.
2. 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 **Advanced** 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.

See: *Naming resources in the Resource filter (page 453)*

However, you cannot select more than one resource type from the basic view. If you want to add more resource types to the resource filter, or the resource conditions, you must edit the **Resource filter** and **Conditions** fields in the **Advanced** section.

### 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. Using the **Advanced** section also enables you to 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.

# 5.5 Creating security rules

Do the following:

1. Select **Security rules** on the QMC start page or from the **Start**▼ drop-down menu.
2. 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.
3. Under **Identification**, in the **Create rule from template** drop-down list, select the resource type to create a rule for.

   *In the **Advanced** 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** | **Security rule will be applied to** |
   |---|---|
   | Unspecified | All resource types |
   | App access | Apps |
   | App object access | Objects<br>The Objects' objectTypes, for example: sheet, story, bookmark, measure, or dimension. |
   | Content library access | Content libraries |
   | Data connection access | Data connections |
   | Extension access | Extensions |
   | 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.*
4. Under **Identification**, give the rule a name and a description.

5. Click **Disabled** if you do not want to enable the rule at this time.
6. 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.
7. 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 463)*.
8. Define the resource filters, see: *Defining resource filters (page 453)*.
9. Select the applicable **Actions** to assign access rights to the user for the resource.

   **Action properties**

   | 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. |
   | Publish | Publish a resource to a stream. |
   | Change owner | Change the owner of a resource. |
   | Change role | Change user role. |

| Action | Description |
|---|---|
| Export data | Export data from an object. This includes the following actions:<br>"Export as image" for visualizations.<br>"Export as PDF" for visualizations.<br>"Export data" for visualizations.<br>"Export sheet" in the menu.<br>"Export story" in storytelling.<br>*You cannot grant access to only a subset of these actions.*<br>*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 installed in Qlik Sense (page 425).* |
| Access offline | Access apps offline. |

10. 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.*

| 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. |

| Property | Description |
|---|---|
| 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.<br>**Example 1:**<br>Define browser and version:<br>Firefox 22.0<br>Chrome 33.0.1750.154<br>*If the browser information contains a slash (/), replace it with a space.*<br>**Example 2:**<br>Use the wildcard (*) to include all versions of the browser:<br>environment.browser = Chrome* |
| environment.context | Security rule will be applied only to the Qlik Sense environment that the call originates from.<br>Available preset values: ManagementAccess or AppAccess. |
| environment.device | Security rule will be applied to the type of device.<br>Available preset values: iPhone, iPad, or Default. |
| environment.ip | Security rule will be applied to an IP number.<br>See: *Security rules example: Access to stream by IP address (page 491)* |
| environment.os | Security rule will be applied to the type of operating system.<br>Available preset values: Windows, Linux, Mac OS X or Unknown. |
| environment.secureRequest | Security rule will be applied to the type of request.<br>Available preset values: SSL True or False. |

11. In the **Advanced** view, you can select where the rule should be applied from the **Context** drop-down list.

**Context properties**

| Property | Description |
|---|---|
| **Context** | Specifies where the rule is applied: **Both in hub and QMC**, **Only in hub**, or **Only in QMC**. |

12. Click **Preview** to view the access rights that your rule will create and the users and resources that they apply to.
13. Click **Apply** to create and save the rule.
    **Successfully added** is displayed at the bottom of the page.

# 5.6 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:

| Example | Result |
|---|---|
| Select **App** from the **Resource** drop-down list. | The following texts appear in the Advanced view:<br>**Resource** `App*`<br>**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:

| 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. |

# 5.7 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

| 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

| Task | App | Stream | App.Object |
|---|---|---|---|
| **Duplicate** | Read and Create | | 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 **Create** a new 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

# 5.8 Available resource filters

The following table lists the resource objects and the resource filters that can be used to target them.

## App related resources

| **Resource filter** | **Filter will target** |
|---|---|
| App | The application |
| App.Content | The content stored in the app-specific content library |
| App.Object | All App.Object resources, such as sheets, stories, script, dimensions, measures, master objects, snapshots, and bookmarks |
| 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 |
| Extension | The extensions installed in Qlik Sense |
| Widgets | The widgets installed in Qlik Sense |
| WebExtensionLibrary | The library of web extensions |

## Task resources

| **Resource filter** | **Filter will target** |
|---|---|
| ReloadTask | Tasks that perform reload on apps |
| UserSyncTask | Tasks that sync users from an external user directory |
| CompositeEvent | Task triggers in the scheduler |
| SchemaEvent | Details for when a scheduled task will run |

## ContentLibrary related resources

| **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 |

| | |
|---|---|
| StaticContentReference | Links to files in a content library |
| TempContent | Content library for temporary content, such as files from exports |
| SharedContent | Links to QlikView documents, Qlik NPrinting generated reports |

## Hub section resources

The following filter can be used to disable user access to the hub.

| Resource filter | Filter will target |
|---|---|
| HubSection_Home | Grants access to open the hub and view the resources you have access to. By default, on.<br>ⓘ *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.* |

## 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.

| Resource filter | Filter will target |
|---|---|
| QmcSection_App | The QmcSectionApp resource |
| QmcSection_App.Object | The QmcSectionApp.Object resource |
| QmcSection_App.Sheet | The QmcSection_App.Sheet resource |
| QmcSection_App.Story | The QmcSection_App.Story resource |
| QmcSection_Audit | The QmcSectionAudit resource |
| QmcSection_Certificates | The QmcSectionCertificate resource |
| QmcSection_Certificates.Export | The QmcSectionCertificateExport resource |
| QmcSection_CompositeEvent | The QmcSectionCompositeEvent resource |
| QmcSection_ContentLibrary | The QmcSectionContentLibrary resource |

| | |
|---|---|
| QmcSection_CustomPropertyDefinition | The QmcSectionCustomPropertyDefinition resource |
| QmcSection_DataConnection | The QmcSectionDataConnection resource |
| QmcSection_EngineService | The QmcSectionEngineService resource |
| QmcSection_Event | The QmcSectionEvent resource |
| QmcSection_Extension | The QmcSectionExtension resource |
| QmcSection_License | The QmcSectionLicense resource |
| QmcSection_Licenses | The QmcSectionLicenses resource |
| QmcSection_License.LoginAccessType | The QmcSection_License.LoginAccessType resource |
| QmcSection_License.UserAccessType | The QmcSection_License.UserAccessType resource |
| QmcSection_License.UserAccessRule | The QmcSection_License.UserAccessRule resource |
| QmcSection_License.ProfessionalAccessType | The QmcSection_License.ProfessionalAccessType resource |
| QmcSection_License.ProfessionalAccessRule | The QmcSection_License.ProfessionalAccessRule resource |
| QmcSection_License.AnalyzerAccessType | The QmcSection_License.AnalyzerAccessType resource |
| QmcSection_License.AnalyzerAccessRule | The QmcSection_License.AnalyzerAccessRule resource |
| QmcSection_License.ApplicationAccessType | The QmcSection_License.ApplicationAccessType resource |
| QmcSection_ProxyService | The QmcSectionProxyService resource |
| QmcSection_ReloadTask | The QmcSectionReloadTask resource |
| QmcSection_RepositoryService | The QmcSectionRepositoryService resource |
| QmcSection_SchedulerService | The QmcSectionSchedulerService resource |
| QmcSection_SchemaEvent | The QmcSectionSchemaEvent resource |

| | |
|---|---|
| QmcSection_ServerNodeConfiguration | The QmcSectionServerNodeConfiguration resource |
| QmcSection_ServiceCluster | The QmcSection_ServiceCluster resource |
| QmcSection_Stream | The QmcSectionStream resource |
| QmcSection_SyncRule | The QmcSectionSyncRule resource |
| QmcSection_SystemRule | The QmcSectionSystemRule resource |
| QmcSection_Tag | The QmcSectionTag resource |
| QmcSection_Task | The QmcSectionTask resource |
| QmcSection_Token | The QmcSectionToken resource |
| QmcSection_User | The QmcSectionUser resource |
| QmcSection_UserDirectory | The QmcSectionUserDirectory resource |
| QmcSection_UserSyncTask | The QmcSectionUserSyncTask resource |
| QmcSection_VirtualProxyConfig | The QmcSectionVirtualProxyConfig resource |
| QmcSection_PrintingService | The QmcSectionPrintingService resource |

## License related resources

| **Resource filter** | **Filter will target** |
|---|---|
| License | The actual license entity (both Qlik Sense and Qlik DataMarket). |
| LicenseLoginAccessType | Login access type. CRUD for allocating tokens for login (time restricted) access and setting up the associated rule. |
| LicenseUserAccessType | User access type. CRUD for manually allocating tokens for user (named) access. |
| LicenseUserProfessionalType | Professional access type. CRUD for manually allocating access for a named user. |
| LicenseUserAnalyzerType | Analyzer access type. CRUD for manually allocating tokens for user (named) access. |

| | |
|---|---|
| LicenseLoginAccessUsage | Type to keep track of login access type usage. Should not be used in resource filters. |
| LicenseUserAccessUsage | Type to keep track of user access type usage. Should not be used in resource filters. |
| LicenseUserProfessionalUsage | Type to keep track of professional access type usage. Should not be used in resource filters. |
| LicenseUserAnalyzerUsage | Type to keep track of analyzer access type usage. Should not be used in resource filters. |
| LicenseUserAccessGroup | Resource for rules used for automatically assigning user access types. |
| TermsAcceptance | Resource for accessing the Qlik DataMarket 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.

| **Resource filter** | **Filter will target** |
|---|---|
| ServerNodeConfiguration | The ServerNodeConfiguration resource |
| ServiceStatus | The ServiceStatus resource |
| ServiceCluster | The ServiceCluster resource |
| EngineService | The EngineService resource |
| ProxyService | The ProxyService resource |
| SchedulerService | The SchedulerService resource |
| RepositoryService | The RepositoryService resource |
| PrintingService | The PrintingService resource |
| VirtualProxyConfig | The VirtualProxyConfig resource |
| Certificates | The Certificates resource |

## Other resources

These filters refer to individual entries in the associated sections of the QMC.

| Resource filter | Filter will target |
|---|---|
| CustomPropertyDefinition | The CustomPropertyDefinition resource |
| DataConnection | The DataConnection resource |
| Stream | The Stream resource |
| SystemRule | The SystemRule resource |
| Tag | The Tag resource |
| User | The User resource |
| UserDirectory | The UserDirectory resource |

## 5.9 Available resource conditions

The following tables list the available resource conditions.

### General

| Property | Description | Example |
|---|---|---|
| resource.@<customproperty> | Custom property associated with the resource. In the examples, @Department is the custom property name. | `resource.@Department = Finance.`<br>`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

| Property | Description | Example |
|---|---|---|
| user.email<br>owner.email | Email of the user.<br>Email of the owner. | `user.email="user@domain.com"`<br>`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. | See: *Security rules example: Access to stream by IP address (page 491)* |
| 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<br>owner.group | Group that the user belongs to.<br>Group that the owner belongs to. | `user.group=resource.app.stream.@AdminGroup`<br>`owner.group=@Developers` |
| user.userdirectory<br>owner.userdirectory | User directory that the user belongs to.<br>User directory that the owner belongs to. | `user.userdirectory="Employees"`<br>`owner.userdirectory="Employees"` |
| user.userId<br>owner.userId | ID of the user.<br>ID of the owner. | `user.userId="<userID>"`<br>`owner.userId="<ownerID>"` |
| user.roles<br>owner.roles | Roles of the user.<br>Roles of the owner. | `user.roles="AuditAdmin"`<br>`owner.roles="SystemAdmin"` |

## Resource app

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

## Resource app.object

| **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:<br>• app_appscript<br>• dimension<br>• embeddedsnapshot<br>• genericvariableentry<br>• hiddenbookmark<br>• masterobject<br>• measure<br>• sheet<br>• snapshot<br>• story<br>• bookmark | `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

| 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

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

## Resource SystemRule

| Property | Description | Example |
|---|---|---|
| Category | System rule category.<br>Possible values:<br>- Security<br>- License<br>- 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.<br>Possible values:<br>- BothQlikSenseAndQMC<br>- QlikSenseOnly<br>- QMCOnly | `resource.rulecontext="BothQlikSenseAndQMC"` |
| Type | Type of rule.<br>Possible values:<br>- Default<br>- Read only<br>- Custom | `resource.type!="custom"` |

## Resource ContentLibrary

| Property | Description | Example |
|---|---|---|
| Type | Possible values:<br>- media | `resource.type="media"` |

## Resource ServerNodeConfiguration

| 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

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

## Resource UserSyncTask

| 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

| 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.*

# 5.10 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:**

| 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:**

| 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:**

| Example | Result |
|---|---|
| `resource.name like "mya*"` | Evaluates all resources with names beginning with "*mya*" to True, irrespective of case.<br>*Entering an asterisk at the end of the condition in the Basic view automatically translates to "like" in the condition in the Advanced view.* |

## 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:**

| 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:**

| 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:**

| 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. |
| 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:**

| 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:**

| 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:**

| 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:**

| Property | Description |
|---|---|
| action | MANDATORY. The action that you want to evaluate access right for. |

Examples and results:

| Example | Result |
|---|---|
| **Resource filter:** `*`<br>**Conditions:** `resource.resourcetype = "App" and resource.Stream.HasPrivilege("read")`<br>**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:

| Example | Result |
|---|---|
| **Resource filter:** `Stream_*`<br>**Conditions:** `user.IsAnonymous()`<br>**Action:** `read` | Anonymous users are allowed to read streams. |
| **Resource filter:** `Stream_*`<br>**Conditions:** `!user.IsAnonymous()`<br>**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:

| Example | Result |
|---|---|
| **Resource filter:** `App_*`<br>**Conditions:** `resource.stream.Empty()`<br>**Action:** `update` | This rule lets the user update an app, provided that the app is not connected (published) to a stream. |
| **Resource filter:** `App.Sheet_*`<br>**Conditions:** `resource.app.stream.Empty()`<br>**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:

| Example | Result |
|---|---|
| **Resource filter:** `*`<br>**Conditions:** `resource.IsOwned() and resource.owner = user`<br>**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.<br>*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.* |

# 5.11 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.

> *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. Select **Security rules** on the QMC start page or from the **Start**▼ drop-down menu.
2. Select the rule you want to edit.
3. 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 **Advanced** 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.*

4. Click **Preview** to view the access rights of your rule in the currently defined audit grid.
5. 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.*

## 5.12 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. Select **Security rules** on the QMC start page or from the **Start**▼ drop-down menu.
2. Select the rules that you want to delete.
3. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
4. Click **OK**.

## 5.13 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.

**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.

| | **Rule 1** | **Rule 2** |
|---|---|---|
| Allow users to | Read | Read |
| On resource | Quarterly results stream | Quarterly results stream |
| Provided that | group=Finance | group=Management |

| | Rule 1 | Rule 2 |
|---|---|---|
| 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.

| | Rule 1 | Rule 2 | Rule 3 |
|---|---|---|---|
| Allow users to | Read | Read | Update |
| 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.

| | 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 |

| | Rule 2 | Rule 3 | Stream rule |
|---|---|---|---|
| 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.

See: *Audit (page 67)*

You can also preview the effects of a rule.

See: *Editing security rules (page 474)*

**Example 1:**

In the example *One property-value pair in conditions: (page 423)* 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 1 | Rule 2 |
|---|---|---|
| Allow users to | Read | Read |
| On resource | Quarterly reports stream | Quarterly reports stream |

| | Rule 1 | Rule 2 |
|---|---|---|
| Provided that | group=Finance | group=Management |
| Evaluates to | FALSE | TRUE |
| Resulting access for Sales director | 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 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 | | |

# 5.14 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 five 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 for the user role CustomAdmin.

| Field | Code | Comments |
|---|---|---|
| Resource filter | `Stream_*, App_*, App.Object_*, ReloadTask_*` | Filters on resource types `Stream`, `App`, `AppObjects`, and `ReloadTasks`.<br>*Alternatively, you could write `App*` instead of `App_*, App.Object_*`, because the wildcard (*), without the underscore (_), targets all resource types beginning with `App`.* |
| 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*.

| **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 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 483)*
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"

| 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"

| 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`<br>`resource.@Department=user.@Department and`<br>`(resource.resourcetype="App" or (resource.resourcetype="ReloadTask"`<br>`or resource.resourcetype="App.Object") or`<br>`resource.resourcetype="SchemaEvent" or`<br>`resource.resourcetype="CompositeEvent" or`<br>`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. |
| 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 | 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**.
   See: *Security rule code for "Create app" (page 486)*.
   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"

| Field | Code | Comments |
|---|---|---|
| **Resource filter** | `App_*,FileReference_*` | Specifically filters on resource type App. |
| **Conditions** | `!user.IsAnonymous() and (user.@usertype= "Developer")` | `!user.IsAnonymous()`<br>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.<br>`(user.@usertype="Developer")`<br>The condition is met by all users that have the custom property `@usertype` set to `Developer`.<br>*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)

| 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")`<br>This condition uses a security rules function **HasPrivilege()** that can be used to evaluate access rights for resource types.<br>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"

| Field | Code | Comments |
|---|---|---|
| **Resource filter** | `DataConnection_*` | Specifically filters on resource type DataConnection. |
| **Conditions** | `resource.resourcetype = "DataConnection" and (user.@usertype="Developer")` | `resource.resourcetype = "DataConnection"`<br>The rule will apply to resources of the type DataConnection.<br>`user.@usertype="Developer"`<br>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 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 488)*.

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"

| **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"

| 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.

| **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 491)*.
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 491)*.

4. Set the actions that the rule should provide.
   In the **Basic** section, select **Actions** as per Security rule code (page 491).
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.

| **Field** | **Code** | **Comments** |
|---|---|---|
| Resource filter | `Stream_<GUID>` | Specifically filters on the stream with a specific GUID. |
| Conditions | `resource.resourcetype="Stream" and (user.environment.<Attribute1>="<Value1 a>")` | `resource.resourcetype="Stream"`<br>The rule applies to streams.<br>`( user.environment.<Attribute1>="<Value1 a>")`<br>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 492)*.
    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 492)*.
    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 492)*.
    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.

| **Field** | **Code** | **Comments** |
|---|---|---|
| Resource filter | `Stream_<GUID>` | Filters on a specific stream. |

| Field | Code | Comments |
|---|---|---|
| Conditions | `(user.environment.ip="<Your_IP_address>")`<br>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.<br>**Example 1:**<br>*IPv4 address: 10.88.0.5 => ::ffff:10.88.0.5 (IPv6)*<br>In this case the rule condition can be written in the following ways:<br>• user.environment.ip like "*10.88.0*"<br>• user.environment.ip like "::ffff:10.88*"<br>• user.environment.ip = "::ffff:10.88.0.5"<br>**Example 2:**<br>*IPv6 address: 2001:0db8:85a3:0000:0000:8a2e:0370:7334*<br>In this case the rule condition can be written in the following ways:<br>• user.environment.ip like "*0db8:85a3:0000:0000:8a2e*"<br>• user.environment.ip like "2001:0db8:85a3:0000:0000*"<br>• user.environment.ip = "2001:0db8:85a3:0000:0000:8a2e:0370:7334"<br>*The asterisks (*) in the examples indicate additional characters.* | `(user.environment.ip="<Your_IP_address>")`<br>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 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 494)*.
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 494)*.
4. Set the actions that the rule should provide.
   In the **Basic** section, select **Actions** as per Security rule code (page 494).
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.

| **Field** | **Code** | **Comments** |
|---|---|---|
| Resource filter | `App_*` | Specifically filters on the resource type App. |
| Conditions | `resource.resourcetype="App_*" and (user.environment.<Attribute1>="<Value1 a>")` | `resource.resourcetype="App_*"`<br>The rule applies to apps.<br>`( user.environment.<Attribute1>="<Value1 a>")`<br>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

| 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)

| 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)<br>(No role = Read access) | Proj1_Aud1 (projX_aud1) | Dashboard 1, Dashboard 2, Dashboard 3 |
| Audience 2 (role_ext)<br>(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:

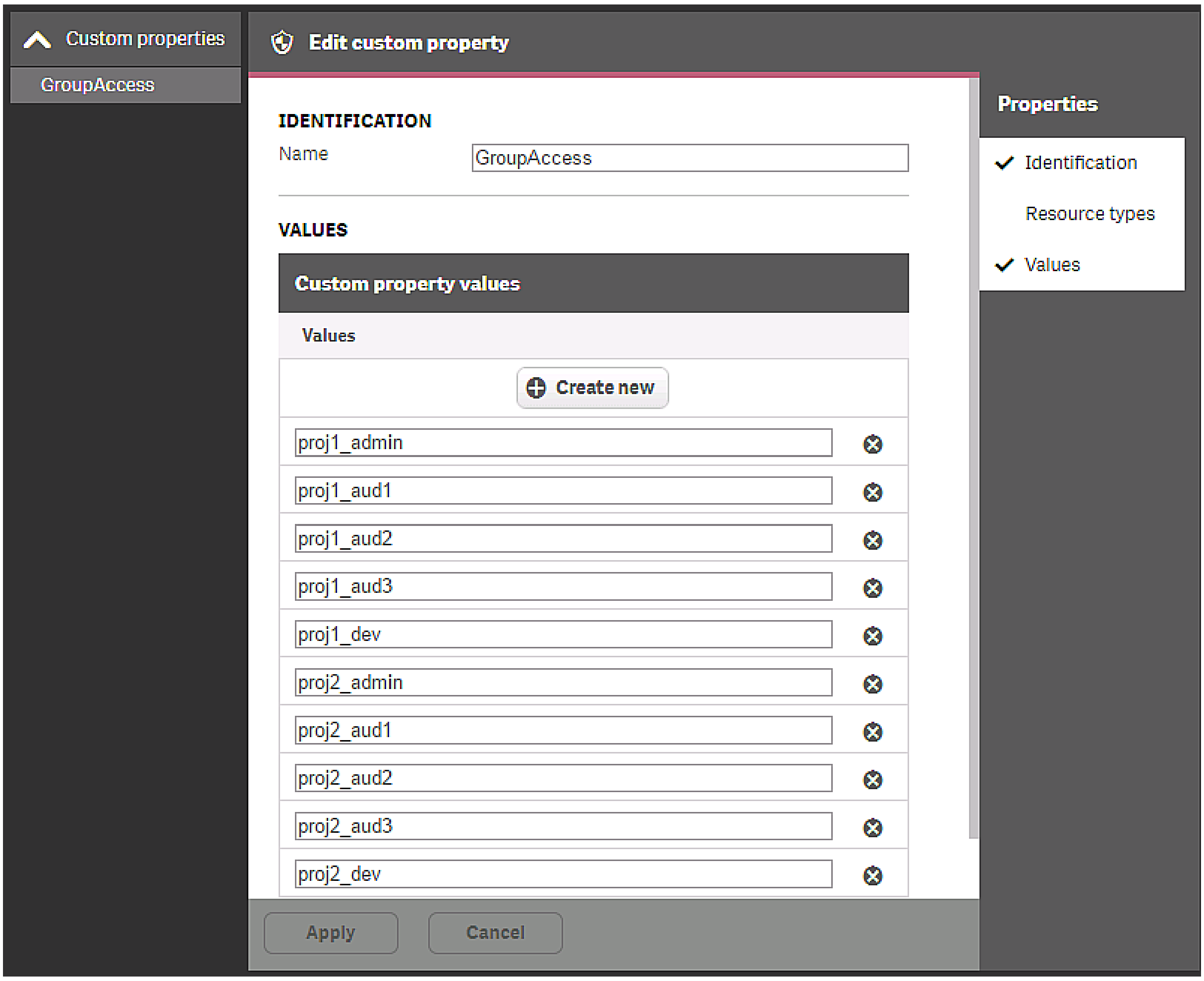
- The number of rules needed to describe the security policy is reduced.
- Rules change slowly. The system is configured through attributes, and it is only when security needs to be changed that rule changes are required.
- User management and provisioning of permissions are maintained in the user directory.

**What rules need to be created?**

One rule is needed for resource access.

| **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.



IDENTIFICATION

Name: GroupAccess

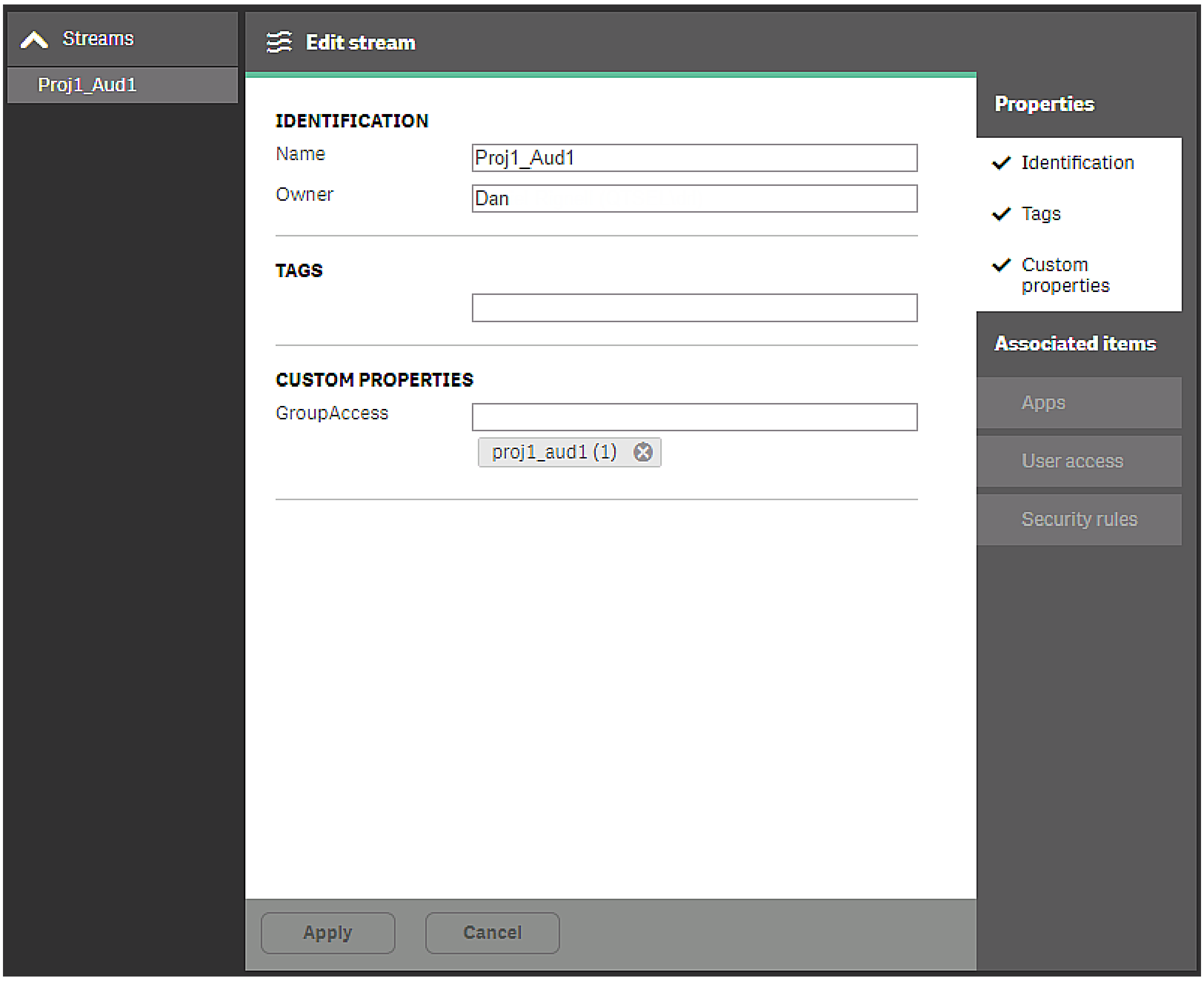
VALUES

Custom property values

Values

proj1_admin
proj1_aud1
proj1_aud2
proj1_aud3
proj1_dev
proj2_admin
proj2_aud1
proj2_aud2
proj2_aud3
proj2_dev

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.



IDENTIFICATION

Name: Proj1_Aud1

Owner: Dan

TAGS

CUSTOM PROPERTIES

GroupAccess: proj1_aud1 (1)

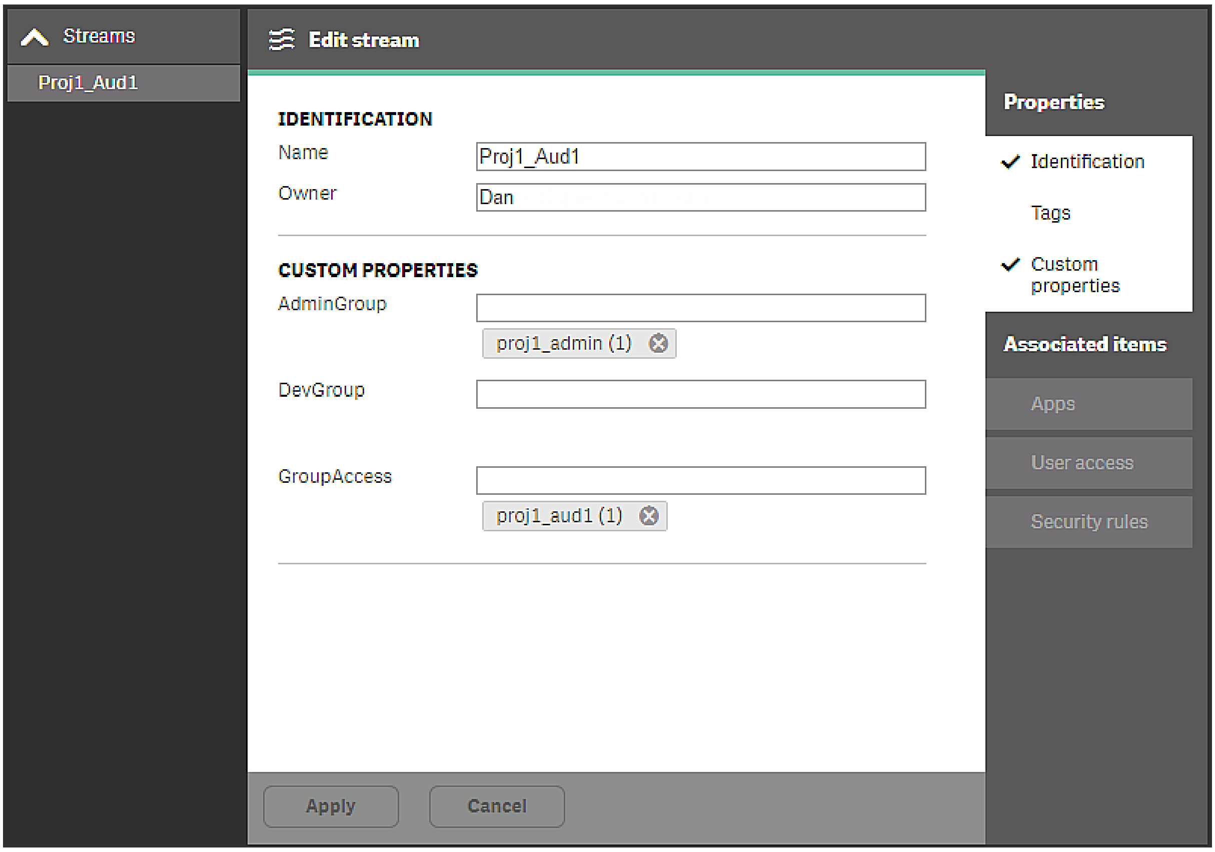
In this example, the proj1_aud1 group has been added in their user directory access to the Proj1_Aud1 stream. If additional groups need access, they can be added to the custom property.

The next rule to be created defines who should be allowed to administer the streams.

| | |
|---|---|
| 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.



IDENTIFICATION

Name: Proj1_Aud1

Owner: Dan

CUSTOM PROPERTIES

AdminGroup: proj1_admin (1)

DevGroup:

GroupAccess: proj1_aud1 (1)

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.

| | |
|---|---|
| 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.

| | |
|---|---|
| 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.

| | |
|---|---|
| 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.

| | |
|---|---|
| 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.*

# 6 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. Click **Audit** on the QMC start page.
2. On the **Audit** page, select **Stream** from the target resource list.
3. To the right of the target resource list, click 🔍 and select the stream `Quarterly reports`.
4. 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.
5. 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
6. 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

# 6.1 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 🔍 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 🔍 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.

## 6.2 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.

| **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.*

# 7 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.

## 7.1 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.

See: *Changing to a signed server proxy certificate (page 409)*

#### 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.

See: *Changing to a signed server proxy certificate (page 409)*

#### 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 Internet Explorer, open **Tools** > **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**.
9. Refresh the browser window.

## 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.

https://support.microsoft.com/en-us/kb/896861

## The shortcuts do not load the QMC

When using Microsoft Windows Server 2008 R2 and Windows 8.1, the shortcuts do not load the QMC when using Internet Explorer 10 or Internet Explorer 11.

### Possible cause

The Internet Explorer security settings are blocking the shortcuts.

### Proposed action

Add *https://<machinename>/* to the local intranet zone in the Internet Explorer settings: *Internet options/Security tab/Local intranet:Sites/Advanced*.

## **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 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>)"

   The path to the QRS security log file is as follows:
   *%ProgramData%\Qlik\Sense\Log\Repository\Trace\<MachineName>_Security_Repository.txt*

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.

See: Plan and deploy Qlik Sense

## 7.2 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: **403 Forbidden**

### Possible cause

- There are too many root certificates on the computer (> ~300), and as a consequence, the Qlik Senseservices 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**

### 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 white 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 white 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 white listed by adding company.com to the white list. This will white 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.

## A task is not executed

**Possible cause**

The task status is not **Success**.

**Proposed action**

On the tasks overview page in the QMC, click ℹ 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 slave-nodes found to execute Task**.

### Possible cause

The Central scheduler is set to **Master** only.

### Proposed action

Re-trigger the task execution.

On the **Edit scheduler** page, under **Advanced**, change **Type** to **Master and slave**.

# 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.

See: *Synchronizing with user directories (page 244)*

## 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.
- Edit the extension so that it is not a duplicate.
  See: *Extension names (page 209)*

# I cannot migrate an app

I cannot migrate an app despite several attempts.

### Possible cause

The app is corrupted.

### Proposed action

Check the app migration log files for information that could explain the failure. The log files are available at this location: *%ProgramData%\Qlik\Sense\Log*\.

## 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.

> *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.*

## An imported file is recreated after deleting it from the local file system

I am using Internet Explorer and after importing an app or an extension in the QMC and removing it from the file system, the file is recreated but cannot be opened, moved, or permanently deleted.

**Possible cause**

The file did not close properly after being imported.

**Proposed action**

Close Internet Explorer and open the QMC again. The locked file should no longer be visible.

## 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>

# 7.3 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**

You are using Windows Internet Explorer.

**Proposed action**

Add the QMC site as a trusted site in Windows Internet Explorer.

Do the following:

1. Open the Windows Internet Explorer **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**.
7. Refresh the browser window.

The icons are correctly displayed.

## Error message: **Untrustworthy Proxy SSL-connection/-certificate**

The browser displays **the Proxy SSL-connection/-certificate is untrustworthy!**, and I am asked if I want 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.

See: *Changing a proxy certificate (page 407)*

## Error message: **404 Not found**

### Possible cause

The URL refers to a non-existent resource.

### Proposed action

Modify the URL.

# 7.4 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.

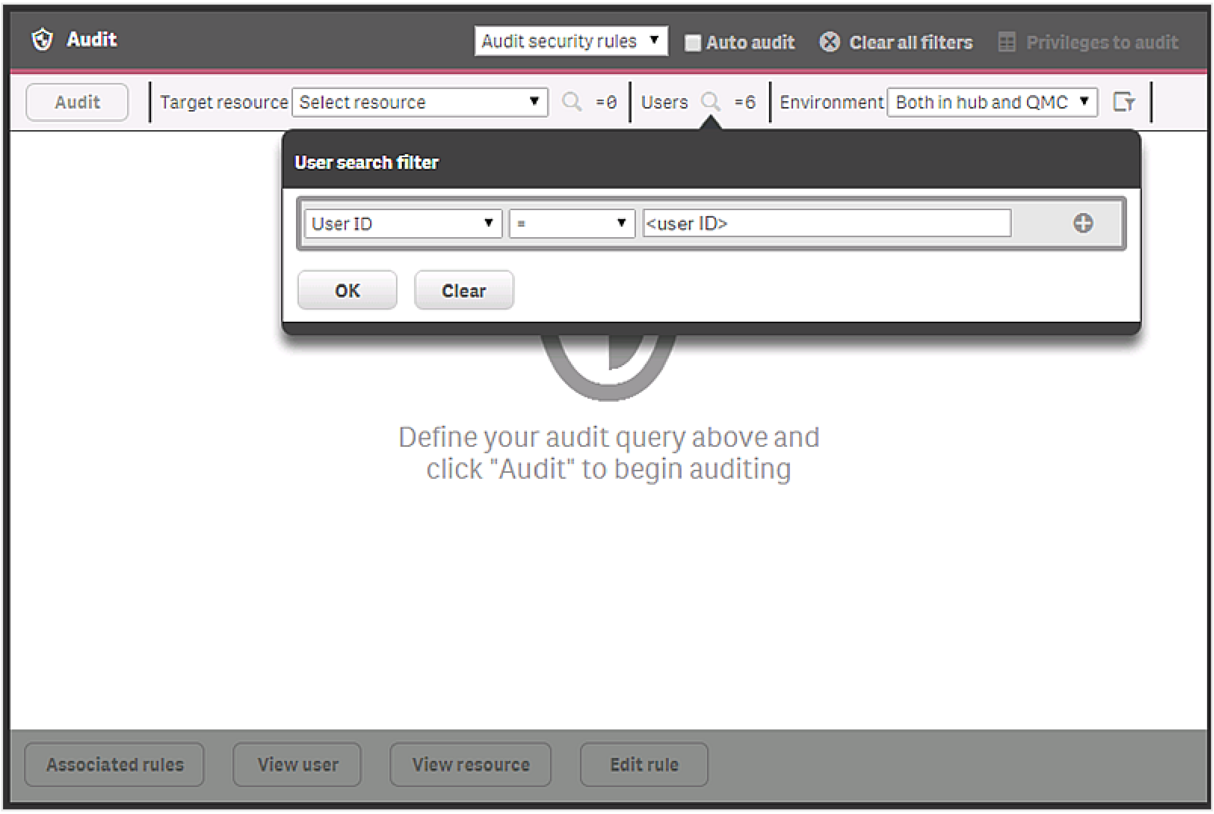
## I suspect that a user can access a stream that should not be accessible

### 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.



# 7.5 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.