Managing a Qlik Sense Site

Qlik Sense®
2.0.10

Contents

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 Installation Guide 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:

- Planning Qlik Sense deployments: Describes Qlik Sense Server and provides reference information on the architecture, security, logging, and licensing.
- Installation Guide: 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 Support services

Contact Qlik for product support, additional training, or consultation concerning application development. Consult the Qlik website for current information on how to get in touch with the support services:

www.qlik.com

Global headquarters:

Qlik Technologies, Inc.
150 N. Radnor Chester Road
Suite E220
Radnor, PA 19087
USA

Phone: +1 (888) 828-9768

Fax: +1 (610) 975-5987

For other locations, visit the Qlik website (see above).

1.5 Managing a Qlik Sense site

The Qlik Management Console (QMC) is a web-based application for configuring and administrating your Qlik Sense site. The QMC always connects to the central Qlik Sense node where all system data is stored and with which all local nodes synchronize. Even if you have a multi-node, geographically distributed Qlik Sense installation, the QMC enables you to perform the following from one location:

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

In a multi-node installation you manage the whole Qlik Sense site from the QMC 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 an app from the Qlik Sense hub, if you have the appropriate access rights. Apps are published to streams from the QMC, which is a part of Qlik Sense. To publish an app that is created 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. 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, and audit, the security rules or sync 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.

Examples of applications for custom properties:

- **Grouping nodes by geography**
  Create a custom property called *Countries* and set the values to names of countries. Apply the custom property to your nodes and you can then create and deploy synchronization rules to countries instead of individual nodes.
- **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 an app from the Qlik Sense hub, if you have the appropriate access rights. Apps are published to streams from the QMC, which is a part of Qlik Sense. To publish an app that is created 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.

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.

Tokens and access types

The License Enabling File (LEF) determines the number of tokens that you can allocate to different access types. An access type allows the users to access streams and apps within a Qlik Sense site. You can adjust the token usage according to the usage need over time. 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.

Users

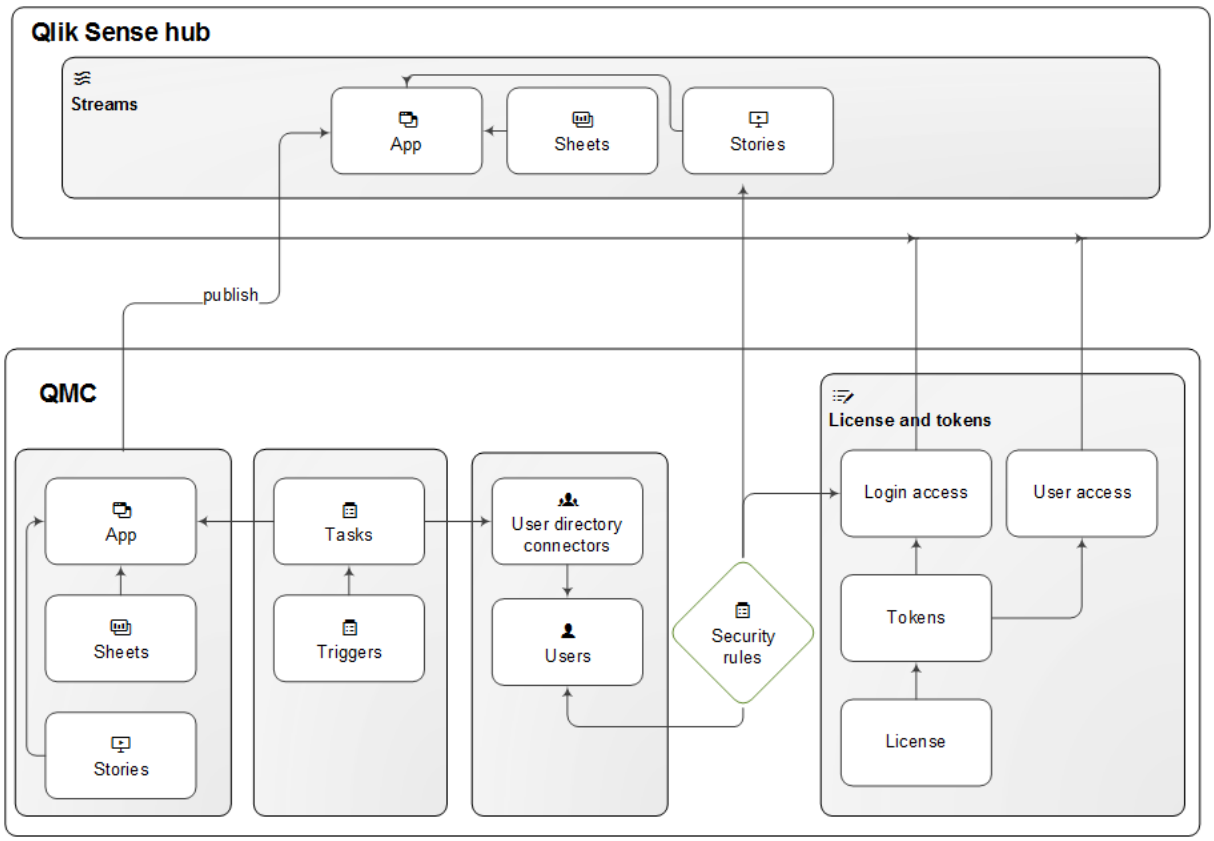
All user data is stored in the Qlik Sense Repository Service (QRS) database. You create user directory connectors in the QMC to be able to synchronize and retrieve the user data from a configured directory service. When a user logs in to Qlik Sense or the QMC, the user data is automatically retrieved.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

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.

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.

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

See also:

- *Configuring Qlik Sense (page 364)*
- *Writing security rules (page 421)*
- *Auditing access control (page 452)*
- *Authentication (page 371)*

1.6 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 is 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 Qlik Management Console (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. Also, a number of tokens become available.
   The License Enabling File (LEF) determines the number of tokens that you can allocate to different access types. An access type allows the users to access streams and apps within a Qlik Sense site. You can adjust the token usage according to the usage need over time.

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

See also:

- *Creating a root administrator user (page 276)*
- *Activating license (page 188)*
- *License and tokens (page 95)*
- *Allocating user access (page 255)*
- *Logging out from the QMC (page 21)*
- *Editing proxies (page 314)*

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.*

1.7 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

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+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

UI icons and symbols

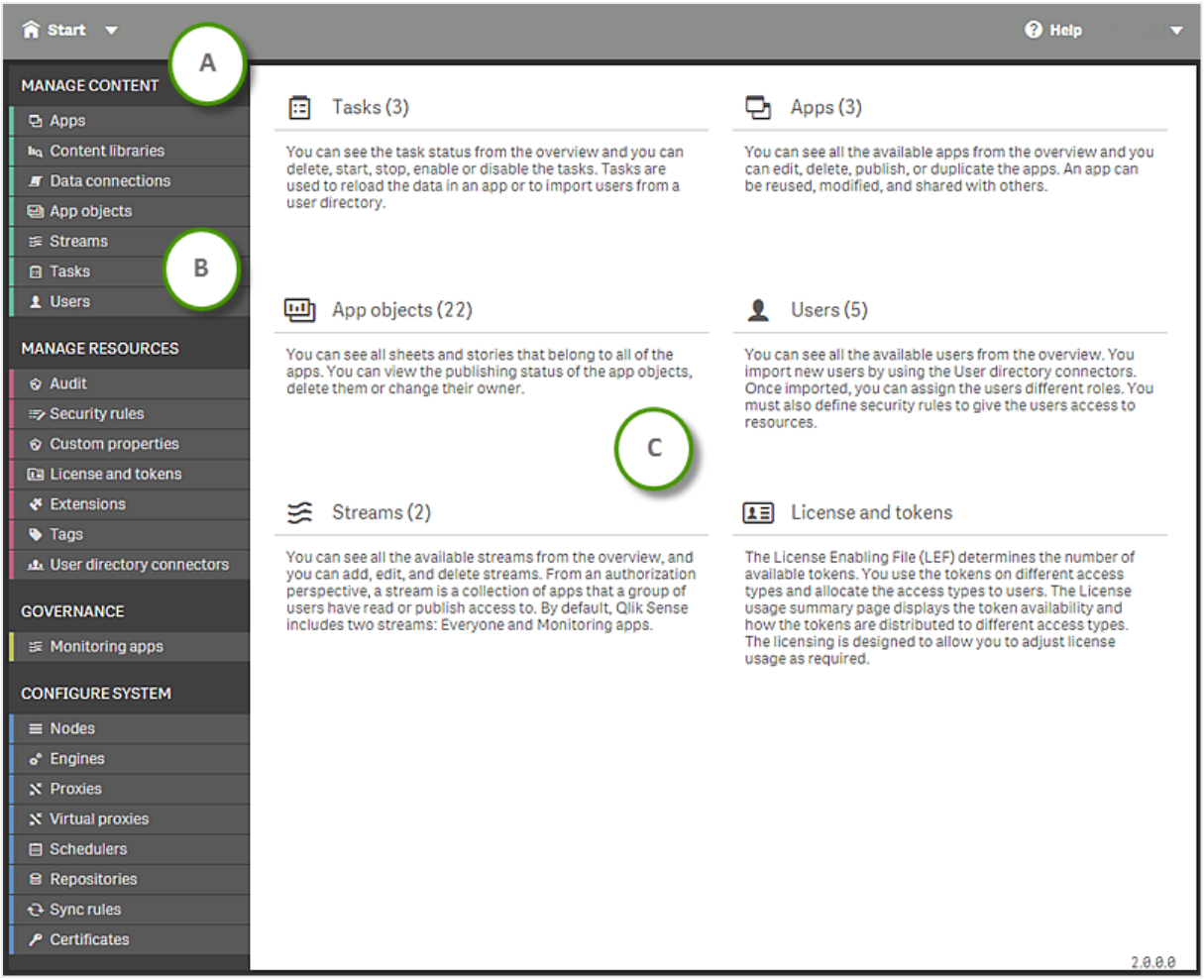
A symbol can be used in more than one context. Here is a list of the icons and symbols used throughout the Qlik Management Console (QMC) user interface.

	Create new
	Apps
	Content libraries
	Data connections
	App objects
	Streams
	Tasks
	Users
	Audit
	Security rules
	Custom properties
	License and tokens
	Extensions
	Tags
	User directory connectors
	License Monitor/Operations Monitor
	Nodes
	Engines
	Proxies
	Virtual proxies
	Schedulers
	Repositories
	Sync 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
	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.



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: Click **Start** to access the QMC start page. Click ▼ next to **Start** to display a drop-down list of all resources. This enables you to select another resource without first having to access the start page. Click **Help** to access the (QMC) help. The top right corner displays who is logged in to the (QMC). Click the drop-down ▼ next to the login name and click **Logout** in the dialog to log out.
B	The left panel contains all QMC resources in groups. If any of the Qlik Sense services are down, the number of services that are not running is displayed with a numeral.

C	The basic resources are also available from the middle of the start page. The number in parentheses indicates the number of occurrences of the resource.

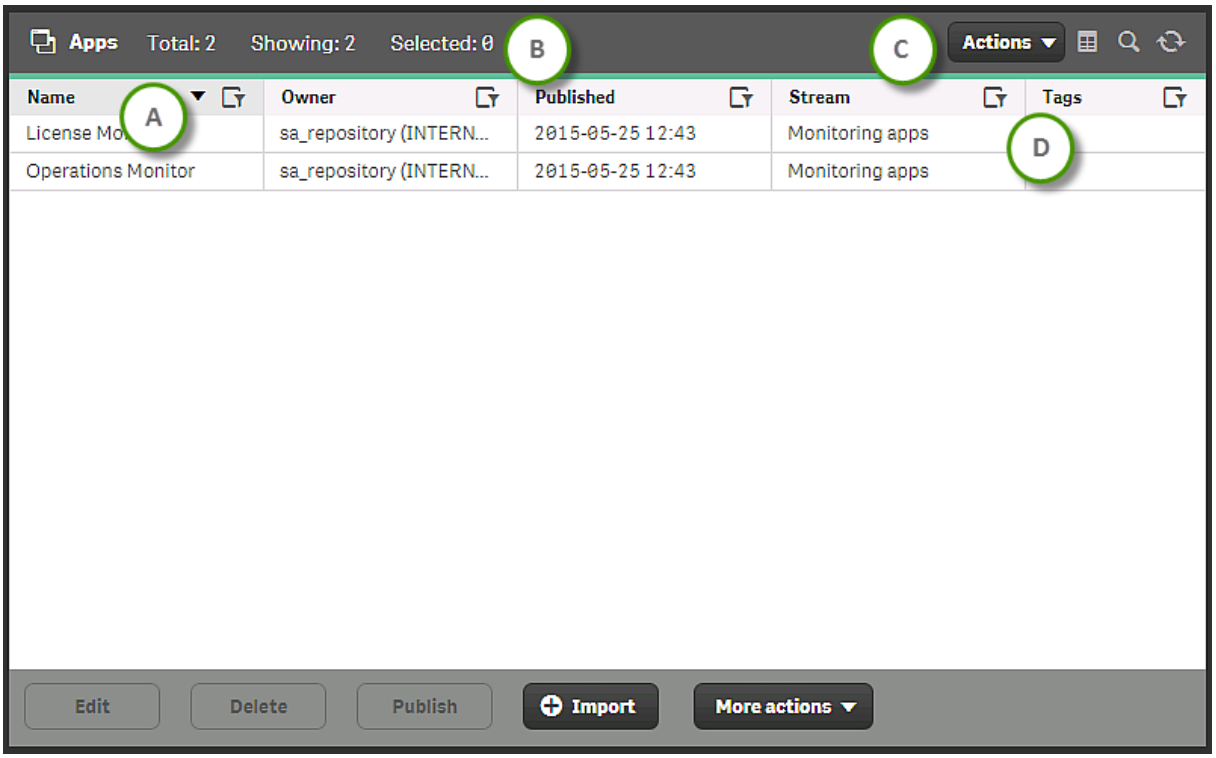
See also:

- *Providing administrators with access using roles (page 279)*

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 items**. 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 select and deselect all rows, and clear search and filters.



Apps overview page

Apps overview

A	Click a column heading to sort that column ascending ▼ or descending ▲ . Click ⊡ next to sorting to display the filter dialog for the column. Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, ⊡ is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**.
B	In the table header, to the left, you get a summary of the status of the current data set. **Total** shows the total number of resources. **Showing** shows the number of resources currently displayed. **Selected** shows the number of selected resources.
C	In the table header to the right, you have options for searching and selecting. Click **Actions** to open a menu with options to clear filters and search, and selecting or deselecting all rows. Options for clearing filter and search, and selecting or deselecting all rows. *The option **Select all rows** is applied to the rows that are currently displayed. Any rows that have been filtered out before selecting all rows are disregarded, even if they were selected. The option **Deselect all rows** is applied to all rows, including those that were filtered out.* Click ⊞ to open the **Column selector**, where you can select which columns to display in the overview. Click ↶ to reset to default columns.
D	You can create QMC tags and apply them to resources so that you can search and manage the QMC content efficiently.
E	The action bar at the bottom of the page contains different action buttons depending on the selected resource type. For example, select an app in the overview and click **Edit** to open the **App edit** page. When you do not have update rights for the selected items, **Edit** is replaced by **View**. If you do not have delete rights for the selected items, **Delete** is disabled.If a resource is deleted, all sync and security rules associated with that resource are deleted automatically.
F	Click ⊕ in the action bar to create a new instance of a resource. In this example, click ⊕ **Import** to open the **Import app** dialog.

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.

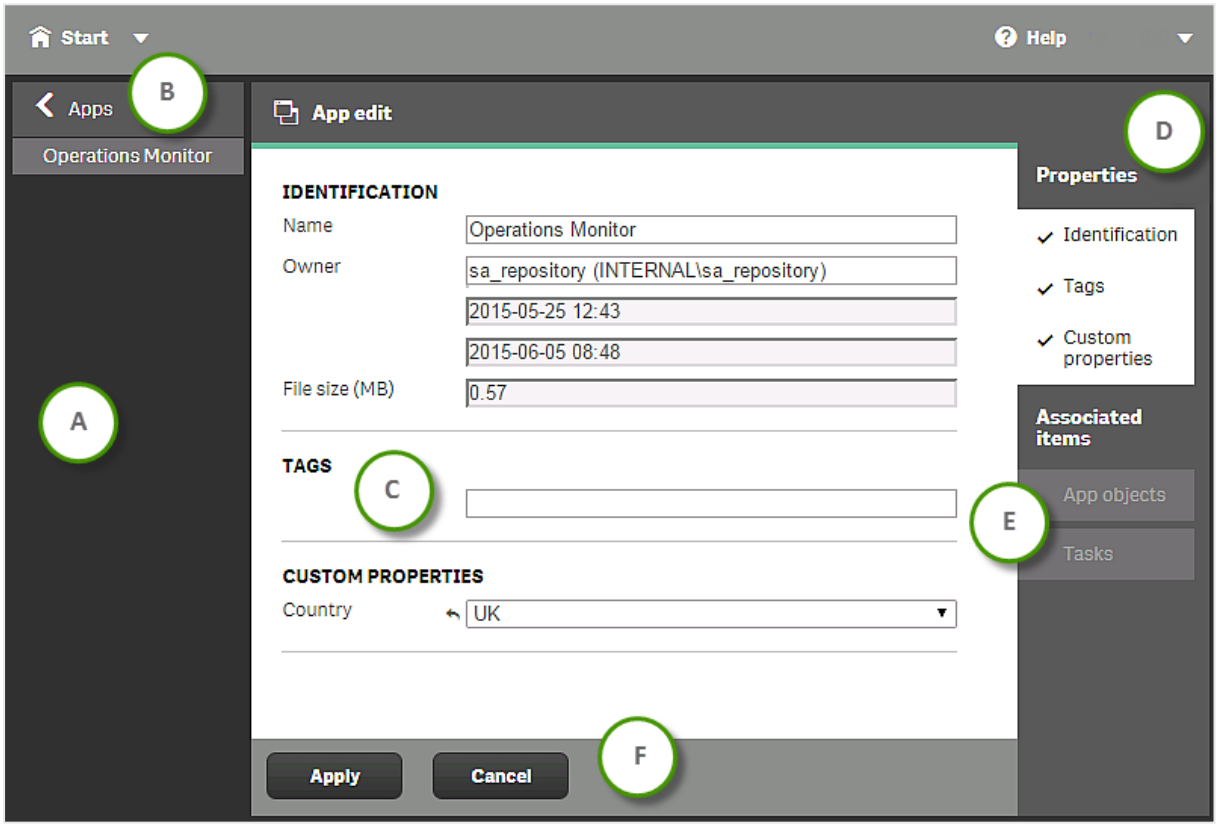
Double-click an item in the overview to open the resource's edit page. For multiple selections, hold down **Ctrl** while clicking the items, or drag over the items.

See also:

Searching and filtering in the QMC (page 29)

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 **App edit** page.



Example: The App edit page

App edit	
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 left panel. If you select several items from the overview and they have different values for a specific field, then *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	**Associated items**: select an associated item and click **Edit** to open the edit page.
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.

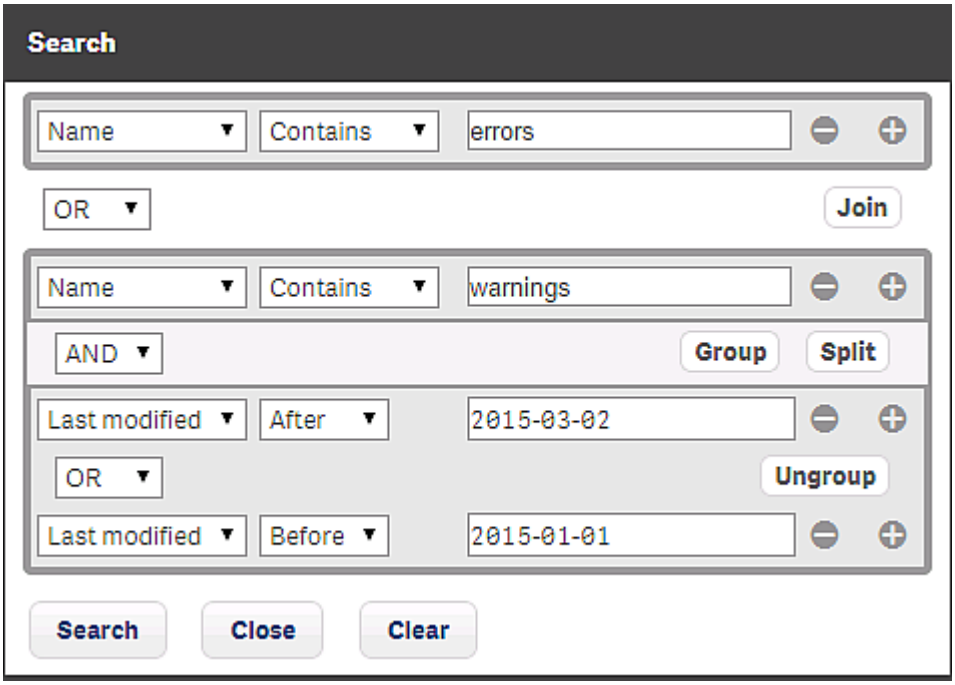
> *You clear search and filters by clicking ⊗ in the table header.*

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.



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.

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

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. You can create an app from the Qlik Sense hub, if you have the appropriate access rights. Apps are published to streams from the QMC, which is a part of Qlik Sense. To publish an app that is created 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.
Content libraries	A content library is a storage that enables the Qlik Sense users to add shared contents to their apps. The user who creates the content library automatically becomes the owner of that library. The library and the library objects can be shared with others through security rules defined in the QMC.
Data connections	Data connections enable you to select and load data from a data source. All data connections are managed centrally from the QMC. Data connections are created in the Qlik Sense data load editor. The user who creates a data connection automatically becomes the owner of that connection and is by default the only user who can access the data connection. The data connection can be shared with others through security rules defined in the QMC. When you import an app developed on Qlik Sense Desktop, existing data connections are imported to the QMC. When you export an app from a server, existing data connections are not exported with the app. *If the name of a data connection in the imported app is the same as the name of an existing data connection, the data connection will not be imported. This means that the imported app will use the existing data connection with an identical name, not the data connection in the imported app.*

App objects	You can manage the following app objects: • Sheets • Stories The user who creates an app is automatically designated as the owner of the app and its app objects. The app objects are published when the app they belong to is published. The users can add private app objects to the apps and share them by publishing the app objects from Qlik Sense.
Streams	A stream enables users to read and/or publish apps, sheets, and stories. Users who have publish access to a stream, create the content for that specific stream. The stream access pattern in 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.*
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 Execution of a task is initiated by a trigger or manually from the tasks overview page. You can create additional triggers to execute the task and there are two types of triggers: • Scheduled • Task event
Users	Users are imported from a user directory via a user directory connector in the QMC.
Audit	On the QMC audit page, you can query for, and audit, the security rules or sync 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 a user or 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 these values can be used in the security rule for a resource.
License and tokens	The License Enabling File (LEF) determines the number of tokens that you can allocate to different access types. An access type allows the users to access streams and apps within a Qlik Sense site. You can adjust the token usage according to the usage need over time.
Extensions	Extensions can be used to visualize data, for example, in an interactive map where you can select different regions.
Tags	You create QMC tags and apply them to resources to be able to search and manage the environment efficiently from the resource overview pages in 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, Local Users, and ODBC. 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.
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 multi-node installation, you manage the whole Qlik Sense site from the QMC on the central node.*
Engines	The Qlik Sense Engine Service (QES) is the application service that handles all application calculations and logic.
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. The QRS also manages the synchronization in multi-node Qlik Sense sites. 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).
Sync rules	The sync rules 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.

See also:

Providing administrators with access using roles (page 279)

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 an app from the Qlik Sense hub, if you have the appropriate access rights. Apps are published to streams from the QMC, which is a part of Qlik Sense. To publish an app that is created 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.

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 QMC tags that are connected to the app.
Description	The app description, if any.
File size (MB)	The file size of the app.
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. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
↻	Refresh the page.
Edit	Edit the selected apps. The number next to **Edit** indicates the number of items in your selection that you are allowed to edit.When you do not have update rights for the selected items, **Edit** is replaced by **View**.
View	View the selected apps. When you do not have update rights for the selected items, **Edit** is replaced by **View**.
Delete	Delete the selected apps. The number next to **Delete** indicates the number of items that will be deleted.If you do not have delete rights for the selected items, **Delete** is disabled.
Publish	Publish the selected apps.
⊕ **Import**	Import a new app.
More actions > **Export**	Export the selected app.
More actions > **Duplicate**	Duplicate the selected app.
More actions > **Reload now**	Reload the selected app. *In a multi-node site, where the Qlik Sense Scheduler Service(QSS) on the central node runs as 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 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**. 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.*

See also:

- *Managing apps (page 194)*
- *Importing apps (page 197)*
- *Editing apps (page 199)*
- *Creating reload tasks (page 205)*
- *Connecting tags (page 360)*
- *Applying a custom property value (page 358)*

Apps properties

The following property groups are available for apps:

Identification

The **Identification** property group contains the identification information for the for the selected apps.

Property	Description
Name	The name of the app.
Owner	The owner of the app.
Created	The date and time that the app was created.
Last modified	The date and time that the app was last modified.
File size (MB)	The file size of the app.

Tags

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

Custom properties

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

Apps 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 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: • **Not approved**: The app object is not approved because it was added to a published app. • **Approved**: The app object is approved because it belonged to the app when the app was published.
Published	The status of the app object: • **Not published**: The app object is not published to a stream. • **Published**: The app object is published to a stream. There are two alternatives: The app object itself has been published from Qlik Sense, or the app that the app object belongs to, has been published.
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.

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.

2.2 Content libraries

Currently, only material in the Default content library is accessible from the Qlik Sense hub.

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 QMC tags that are connected to the content library.
ID	The ID of the content library. By default, not displayed.
Created	The date and time when the content library was created.
Last modified	The date and time when the content library was last modified.
Modified by	By whom the content library was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.
	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	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 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**. 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.*

See also:

- *Creating content libraries (page 218)*
- *Editing content libraries (page 220)*
- *Uploading objects to content libraries (page 222)*
- *Creating access rights for content libraries (page 224)*

Content libraries properties

The following property groups are available for content libraries:

Identification

The **Identification** property group contains the identification information for the selected content libraries.

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

The property group **Tags** contains the QMC tags that are connected to the content library.

Property	Description
Tags	The available QMC tags are listed to the right. Connected QMC tags are listed to the left.

Custom properties

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

Content libraries 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
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>*. Click the link to preview the image in a new tab.
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.

Users

Users is available from **Associated items** when you edit a content library. The overview contains a list of the users that have access rights to selected content library.

Property name	Explanation
Name	The user information: *<name> (<User directory name>\<user ID>)*.
Permitted action	The actions that the user is allowed to perform on the resource, for example, Read or Update.
User directory	The user directory of the user.
User ID	The ID of the user.

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

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.

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 QMC tags that are connected to the data connection.
Connection string	The connection string for the data connection. Typically, includes the name of the data source, drivers, and path.
Type	The type of data connection. Standard data connections include ODBC, OLEDB, and Folder.
User ID	The user ID that is used in the connection string.
ID	The ID of the data connection. By default, not displayed.
Created	The date and time when the data connection was created.
Last modified	The date and time when the data connection was last modified.
Modified by	By whom the data connection was modified.
<Custom properties>	Custom properties, if any, are listed here.

▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.
	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	Refresh the page.
Edit	Edit the selected data connections.
Delete	Delete the selected data connections.
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**. 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.*

See also:

- *Editing data connections (page 232)*
- *Managing apps (page 194)*
- *Connecting tags (page 360)*

Applying a custom property value (page 358)

Data connections properties

The following property groups are available for data connections:

Identification

The **Identification** property group contains the identification information for the for the selected data connections.

Property	Description
Name	The name of the data connection.
Owner	The user name of the owner of the data connection.
Connection string	The connection string for the data connection. Typically, includes the name of the data source, drivers, and path.
Type	The type of data connection. Standard data connections include ODBC, OLEDB, and Folder.
User ID	The user ID that is used in the connection string.
Password	The password associated with the user ID used in the connection string. *The password is saved encrypted.*

Tags

The property group **Tags** contains the QMC tags that are connected to the data connection.

Property	Description
Tags	The available QMC tags are listed to the right. Connected QMC tags are listed to the left.

Custom properties

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

Data connections 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.

Users

Users is available from **Associated items** when you edit data connections. The overview contains a list of the users who are associated with the selected data connections.

Property name	Explanation
Name	The user information: *<name> (<User directory name>\<user ID>)*.
Permitted action	The actions that the user is allowed to perform on the resource, for example, Read or Update.
User directory	The user directory of the user.
User ID	The ID of the user.

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

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.

Property	Description
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 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: • **Not approved**: The app object is not approved because it was added to a published app. • **Approved**: The app object is approved because it belonged to the app when the app was published.
Published	The status of the app object: • **Not published**: The app object is not published to a stream. • **Published**: The app object is published to a stream. There are two alternatives: The app object itself has been published from Qlik Sense, or the app that the app object belongs to, has been published.

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 QMC tags that are connected to the app object.
ID	The ID of the app object.
Created	The date and time when the app object was created.
Modified by	By whom the app object was modified.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.
	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	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 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**. 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.*

See also:

- *Editing app objects (page 225)*
- *Deleting app objects (page 226)*

App objects properties

The following property groups are available for app objects.

Identification

The **Identification** property group contains the basic app object properties.

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

Tags

The **Tags** property group contains the QMC tags that are connected to the app objects.

Property	Description
Tags	The available QMC tags are listed to the right. Connected QMC tags are listed to the left.

2.5 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 in 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.
Tags	The QMC tags that are connected to the stream.
ID	The ID of the stream.
Created	The date and time when the stream was created.
Last modified	The date and time when the stream was last modified.
Modified by	By whom the stream was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.
	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	Refresh the page.
Edit	Edit the selected streams.
Delete	Delete the selected streams.
Create new	Create a new stream.
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**. 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.*

See also:

- *Creating streams (page 227)*
- *Editing streams (page 228)*
- *Connecting tags (page 360)*
- *Applying a custom property value (page 358)*

Streams properties

The following property groups are available for streams:

Identification

The **Identification** property group contains the identification information for the for the selected streams.

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

The **Tags** property group contains the QMC tags that are connected to the selected streams.

Property	Description
Tags	The available QMC tags are listed to the right. Connected QMC tags are listed to the left.

Custom properties

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

Streams 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.

Property	Description
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.

Users

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

Property name	Explanation
Name	The user information: *<name> (<User directory name>\<user ID>)*.
Permitted action	The actions that the user is allowed to perform on the resource, for example, Read or Update.
User directory	The user directory of the user.
User ID	The ID of the user.

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

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.

Property	Description
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.

2.6 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: • Reload (for app) • User synchronization (for user directory connector)
Enabled	Status values: **Yes** or **No**.

Status	The status of the task: ··· Never started Triggered Started Queued Abort initiated Aborting Aborted ✓ Success ✗ Failed ··· Skipped Retrying ✗ Error ··· Reset Click ⓘ to open a summary of the latest reload or user synchronization tasks. 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: • **On task event trigger**: The task execution is initiated by the completion of another task. • **On multiple triggers**: The task has more than one trigger applied. • The date and time for the next execution of the task is displayed if the task has a scheduled trigger applied. • If the field is empty, no trigger is created for the task.
Tags	The QMC tags that are connected to the task.
ID	The ID of the task.
Created	The date and time when the task was created.
Last modified	The date and time when the task was last modified.

Modified by	By whom the task was modified.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.
	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	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 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**. 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.*

See also:

- *Creating reload tasks (page 205)*
- *Creating a user directory connector (page 243)*
- *Viewing task chains (page 289)*
- *Searching and filtering in the QMC (page 29)*
- *Connecting tags (page 360)*
- *Applying a custom property value (page 358)*

Reload tasks properties

The following property groups are available for reload tasks.

Identification

The **Identification** property group contains the basic reload task properties in the Qlik Sense system.

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

The **Execution** property group contains the reload task execution properties in the Qlik Sense system.

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

The following properties are available for a scheduled trigger.

Property	Description
Name	The name of the trigger. Mandatory.
Type	The trigger type.
Enabled	The trigger is enabled when selected.
Start	Select when the trigger takes effect by typing the following values: • **Time to start (hh:mm)** and • **Start date (YYYY-MM-DD)**

Property	Description

Schedule	Set the trigger schedule:
	• **Once**.
	• **Hourly**. Set the time period between the executions of the trigger. Edit **Repeat after each** by typing the values for:
	  • **hour(s)** (default is 1)
	  • **minute(s)** (default is 0)
	• **Daily**. Set the time between the executions of the trigger by typing a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	• **Weekly**. Set the time between the executions of the trigger:
	  • Type a value for **Every week(s)** (default is 1) and
	  • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	  *If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*

End	Type values for the following: • **Time to end (hh:mm)** • **End date (YYYY-MM-DD)** Select **Infinite** to create a never ending trigger.

Triggers - task chain

The following properties are available for a task event trigger.

Property	Description
Name	The name of the trigger. Mandatory.
Type	The trigger type.
Enabled	The trigger is enabled when selected.

Property	Description
Time constraint	Defines the time period (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. See: *Creating a task chain (page 286)*
Add task **Task successful** or **Task failed**	Do the following: a. Click **Add task** to add a tasks that will function as a trigger condition. A drop-down list and an empty field is added. b. Click the empty field to add a task. The dialog **Double-click to select** is opened and displays a list of tasks with the following columns: **App name**, **Tags** connected to the task, and **Name**, which is the task name. Click a column heading to sort that column ascending ▼ or descending ▲ . *You can filter a column by using the filtering option:* . c. Double-click the task that will function as a trigger condition. The task is added to the trigger and the dialog is closed. d. Use the drop-down list to select whether the trigger condition is fulfilled on **Task successful** or **Task failed**. Click **Delete** to remove a task from the trigger. *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).* 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 **Select task by double-click** dialog if it has already been added to the trigger. There is a logical AND between

*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 time period is reached, the task that was first completed is no longer considered executed and the end of the time period is recalculated. The trigger then waits for all tasks to be completed within the recalculated time period.*

Tags

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

Custom properties

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

User sync tasks properties

The following property groups are available for user sync tasks.

Identification

The **Identification** property group contains the basic user sync task properties in the Qlik Sense system.

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

Tags

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

User sync task associated items

The following associated items are available for user sync tasks.

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.
Valid until	Displays year, date, and time according to the **End** values that was entered when creating the trigger.
Repeat	Displays the repeat pattern according to the **Repeat** 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.
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.

See also:

Creating reload tasks (page 205)

2.7 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, click **Users** from the property groups, select the user and click **Edit**.*

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**.
Removed externally	Status values: **Yes** or **No**. When **Yes**, it is normally because the user has been removed from the user directory.
Tags	The QMC tags that are connected to the user.
ID	The ID of the user.
Created	The date and time when the user was created.
Last modified	The date and time when the user was last modified.
Modified by	By whom the user was modified.

<Custom properties>	Custom properties, if any, are listed here.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.
	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	Refresh the page.
Edit	Edit the selected users.
Delete	Delete the selected users.
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**. 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.*

See also:

- *Setting up a user directory connector and schedule by task (page 238)*
- *Deleting user directory connector and users (optional) (page 253)*

- *Synchronizing with user directories (page 254)*
- *Managing admin roles for a user (page 276)*
- *Editing items owned by users (page 278)*
- *Providing administrators with access using roles (page 279)*
- *Connecting tags (page 360)*
- *Applying a custom property value (page 358)*

Users properties

The following property groups are available for users.

Identification

The property group **Identification** contains identification information for the selected user.

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.
Admin roles	The QMC administration roles associated with the user.

Tags

The property group **Tags** contains the QMC tags that are connected to the user.

Property	Description
Tags	The available QMC tags are listed to the right. Connected QMC tags are listed to the left.

Custom properties

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

Users associated items

The following associated items are available for users.

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

Owned items

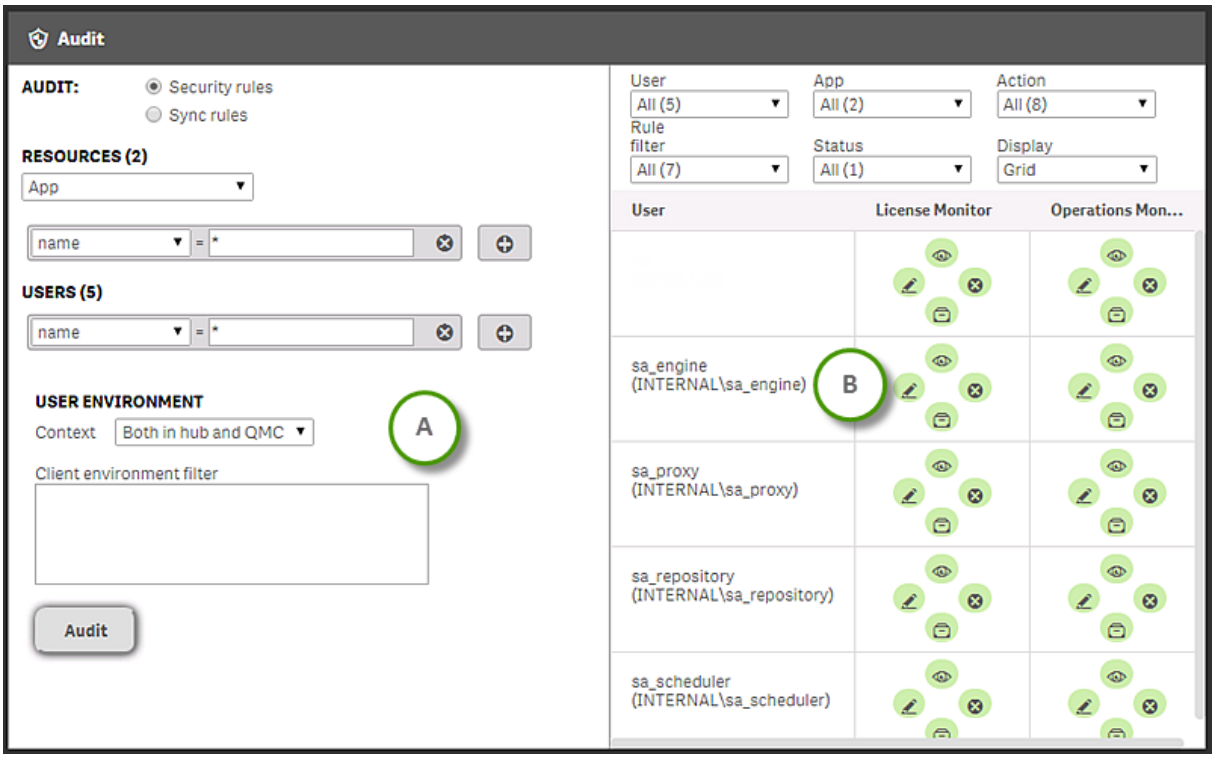
Owned items is available from **Associated items** when you edit users. The overview contains a list of the resources owned by the selected users.

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 if they have the same edit page.

2.8 Audit

On the QMC audit page, you can query for, and audit, the security rules or sync rules that have been defined in the Qlik Sense system. The **Audit** page is split into two views: query and results.



Audit page with the query view and the results view

A. Query view
B. Results view

> *You can only view security rules that you have read access rights to.*

You can narrow your query further by defining one or more conditions for the following items in the query view:

- Resources
- Users
- User environment

> *You can use the **Client environment filter** to simulate browser environment parameters, that is, parameters that are specific to a certain browser.*

The results of the search are presented in the results view. You can filter results using a number of different parameters.

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**. Searching, sorting, and filtering of items is always done on the full database list of items, not only the items that are displayed.

See also:

- *Auditing access control (page 452)*
- *Defining an audit query (page 453)*
- *Viewing and filtering audit query results (page 454)*
- *Previewing rules (page 455)*

Audit properties

The following property groups are available for audit.

Resources

The **Resources** attribute list contains a list of the resources that matched your search conditions. For example, if you searched for app the Resource drop-down list will be titled **App** and contain a list of available apps.

User

The **User** attributes list contains a list of the users that were identified by the search conditions.

Rule filter

The **Rule filter** attribute list contains the security rules that apply to the resources that matched your search conditions.

Status

The **Status** attributes list contains the possible status markers associated with the security rules that matched your search criteria.

> *You can only view security rules that you have access rights to read.*

Attribute name	Explanation
OK	The rule is enabled and you have the access rights to be allowed to see it.
Broken	A rule is broken when it was not possible to verify it.
Disabled	The rule has been disabled. Rules are enabled or disabled from the Security rules edit view.

Action

The **Action** list contains the available action properties.

Property name	Description
create	Create resource
read	Read resource
update	Update resource
delete	Delete resource
export	Be able to export a resource to a new format, for example Excel
publish	Be able to publish a resource to a stream
changeOwner	Be able to change the owner of a resource
changeRole	Be able to change user role
exportData	Be able to export data from an object

Display

The **Display** list enables you to switch between the Audit viewing modes.

Attribute name	Explanation
List	The default view showing the search results in a standard list.
Grid	An overview of user access rights to the resources that were returned by the search.

Audit grid icons

The **Grid** icons show the access types that matched your search conditions.

Icon	Description
	Read
	Update and/or Write and/or Edit
	Delete
	Sync
	Other, for example Create, ChangeOwner and/or Export

2.9 Security rules

The Qlik Sense system includes an attribute-based security rules engine that uses rules as expressions to evaluate what type of access a user or 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. 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 QMC tags that are connected to the rule.
Conditions	Shows the conditions for the security rule.
ID	The security rule ID.
Created	The date and time when the security rule was created.
Last modified	The date and time when the security rule was last modified.

Modified by	By whom the security rule was modified.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.
	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	Refresh the page.
Edit	Edit the selected security rule.
Delete	Delete the selected security rules.
Create new	Create a new security rule.
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**. 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 sync 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.*

See also:

- *Designing access control (page 391)*
- *Getting to know the security rules edit page (page 398)*
- *Creating security rules (page 399)*
- *Allocating user access (page 255)*
- *Previewing how security rules affect user privileges (page 409)*
- *Editing security rules (page 410)*
- *Deleting security rules (page 420)*
- *Security rule conventions (page 422)*
- *Operators and functions for conditions (page 426)*
- *Security rules examples (page 439)*
- *Connecting tags (page 360)*

Security rules properties

The following property groups are available for security rules.

Identification

The following **Identification** property groups are available.

Create rule from template

The option **Create rule from template** is only available when creating a new security rule.

Property	Security rule will be applied to
Unspecified	Access rules
App access	Apps
App object access	Objects The Objects' objectTypes, for example: sheet, story, bookmark, measure, or dimension.
Content library access	Content libraries
Data connection access	Data connections
Extension access	Extensions

Property	Security rule will be applied to
Reload task access	Reload tasks
Node access	The configuration of Qlik Sense nodes
Stream access	Streams
User access	Users
Security rule access	Security rules
User directory connector access	User directories
User sync task access	User synchronization tasks

Name

Property	Description
Name	The name of the rule.

Disabled

Property	Description
Disabled	When selected, the rule is disabled.

Description

Property	Description
Description	Text describing what the rule does.

Resource filter (Advanced view)

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

Syntax:

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

If you select a resource from the **Resource** drop-down list in the Basic view, the **Resource** field in the Advanced view is automatically filled in with the selected resource. The optional asterisk ('*') is added by default. The **Conditions** field is also automatically filled in with the corresponding code for the selected resource type.

> *If you define a rule without specifying at least one **Resource** or **User** condition, your rule will apply to all resources and/or users as indicated by **(ALL)** next to the condition heading.*

Arguments:

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

Properties:

Property	Security rule will be applied to
App	Apps
App.Object	Objects The Objects' objectTypes, for example: sheet, story, bookmark, measure or dimension.
ContentLibrary	Content libraries
DataConnection	Data connections
Extension	Extensions
ReloadTask	Reload tasks
ServerNodeConfiguration	The configuration of Qlik Sense nodes
Stream	Streams
SystemRule	System rules
UserDirectory	User directories
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.
`App*, Streams*, App.Object* resource.resourcetype="App.Object" and (((resource.objectType="sheet")))`	The rule will apply to apps, streams and sheets. *You can leave out App.Object* ... in this example as App* will apply the rule to both apps and sheets.*
`Stream_88ee46c6-5e9a-41a7-a66a-f5d8995454ec`	The rule will apply to the stream with the specified GUID.
`Stream_\w{8}-\w{4}-\w{4}-\w{4}-\w{12}`	The rule will apply to all existing streams.
Select **App** from the **Resource** drop-down list.	The following texts appear in the Advanced view: **Resource***`App*` **Conditions***`resource.resourcetype="App" and ( )` *If you don't enter a resource or a user condition inside the brackets, the security rule will by default apply to all apps and all users.*

See also:

- *Available resource filters (page 434)*

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.

*If you define a rule without specifying at least one **Resource** or **User** condition, your rule will apply to all resources and/or users as indicated by **(ALL)** next to the condition heading.*

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 can ungroup them by clicking **Ungroup**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that OR is superior to AND.
To enable synchronization between the **Basic** and **Advanced** sections (so called backtracking), extra parenthesis 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**. 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 77)* for available names.
propertyvalue	The value of the selected property name.
user	Implies that the conditions will be applied to a user.

Properties:

Property name	Available in	Description
@<customproperty>	App, App.Object, DataConnection, ReloadTask, ServerNodeConfiguration, Stream, Task	The custom property associated with the resource.
resource.@<customproperty>	App.Object, ReloadTask	The custom property associated with the resource.

Property name	Available in	Description
app.name	App.Object, ReloadTask	The name of the associated app.
app.owner.@<customproperty>	ReloadTask	The custom property associated to the stream of an app. See the corresponding owner property for a description.
app.owner.email	ReloadTask	Owner property associated with the app. See the corresponding owner property for a description.
app.owner.environment.browser	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.context	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.device	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.ip	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.os	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.secureRequest	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.group	ReloadTask	Owner property associated with the app. See corresponding owner property for description.

Property name	Available in	Description
app.owner.name	ReloadTask	The user name of the owner of the resource.
app.owner.userDirectory	ReloadTask	The user directory of the owner of the resource
app.owner.userId	ReloadTask	The user id of the owner of the resource
app.stream.@<customproperty>	App.Object, ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.stream.name	App.Object, ReloadTask	The name of the associated stream.
category	SystemRule	The system rule category: License, Security or Sync.
description	User	The description of the owner retrieved from the user directory.
email	User	The email addresses that are available from the connected user directories.

Property name	Available in	Description
environment.browser	User	Security rule will be applied to the type of browser. Supported browsers: Chrome, Firefox, Safari, MSIE or Unknown. **Example 1:** Define browser and version: Firefox 22.0 Chrome 33.0.1750.154 *If the browser information contains a slash (/), replace it with a space.* **Example 2:** Use the wildcard (*) to include all versions of the browser: environment.browser like Chrome*
environment.context	User	Security rule will be applied only to the Qlik Sense environment that the call originates from. Available preset values: ManagementAccess or AppAccess.
environment.device	User	Security rule will be applied to the type of device. Available preset values: iPhone, iPad or Default.

Property name	Available in	Description
environment.ip	User	Security rule will be applied to an IP number.
environment.os	User	Security rule will be applied to the type of operating system. Available preset values: Windows, Linux, Mac OS X or Unknown.
environment.secureRequest	User	Security rule will be applied to the type of request. Available preset values: SSL True or False.
group	User	The group memberships of the owner retrieved from the user directory.
roles	User	A role that is associated with the user.
name	App, App.Object, DataConnection, Extension, License.LoginAccessType, ReloadTask, ServerNodeConfiguration, Stream, User, UserDirectory, UserSyncTask, SystemRule,	The name of the resource or user.
objectType	App.Object	The type of app object. Available preset values: story, masterobject, properties, sheet, dimension.
owner.@<customproperty>	App, App.Object, DataConnection, Extension, Stream	The custom property associated with the owner of the resource.
owner.description	App, DataConnection, Extension, Stream	The description of the owner retrieved from the user directory.
owner.email	App, App.Object, DataConnection, Extension, Stream	The email of the owner retrieved from the user directory.

Property name	Available in	Description
owner.environment.browser	App, App.Object, DataConnection, Extension, Stream	The browser environment of the owner of the resource.
owner.environment.context	App, App.Object, DataConnection, Extension, Stream	Security rule will be applied only to the Qlik Sense environment that the call originates from. Available preset values: ManagementAccess or AppAccess.
owner.environment.device	App, App.Object, DataConnection, Extension, Stream	The device environment of the owner of the resource.
owner.environment.ip	App, App.Object, DataConnection, Extension, Stream	The IP environment of the owner of the resource.
owner.environment.os	App, App.Object, DataConnection, Extension, Stream	The OS environment of the owner of the resource.
owner.environment.secureRequest	App, App.Object, DataConnection, Extension, Stream	Indicates if the sent request is encrypted or not, that is using SSL or not (True or False).
owner.group	App, App.Object, DataConnection, Extension, Stream	The group memberships of the owner retrieved from the user directory.
owner.name	App, App.Object, DataConnection, Extension, Stream	The user name of the owner of the resource.
owner.userDirectory	App, App.Object, DataConnection, Extension, Stream	The user directory of the owner of the resource
owner.userId	App, App.Object, DataConnection, Extension, Stream	The user id of the owner of the resource.
published	App.Object	The status of the app object.

Property name	Available in	Description
resourceFilter	SystemRule	The existing resource definitions (from the Resource column in the security rules overview).
ruleContext	SystemRule	Specifies where the rule is to be applied: **Both in hub and QMC**, **Only in hub**, or **Only in QMC**.
stream.@<customproperty>	App	The custom property associated with the stream.
stream.name	App	The name of the associated stream.
type	SystemRule, DataConnection	The type of security rule or data connection.
userid	User	A user's ID.
userdirectory	User	The name of a user directory.
userDirectory.name	UserSyncTask	The name of the user directory connection that the user sync task applies to.
userDirectory.userDirectoryName	UserSyncTask	The name of the user directory that the user directory connector is connected to.
userDirectoryName	UserDirectory	The name of the user directory connection in the QMC.

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* **Conditions:**`resource.resourcetype="App" and (resource.name like "*")`	The rule will apply to all apps. *The same rule can be defined by simply setting the **Resource** field to App* and leaving the **Conditions** field empty.*
Resource filter: App* or App.Object* or Stream* **Conditions:**`resource.resourcetype="App" or resource.resourcetype="Stream" or (resource.resourcetype="App.Object" and resource.objectType="sheet") and resource.name like "My*"`	The rule will apply to all apps, streams and sheets that have names beginning with "My".
`resource.resourcetype="ServerNodeConfiguration" and (resource.@Geographies="Canada")`	The rule will apply to all nodes with the custom property Geographies set to Canada.
`resource.resourcetype="ServerNodeConfiguration" and !(resource.@Geographies="Canada")`	The rule will apply to all nodes except the nodes with custom property Geographies set to Canada.
With **Resource filter** **=** `resource.resourcetype="App.Object" and (((resource.objectType="sheet" or resource.objectType="story")) and ((user.name="Myname")))`	The rule will apply to all apps, sheets, stories and the user with the name MyName.
With **Resource filter=**`Stream_*` `user.@Geographies="Canada" and !user.IsAnonymous()`	The rule will apply to all streams and users with the custom property Geographies set to Canada given that the user is not logged in as anonymous.
With **Resource filter=**`*` and Conditions field empty	This rule will apply to all resources and all users.
user.name="MyUserName"	The rule will apply to the user with the user name MyUserName. *Try as much as possible not to create rules that apply to individuals. Use group memberships, user roles or custom properties to apply rules to groups of users.*
user.group="DL-MyDepartment"	The rule will apply to all members of the distribution group MyDepartment.

Example	Result
user.@Department="Sales"	The rule will apply to all users with the custom property @Department set to Sales.
user.roles="Developer"	The access rights defined in the Resource, Conditions and Actions field will be applied to the user role Developer. This role will now be available from the Roles drop-down list in the User edit page.
resource.resourcetype="App" and resource.name="My*" and user.role="QlikSenseAdmin"	The user.role can also be used together with an operator to specify that the rule applies if the user has the specified user role.
user.environment.os="Windows"	The rule will be applied to all external environments with operating system = Windows.

See also:

- *Conditions (Basic view) (page 85)*
- *Operators and functions for conditions (page 426)*
- *Writing security rules (page 421)*

Context (Advanced view)

Define in which context the rule is to be applied.

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

Conditions (Basic view)

*Any user properties contained in connected user directories will be shown in the **User access conditions** drop-down list. This could, for example, be an email address or department name.*

Property name	Available in	Description
@<customproperty>	App, App.Object, DataConnection, ReloadTask, ServerNodeConfiguration, Stream, Task	The custom property associated with the resource.

Property name	Available in	Description
resource.@<customproperty>	App.Object, ReloadTask	The custom property associated with the resource.
app.name	App.Object, ReloadTask	The name of the associated app.
app.owner.@<customproperty>	ReloadTask	The custom property associated to the stream of an app. See the corresponding owner property for a description.
app.owner.email	ReloadTask	Owner property associated with the app. See the corresponding owner property for a description.
app.owner.environment.browser	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.context	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.device	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.ip	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.os	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.secureRequest	ReloadTask	Owner property associated with the app. See corresponding owner property for description.

Property name	Available in	Description
app.owner.group	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.name	ReloadTask	The user name of the owner of the resource.
app.owner.userDirectory	ReloadTask	The user directory of the owner of the resource
app.owner.userId	ReloadTask	The user id of the owner of the resource
app.stream.@<customproperty>	App.Object, ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.stream.name	App.Object, ReloadTask	The name of the associated stream.
category	SystemRule	The system rule category: License, Security or Sync.
description	User	The description of the owner retrieved from the user directory.
email	User	The email addresses that are available from the connected user directories.

Property name	Available in	Description
environment.browser	User	Security rule will be applied to the type of browser. Supported browsers: Chrome, Firefox, Safari, MSIE or Unknown. **Example 1:** Define browser and version: Firefox 22.0 Chrome 33.0.1750.154 *If the browser information contains a slash (/), replace it with a space.* **Example 2:** Use the wildcard (*) to include all versions of the browser: environment.browser like Chrome*
environment.context	User	Security rule will be applied only to the Qlik Sense environment that the call originates from. Available preset values: ManagementAccess or AppAccess.
environment.device	User	Security rule will be applied to the type of device. Available preset values: iPhone, iPad or Default.

Property name	Available in	Description
environment.ip	User	Security rule will be applied to an IP number.
environment.os	User	Security rule will be applied to the type of operating system. Available preset values: Windows, Linux, Mac OS X or Unknown.
environment.secureRequest	User	Security rule will be applied to the type of request. Available preset values: SSL True or False.
group	User	The group memberships of the owner retrieved from the user directory.
roles	User	A role that is associated with the user.
name	App, App.Object, DataConnection, Extension, License.LoginAccessType, ReloadTask, ServerNodeConfiguration, Stream, User, UserDirectory, UserSyncTask, SystemRule,	The name of the resource or user.
objectType	App.Object	The type of app object. Available preset values: story, masterobject, properties, sheet, dimension.
owner.@<customproperty>	App, App.Object, DataConnection, Extension, Stream	The custom property associated with the owner of the resource.
owner.description	App, DataConnection, Extension, Stream	The description of the owner retrieved from the user directory.
owner.email	App, App.Object, DataConnection, Extension, Stream	The email of the owner retrieved from the user directory.

Property name	Available in	Description
owner.environment.browser	App, App.Object, DataConnection, Extension, Stream	The browser environment of the owner of the resource.
owner.environment.context	App, App.Object, DataConnection, Extension, Stream	Security rule will be applied only to the Qlik Sense environment that the call originates from. Available preset values: ManagementAccess or AppAccess.
owner.environment.device	App, App.Object, DataConnection, Extension, Stream	The device environment of the owner of the resource.
owner.environment.ip	App, App.Object, DataConnection, Extension, Stream	The IP environment of the owner of the resource.
owner.environment.os	App, App.Object, DataConnection, Extension, Stream	The OS environment of the owner of the resource.
owner.environment.secureRequest	App, App.Object, DataConnection, Extension, Stream	Indicates if the sent request is encrypted or not, that is using SSL or not (True or False).
owner.group	App, App.Object, DataConnection, Extension, Stream	The group memberships of the owner retrieved from the user directory.
owner.name	App, App.Object, DataConnection, Extension, Stream	The user name of the owner of the resource.
owner.userDirectory	App, App.Object, DataConnection, Extension, Stream	The user directory of the owner of the resource
owner.userId	App, App.Object, DataConnection, Extension, Stream	The user id of the owner of the resource.
published	App.Object	The status of the app object.

Property name	Available in	Description
resourceFilter	SystemRule	The existing resource definitions (from the Resource column in the security rules overview).
ruleContext	SystemRule	Specifies where the rule is to be applied: **Both in hub and QMC**, **Only in hub**, or **Only in QMC**.
stream.@<customproperty>	App	The custom property associated with the stream.
stream.name	App	The name of the associated stream.
type	SystemRule, DataConnection	The type of security rule or data connection.
userid	User	A user's ID.
userdirectory	User	The name of a user directory.
userDirectory.name	UserSyncTask	The name of the user directory connection that the user sync task applies to.
userDirectory.userDirectoryName	UserSyncTask	The name of the user directory that the user directory connector is connected to.
userDirectoryName	UserDirectory	The name of the user directory connection in the QMC.

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

See also:

- *Conditions (Advanced view) (page 76)*
- *Operators and functions for conditions (page 426)*

Actions (Basic view)

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

Property name	Description
Create	Create resource
Read	Read resource
Update	Update resource
Delete	Delete resource
Export	Be able to export a resource to a new format, for example Excel
Publish	Be able to publish a resource to a stream
Change owner	Be able to change the owner of a resource
Change role	Be able to change user role
Export data	Be able to export data from an object

Tags

Property	Description
Tags	The available QMC tags are listed in the text box. Connected QMC tags are listed under the text box.

Security rules associated items

The following associated items are available for **Security rules**.

Preview

Preview is available from **Associated items** when you edit security rules. The preview page shows you a preview of the effects that your rules will have when you apply them.

2.10 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 these values can be used 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. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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 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**. 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.*

See also:

- *Using custom properties (page 353)*
- *Creating a custom property (page 355)*
- *Applying a custom property value (page 358)*
- *Editing a custom property (page 356)*

Custom property properties

The following property groups are available for custom properties:

Identification

The **Identification** property group contains the name of the custom property.

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

The **Resource types** property group contains the resources that the custom property can be used on.

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

Values

The **Values** property group contains values that you create for the custom property.

Property	Description
Values	The values that you create can be used in security rules.

2.11 License and tokens

The License Enabling File (LEF) determines the number of tokens that you can allocate to different access types. An access type allows the users to access streams and apps within a Qlik Sense site. You can adjust the token usage according to the usage need over time.

- On the **License usage summary** page, you can see the token availability and how the tokens are distributed to the different access types.

- 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 **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.

See also:

- *Managing license and tokens (page 187)*
- *Getting to know the license usage summary page (page 189)*

License usage summary

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.

See also:

- *Allocating user access (page 255)*
- *Deallocating user access (page 255)*

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. **Deleted user** is displayed if the user is deleted. When the quarantine period is over, the deleted user is removed from the overview.
User directory	The user directory that the user is imported from.
Status	The status of the user access: **Allocated** means that user access is allocated to the identified user and the user can access the hub and apps. **Quarantined** means the following: • The user cannot access streams and apps on the hub. • User access was previously allocated to the user and thereafter deallocated. • The token is not available for new allocation until the end of the quarantine period (seven days). • During the quarantine period, user access can be reinstated to the original user.
Last used	The date and time when the user accessed the hub.
ID	The user access ID.
Created	The date and time when the user access was created.
Last modified	The date and time when the user access was last modified.
Modified by	By whom the user access was modified.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.
	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*

Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	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 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**. 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.*

See also:

- *Allocating user access (page 255)*
- *Deallocating user access (page 255)*
- *Reinstating user access (page 256)*
- *Searching and filtering in the QMC (page 29)*

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.
▼ ▲	Click to sort the list alphabetically, ascending or descending according to the nature of 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**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
↻	Refresh the page.
Edit	Edit the selected user access rule.
Delete	Delete the selected user access rules.
⊕ Create associated rule	Create a new user access rule.
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**. 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.*

See also:

- *Creating user access rule (page 261)*
- *Editing user access rule (page 263)*
- *Deleting user access rule (page 265)*

User access rules properties

The following property groups are available for user access rules.

Identification

The following **Identification** property groups are available.

Name

Property	Description
Name	The name of the rule.

Disabled

Property	Description
Disabled	When selected, the rule is disabled.

Description

Property	Description
Description	Text describing what the rule does.

Advanced

The following **Advanced** property groups are available.

Resource filter

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

The **Resource** field in the **Advanced** section is automatically filled in.

> *Do not edit the Resource filter field. If you do, the rule might not work as intended.*

Property	Description
Resource filter	The type of resource that the rule applies to. An asterisk (*) indicates that the rule applies to all resources. For generated rules the **Resource filter** field includes the ID for the rule.

Conditions

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

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.

Property	Description
Conditions	The conditions define the resource and/or user conditions that the user access rule is to apply to.

Context

Define in which context the rule is to be applied.

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

Basic

The following **Basic** property groups are available.

Actions

The action that the user is allowed to perform on the resource. For user access rules the action is always **Allow access**.

Conditions

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

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

Item	Description
Conditions	The conditions define the resource and/or user conditions that the user access rule is to apply to.

Tags

Property	Description
Tags	The available QMC tags are listed in the text box. Connected QMC tags are listed under the text box.

User access rules associated items

The following table presents 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.

Users

Users is available from **Associated items** when you edit user access rules. The overview contains a list of the users who are associated with the selected user access rule.

Property	Description
Name	The user name of the user followed by (User directory name\user ID).
Permitted action	The actions the user is allowed to perform on the resource UseAccessType.
User directory	The user directory of the associated user.
User ID	The user ID of the associated user.

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.

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.

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

Name	The name of the login access group.
Allocated tokens	The number of tokens that are allocated to the login access group, providing a number of access passes.
Used login access passes	The number of access passes that have been used, when users from the group have logged in to the hub.
Remaining login access passes	The number of access passes that are available for users in the group, for logins to the hub.
ID	The ID of the login access group.
Created	The date and time when the login access group was created.
Last modified	The date and time when the login access group was last modified.
Modified by	By whom the login access group was modified.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.
	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*

Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	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 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**. 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.

See also:

- *Creating login access (page 256)*
- *Editing login access (page 259)*
- *Deleting login access (page 260)*

Login access properties

The following property groups are available for login access.

Identification

The property group **Identification** contains a user login access property.

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

Tokens

The property group **Allocated tokens** contains a login access property.

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

Login access 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.

Users

Users is available from **Associated items** when you edit a login access (group). The overview contains a list of the users who are associated with the selected user access rule.

Property	Description
Name	The user name of the user followed by (User directory name\user ID).
Permitted action	The actions the user is allowed to perform on the resource: UseAccessType.
User directory	The user directory of the user.
User ID	The user ID of the user.

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

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.

Property name	Description
Conditions	The license rule conditions.
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 Enabling 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.

See also:

- *Activating license (page 188)*
- *Changing license (page 191)*

Site license properties

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.

2.12 Extensions

Extensions can be 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 QMC tags that are connected to the extension.
ID	The ID of the extension.
Created	The date and time when the extension was created.
Last modified	The date and time when the extension was last modified.
Modified by	By whom the extension was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.
	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	Refresh the page.
Edit	Edit the selected extensions.
Delete	Delete the selected extensions.
Import	Import a new extension.
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**. 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.*

See also:

- *Importing extensions (page 235)*
- *Editing extensions (page 236)*
- *Connecting tags (page 360)*

Extensions properties

The following property groups are available for extensions.

Identification

The property group **Identification** contains identification information for the for the selected extensions.

Property	Description
Name	The name of the extension is obtained from the file name of the extension definition file (*.qext*) in the uploaded zip file and cannot be modified.
Owner	The user name of the owner of the extension. *This property is only visible when editing an extension.*

Tags

The property group **Tags** contains the QMC tags that are connected to the selected extensions.

Property	Description
Tags	The available QMC tags are listed to the right. Connected QMC tags are listed to the left.

Custom properties

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

Extensions 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.

Users

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

Property name	Explanation
Name	The user information: *<name> (<User directory name>\<user ID>)*.
Permitted action	The actions that the user is allowed to perform on the resource, for example, Read or Update.
User directory	The user directory of the user.
User ID	The ID of the user.

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

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.

2.13 Tags

You create QMC 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. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	Refresh the page.
Edit	Edit the selected tags.
Delete	Delete the selected tags.
Create new	Create a new tag.
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**. 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.*

See also:

- *Creating tags (page 359)*
- *Connecting tags (page 360)*

- *Editing tags (page 362)*
- *Searching and filtering in the QMC (page 29)*

Tags properties

The following property groups are available for tags.

Identification

The property group **Identification** contains the basic tag properties in the Qlik Sense system.

Property	Description
Name	The name of the QMC 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 apps that the tag is connected to.
App objects	The app objects that the tag is connected to.
Security rules	The security rules that the tag is connected to.
Extensions	The extensions that the tag is connected to.
Content libraries	The content libraries that the tag is connected to.
Data connections	The data connections that the tag is connected to.
Nodes	The nodes that the tag is connected to.
Engines	The engines that the tag is connected to.
Proxies	The proxies that the tag is connected to.
Virtual proxies	The virtual proxies that the tag is connected to.
Repositories	The repositories that the tag is connected to.
Schedulers	The schedulers that the tag is connected to.
Streams	The streams that the tag is connected to.
Users	The users that the tag is connected to.
User directory connectors	The user directories that the tag is connected to.
Reload tasks	The reload tasks that the tag is connected to.
User synchronization tasks	The user synchronization tasks that the tag is connected to.

See also:

Connecting tags (page 360)

2.14 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, Local Users, and ODBC.

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.

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

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

Status	The status of the user directory connector: • **Idle**: When no synchronization is performed. • **External fetch**: The first phase of the synchronization, when fetching the data from the directory service. • **Database store**: The second phase of the synchronization, when storing the data in the QRS. *If the status is displayed as **Idle** and **Last started** is more recent than **Last finished** the synchronization has failed.*
Last started sync	The date and time when synchronization of user data last started. The synchronization is either triggered by a task or started manually from the user directory connectors overview.
Last successfully finished sync	The date and time when synchronization of user data last finished successfully.
Tags	The names of the connected QMC tags.
Fetch user data on first access, then keep in sync	Status values: **Yes** or **No**. Yes is displayed when this option is selected. • When selected, only the existing users are synchronized. An existing user is a user who has logged in to Qlik Sense and/or been previously synchronized from the configured directory service. • When not selected, all the users, defined by the properties for the UDC, are synchronized from the configured directory service. You can create a filter to **Active Directory** or **Generic LDAP** if you only want to synchronize a selection of users.
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. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	Refresh the page. *If you have added a new user directory connector type you need to press F5 to refresh the list of available user directory connectors.*
Edit	Edit the selected user directory connector.
Delete	Delete the selected user directory connector.
Sync	Synchronize the user data via the selected user directory connectors.
Create new	Click to create a new user directory connector.
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**. 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.*

See also:

- *Setting up a user directory connector and schedule by task (page 238)*
- *Creating a user directory connector (page 243)*
- *Editing user directory connector (page 248)*
- *Synchronizing with user directories (page 254)*
- *Editing user sync task (page 266)*
- *Searching and filtering in the QMC (page 29)*
- *Connecting tags (page 360)*

User directory connectors Generic LDAP properties

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

Identification

The **Identification** property group contains the basic UDC properties in the Qlik Sense system.

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

The **User sync settings** property group contains the user sync properties for the user directory connector.

Property	Description	Default value
Fetch user data on first access, then keep in sync	• 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** or **Generic LDAP** if you only want to synchronize a selection of users.	Selected

Connection

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

Property	Description	Default value
User directory name *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 AD domain. To support SSL, specify the protocol as LDAPS instead.	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.	-

When a user creates an Active Directory connector that uses LDAPS, the connector will only work when that user (the creator of the UDC) is logged on to the machine and running the Qlik Sense services.
To sync users using LDAPS, you must provide user name and password.

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 AD.	-
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. *If the user synchronization is unsuccessful, try setting the value to no value.*	2000

Directory entry attributes

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

Property	Description	Default value
Type	The name of the attributes 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 name of the attributes 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 name of the attributes 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.	memberOf
Members of directory entry	The name of the attributes that holds a reference to the direct members of this directory entry. See also the **Group membership** setting, above.	member

Tags

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

Property	Description
Tags	*If no QMC tags are available, this property group is empty.* Connected QMC 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

The **Identification** property group contains the basic UDC properties in the Qlik Sense system.

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

The **User sync settings** property group contains the user sync properties for the user directory connector.

Property	Description	Default value
Fetch user data on first access, then keep in sync	• 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** or **Generic LDAP** if you only want to synchronize a selection of users.	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. To support SSL, specify the protocol as LDAPS instead.	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. *If the user synchronization is unsuccessful, try setting the value to no value.*	2000

Tags

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

User directory connectors Local network properties

The following property groups are available for user directory connectors of the type Local network:

Identification

The **Identification** property group contains the basic UDC properties in the Qlik Sense system.

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

The **User sync settings** property group contains the user sync properties for the user directory connector.

Property	Description	Default value
Fetch user data on first access, then keep in sync	• 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** or **Generic LDAP** if you only want to synchronize a selection of users.	Selected

Connection

The **Connection** property group contains the local network connection properties in the Qlik Sense system.

Property	Description	Default value
Sync all domain users	• When not selected, only the users on your local computer will be synchronized. • When selected, all users in the domain that your computer belongs to will be synchronized.	Not selected

Tags

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

User directory connectors ODBC properties

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

Identification

The **Identification** property group contains the basic UDC properties in the Qlik Sense system.

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

The **User sync settings** property group contains the user sync properties for the user directory connector.

Property	Description	Default value
Fetch user data on first access, then keep in sync	• 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** or **Generic LDAP** if you only want to synchronize a selection of users.	Selected

Connection

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

Property	Description	Default value
User directory name	The name of the user directory. Must be unique, otherwise the connector will not be configured.	-
Users table name	The name of the table containing the users.	-
Attributes table name	The name of the table containing the attributes of the users.	-
Visible connection string	The visible part of the connection string that is used to connect to the data source. *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 contains user name and password. *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

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

User directory connectors 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.

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.

2.15 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.)*

2.16 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.

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: • **(x) of (y) services are running** The number of services (x) that are running compared to the number of enabled services (y) on the node. • **(x) of (y) services are stopped** The number of services (x) that are stopped compared to the number of enabled services (y) on the node. • **(z) has stopped** The name of the service (z) that has stopped (if only one service has stopped). *Click ⓘ in the **Status** column for more detailed information on the status of the node.*
Tags	The QMC 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**. **Yes**: The Qlik Sense Engine Service (QES) is active.
Proxy	Status values: **Yes** or **No**. **Yes**: The Qlik Sense Proxy Service (QPS) is active.
Scheduler	Status values: **Yes** or **No**. **Yes**: The Qlik Sense Scheduler Service (QSS) is active.
ID	The ID of the node.
Created	The date and time when the node was created.
Last modified	The date and time when the node was last modified.
Modified by	By whom the node was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.

	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	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 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**. 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.*

See also:

- *Checking the status of Qlik Sense services (page 298)*
- *Creating node (page 309)*

- *Editing nodes (page 311)*
- *Redistributing certificate (page 313)*
- *Connecting tags (page 360)*
- *Applying a custom property value (page 358)*

Node properties

The following property groups are available for nodes.

Identification

The **Identification** property group contains the basic node properties in the Qlik Sense system.

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.

Node purpose

The **Node purpose** property group contains the basic node properties in the Qlik Sense system.

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 buttons in the Hub to create apps and the My Work section are not displayed to the user.
- 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.

Services activation

The **Services activation** property group contains the service activation properties in the Qlik Sense system.

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).
Proxy	The Qlik Sense Proxy Service (QPS).
Scheduler	The Qlik Sense Scheduler Service (QSS).

Tags

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

Custom properties

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

2.17 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: • **Running** The service is running as per normal. • **Stopped** The service has stopped. • **Disabled** The service has been disabled. *Click ⓘ in the **Status** column for more detailed information on the status.* See: *Checking the status of Qlik Sense services (page 298)*.
Tags	The QMC 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 timeout (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.
Max number of undos	The maximum number of undos when editing app content, such as sheets, objects, bookmarks, and stories: min = 0, max = 999.
Performance log interval (minutes)	The number of minutes in-between performance logging entries.
Audit activity log level	Levels: **Off** or **Basic** (a limited set of entries)
Service log level	Each level from **Error** to **Info** includes more information than the previous level.
System log level	All the standard engine messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log level	All the performance messages are saved to this logger (by default updated default every five minutes). The log contains, for example, the number of active users, the number of open sessions, and the CPU load.Each level from **Fatal** to **Debug** includes more information than the previous level.

QIX performance log level	All the QIX protocol performance messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Audit log level	More detailed, user-based messages are saved to this logger, for example, when the user makes a selection in an app. Each level from **Fatal** to **Debug** includes more information than the previous level.
Session log level	All the session messages are saved to this logger when a client session is terminated, for example, user information, machine ID, IP address and port number.Each level from **Fatal** to **Debug** includes more information than the previous level.
Traffic log level	All the traffic messages are saved to this logger, for example, all JSON-messages to and from the engine.Each level from **Fatal** to **Debug** includes more information than the previous level.
Allow data lineage	Status values: **Yes** or **No**. The data lineage is the origin of the data that is loaded into Qlik Sense).
Min memory usage (%)	The minimum memory capacity used by Qlik Sense.
Max memory usage (%)	The maximum memory capacity used by Qlik Sense.
CPU throttle (%)	The amount of CPU capacity used by Qlik Sense. Range: 0 - 100%
Standard mode	Status values: **Yes**: standard mode. **No**: legacy mode. For security reasons, Qlik Sense in standard mode does not support absolute or relative paths in the data load script or functions and variables that expose the file system. *Disabling standard mode can create a security risk by exposing the file system.*
ID	The ID of the engine.
Created	The date and time when the engine was created.
Last modified	The date and time when the engine was last modified.
Modified by	By whom the engine was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.

	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	Refresh the page.
Edit	Edit the selected engines.
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**. 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.*

See also:

- *Editing engine (page 347)*
- *Connecting tags (page 360)*
- *Disconnecting tags (page 361)*
- *Applying a custom property value (page 358)*

Engines properties

The following property groups are available for engines:

Identification

The **Identification** property group contains the basic engine properties in the Qlik Sense system.

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

Apps

The **Apps** property group contains engine properties in the Qlik Sense system.

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 timeout (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
Working folder	A scheduled reload will search for files in this directory when relative paths are used to define file location.	%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

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

Property	Description	Default value
Listen ports	The listen port used by Qlik Sense Engine Service (QES) for communication with the Qlik Sense web clients. 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.	Selected
Min memory usage (%)	The minimum memory capacity used by Qlik Sense.	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: • **Hard max limit**: never use more memory than defined by the property above. • **Ignore max limit**: use as much memory as necessary, regardless of the **Max memory usage (%)** setting. • **Soft max limit**: use more memory than defined by the**Max memory usage (%)** setting, if necessary and available.	Hard max limit
CPU throttle (%)	The amount of CPU capacity used by Qlik Sense. Range: 0 – 100 %	0 (that is, no throttling)
Standard mode	When selected, standard mode is used. If cleared, legacy mode is used. For security reasons, Qlik Sense in standard mode does not support absolute or relative paths in the data load script or functions and variables that expose the file system. *Disabling standard mode can create a security risk by exposing the file system.*	Selected

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: • **Off**: no entries • **Basic**: a limited set of entries	Basic
Service log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Error**: only error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries	Info

Tracing

Performance log interval (minutes)	The number of minutes in-between performance logging entries.	5
System log level	All the standard engine messages are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

Performance log level	All the performance messages are saved to this logger (by default updated default every five minutes). The log contains, for example, the number of active users, the number of open sessions, and the CPU load. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
QIX performance log level	All the QIX protocol performance messages are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Off

Audit log level	More detailed, user based, messages are saved to this logger, for example, when the user makes a selection in an app. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Off
Session log level	All the session messages are saved to this logger when a client session is terminated, for example, user information, machine ID, IP address and port number. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

Traffic log level	All the traffic messages are saved to this logger, for example, all JSON-messages to and from the engine. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Off

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

Tags

The **Tags** property group contains the available tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

2.18 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: • **Running** The service is running as per normal. • **Stopped** The service has stopped. • **Disabled** The service has been disabled. *Click in the **Status** column for more detailed information on the status.* See: *Checking the status of Qlik Sense services (page 298)*.
Tags	The QMC tags that are connected to the proxy.
Service listen port HTTPS (default)	The secure listen port for the proxy, which by default manages all Qlik Sense communication. *Make sure that port 443 is available for the Qlik Sense Proxy Service (QPS) to use because the port is sometimes used by other software, for example, web servers.*
Allow HTTP	Status values: **Yes** or **No**. **Yes**: Unencrypted communication is allowed. This means that both https (secure communication) and (http) unencrypted communication is allowed.
Service listen port HTTP	The unencrypted listen port, used when HTTP connection is allowed.
Authentication listen port HTTPS (default)	The secure listen port for the default (internal) authentication module.

Kerberos authentication	Status values: **Yes** or **No**. **Yes**: Kerberos authentication is enabled.
Authentication listen port HTTP	The unencrypted authentication listen port, used when HTTP connection is allowed.
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.
Keep-alive timeout (seconds)	The maximum timeout period for a single HTTP request before closing the connection. Protection against denial-of-service attacks. This means that if an ongoing request exceeds this period, Qlik Sense proxy will close the connection. Increase this value if your users work over slow connections and experience closed connections.
Max header size (bytes)	The maximum total header size.
Max header lines	The maximum number of lines in the header.
Audit activity log level	Levels: **Off** or **Basic** (a limited set of entries)
Audit security log level	Levels: **Off** or **Basic** (a limited set of entries)
Service log level	Each level from **Error** to **Info** includes more information than the previous level.
Audit log level	More detailed, user-based messages are saved to this logger, for example, proxy calls. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log level	All the performance messages are saved to this logger. For example, performance counters and number of connections, streams, sessions, tickets, web sockets and load balancing information. Each level from **Fatal** to **Debug** includes more information than the previous level.
Security log level	All the certificates messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
System log level	All the standard proxy messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log interval (minutes)	The interval of performance logging.

REST API listen port	The listen port for the proxy API.
ID	The ID of the proxy.
Created	The date and time when the proxy was created.
Last modified	The date and time when the proxy was last modified.
Modified by	By whom the proxy was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.
	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	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 items**. 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.*

See also:

- *Editing proxies (page 314)*
- *Creating virtual proxy (page 324)*
- *Adding load balancing (page 321)*
- *Connecting tags (page 360)*
- *Applying a custom property value (page 358)*

Proxies properties

The following property groups are available for proxies.

Identification

The **Identification** property group contains the basic proxy properties in the Qlik Sense system.

All fields are mandatory and must not be empty.

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

Ports

The **Ports** property group contains the proxy ports properties in the Qlik Sense system.

Property	Description	Default value
Service listen port HTTPS (default)	The secure listen port for the proxy, which by default manages all Qlik Sense communication. *Make sure that port 443 is available for the Qlik Sense Proxy Service (QPS) to use because the port is sometimes used by other software, for example, web servers.*	443
Authentication listen port HTTPS (default)	The secure listen port for the default (internal) authentication module.	4244
Kerberos authentication	Select to enable Kerberos authentication.	Not selected
REST API listen port	The listen port for the proxy API.	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 is allowed. Then the QMC address is *https://<QPS server name>:Service listen port HTTP/qmc* (where *https* can be replaced by *http*). By default the QMC address is *https://<QPS server name>/qmc*. *If you change the property **Allow HTTP**, please know that all web browser bookmarks (that Qlik Sense users or QMC admin users have created) will not be valid anymore.* *The **Service listen port HTTP** and **Authentication listen port HTTP** need to be set when **Allow HTTP** is checked.*	False (not allowed)
Service listen port HTTP	The unencrypted listen port, used when HTTP connection is allowed.	80
Authentication listen port HTTP	The unencrypted authentication listen port, used when HTTP connection is allowed.	4248

Advanced

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

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

Tracing

Performance log interval (minutes)	The interval of performance logging.	5 minutes
Audit log level	More detailed, user-based messages are saved to this logger, for example, proxy calls. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
Performance log level	All the performance messages are saved to this logger. For example, performance counters and number of connections, streams, sessions, tickets, web sockets and load balancing information. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

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

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

Security

The **Security** property group contains the proxy security properties in the Qlik Sense system.

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. *To be valid, the certificate must contain a private key.*

Tags

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

Custom properties

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

Proxies 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: *https://[node/[prefix]/*

Property	Description
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. *It can be useful to include the value 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.

2.19 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.
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. • **Header authentication static user directory**: allows static header authentication, where the user directory is set in the QMC. • **Header authentication dynamic user directory**: allows dynamic header authentication, where the user directory is fetched from the header. • **SAML**: SAML2 is used for authentication.
Linked to proxy service	Status values: **Yes** or **No**.
Tags	The QMC 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: • **No anonymous user** • **Allow anonymous user** • **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: `company.com`

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

Session inactivity timeout (minutes)	The maximum period of time with inactivity before timeout. After this, the session is invalid and the user is logged out from the system.
Extended security environment	Status values: **Yes** or **No**. **Yes**: The following information about the client environment is sent in the security header: OS, device, browser, and IP. **No**: The user can run the same engine session simultaneously on multiple devices.
SAML Metadata IdP	The metadata from the IdP, used to configure the service provider. Must exist for SAML authentication to work.
SAML entity ID	ID to identify the service provider. The ID must be unique.

SAML attribute for user ID	The SAML attribute name for the attribute describing the user ID.
SAML attribute for user directory	The SAML attribute name for the attribute describing the user directory.
ID	The ID of the virtual proxy.
Created	The date and time when the virtual proxy was created.
Last modified	The date and time when the virtual proxy was last modified.
Modified by	By whom the virtual proxy was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.
	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	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 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**. 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.*

See also:

- *Editing proxies (page 314)*
- *Creating virtual proxy (page 324)*
- *Editing virtual proxy (page 331)*
- *Adding load balancing (page 321)*
- *Connecting tags (page 360)*
- *Applying a custom property value (page 358)*

Virtual proxies properties

The following property groups are available for virtual proxies.

Identification

The **Identification** property group contains the basic virtual proxy properties in the Qlik Sense system.

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. Example: *https://[node]/[prefix]/* You can only use characters that can be part of a URI path. You can use slashes (/), but the prefix cannot begin nor end with a slash. Hash signs (#) cannot be used. Uniform Resource Identifier (URI): Generic Syntax	Blank
Session inactivity timeout (minutes)	The maximum period of time with inactivity before timeout. After this, the session is invalid and the user is logged out from the system.	30 minutes
Session cookie header name	The name of the HTTP header used for the session cookie. This value is blank by default and you must enter a value. *It can be useful to include the value of the **Prefix** property above as a suffix in the cookie name.*	Blank

Authentication

The **Authentication** property group contains the authentication method properties for the virtual proxies in the Qlik Sense system.

Property	Description	Default value
Anonymous access mode	How to handle anonymous access: • **No anonymous user** • **Allow anonymous user** • **Always anonymous user**	No anonymous user

Property	Description	Default value
Authentication method	• **Ticket**: a ticket is used for authentication. • **Header authentication static user directory**: allows static header authentication, where the user directory is set in the QMC. • **Header authentication dynamic user directory**: allows dynamic header authentication, where the user directory is fetched from the header. • **SAML**: SAML2 is used for authentication.	Ticket
Header authentication header name	The name of the HTTP header that identifies users, when header authentication is allowed. Mandatory if you allow header authentication (by selecting either **Header authentication static user directory** or **Header authentication dynamic user directory** for the **Authentication method** property). *Header authentication only supports US-ASCII (UTF-8 is not supported).*	Blank
Header authentication static user directory	The name of the user directory where additional information can be fetched for header authenticated users. Mandatory if you allow static header authentication (by selecting **Header authentication static user directory** for the **Authentication method** property).	Blank

Property	Description	Default value
Header authentication dynamic user directory	Mandatory if you allow dynamic header authentication (by selecting **Header authentication dynamic user directory** for the **Authentication method** property). The pattern you supply must contain '$ud', '$id' and a way to separate them. **Example setting and matching header:** `$ud\\$id` – matches USERDIRECTORY\userid (backslashes must be escaped with an additional \) `$id@$ud` – matches userid@USERDIRECTORY ($id and $ud can be in any order) `$ud:::$id` – matches USERDIRECTORY:::userid	Blank
Windows authentication pattern	The chosen authentication pattern for logging in. If the User-Agent header contains the Windows authentication pattern string, Windows authentication is used. If there is no matching string, form authentication is used.	Windows
Authentication module redirect URI	When using an external authentication module, the clients are redirected to this URI for authentication.	Blank (default module, that is Windows authentication Kerberos/NTLM)

Property	Description	Default value
SAML host URI	The server name that is exposed to the client. This name is used by the client for accessing Qlik services, such as the QMC. The server name does not have to be the same as the machine name, but in most cases it is. You can use either http:// or https:// in the URI. To be able to use http://, you must select **Allow HTTP** on the edit page of the proxy that the virtual proxy is linked to. Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property).	Blank
SAML entity ID	ID to identify the service provider. The ID must be unique. Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property).	Blank
SAML metadata IdP	The metadata from the IdP is used to configure the service provider, and is essential for the SAML authentication to work. A common way of obtaining the metadata is to download it from the IdP website. Click the browse button and open the IdP metadata .xml file for upload. To avoid errors, you can click **View content** and verify that the file has the correct content and format. The configuration is incomplete without metadata.	

Property	Description	Default value
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. See: *I do not know the name of a mandatory SAML attribute (page 459)*	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'. See: *I do not know the name of a mandatory SAML attribute (page 459)*	Blank
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'.	

Load balancing

The **Load balancing** property group contains the load balancing properties for the virtual proxies in the Qlik Sense system.

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

Advanced

The **Advanced** property group contains the advanced properties for the virtual proxies in the Qlik Sense system.

Property	Description	Default value
Extended security environment	Enabling this setting will send the following information about the client environment in the security header: OS, device, browser, and IP. If not selected, the user can run the same engine session simultaneously on multiple devices.	Blank
Session cookie domain	By default the session cookie is valid only for the machine that the proxy is installed on. This (optional) property allows you to increase its validity to a larger domain. Example: `company.com`	Blank (default machine)

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

Websocket origin 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.	Blank

Integration

The **Integration** property group contains the integration properties for the virtual proxies in the Qlik Sense system.

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)

Tags

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

Custom properties

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

Virtual proxies 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: • **Running** The service is running as per normal. • **Stopped** The service has stopped. • **Disabled** The service has been disabled. *Click ⓘ in the **Status** column for more detailed information on the status.* See: *Checking the status of Qlik Sense services (page 298)*.

Service listen port HTTPS (default)	The secure listen port for the proxy, which by default manages all Qlik Sense communication. *Make sure that port 443 is available for the Qlik Sense Proxy Service (QPS) to use because the port is sometimes used by other software, for example, web servers.*
Allow HTTP	Status values: **Yes** or **No**. **Yes**: Unencrypted communication is allowed. This means that both https (secure communication) and (http) unencrypted communication is allowed.
Service listen port HTTP	The unencrypted listen port, used when HTTP connection is allowed.
Authentication listen port HTTPS (default)	The secure listen port for the default (internal) authentication module.
Kerberos authentication	Status values: **Yes** or **No**. **Yes**: Kerberos authentication is enabled.
Authentication listen port HTTP	The unencrypted authentication listen port, used when HTTP connection is allowed.
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.
Keep-alive timeout (seconds)	The maximum timeout period for a single HTTP request before closing the connection. Protection against denial-of-service attacks. This means that if an ongoing request exceeds this period, Qlik Sense proxy will close the connection. Increase this value if your users work over slow connections and experience closed connections.
Max header size (bytes)	The maximum total header size.
Max header lines	The maximum number of lines in the header.
Audit activity log level	Levels: **Off** or **Basic** (a limited set of entries)
Audit security log level	Levels: **Off** or **Basic** (a limited set of entries)

Service log level	Each level from **Error** to **Info** includes more information than the previous level.
Audit log level	More detailed, user-based messages are saved to this logger, for example, proxy calls. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log level	All the performance messages are saved to this logger. For example, performance counters and number of connections, streams, sessions, tickets, web sockets and load balancing information. Each level from **Fatal** to **Debug** includes more information than the previous level.
Security log level	All the certificates messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
System log level	All the standard proxy messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log interval (minutes)	The interval of performance logging.
REST API listen port	The listen port for the proxy API.
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.
	You can combine filtering with searching. *Searching and filtering in the QMC (page 29)*
Edit	Click **Edit** in the action bar and edit the selected proxy.
Unlink	Click to unlink a proxy service from the selected proxy. *A virtual proxy must be linked to a proxy service in order to work.*
Link	Click to 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.*

See also:

- *Editing proxies (page 314)*
- *Creating virtual proxy (page 324)*
- *Editing virtual proxy (page 331)*
- *Adding load balancing (page 321)*
- *Connecting tags (page 360)*
- *Applying a custom property value (page 358)*

2.20 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: • **Running** The service is running as per normal. • **Stopped** The service has stopped. • **Disabled** The service has been disabled. *Click ⓘ in the **Status** column for more detailed information on the status.* See: *Checking the status of Qlik Sense services (page 298)*.

Tags	The QMC tags that are connected to the scheduler.
Type	• **Master**: sends the task to a slave QSS within the site. • **Slave**: receives the task from the master QSS and executes the task. • **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. Levels: **Off** or **Basic** (a limited set of entries)
Service log level	Each level from **Error** to **Info** includes more information than the previous level.
Application log level	All the application messages for the scheduler service are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Audit log level	Detailed, user-based messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log level	All the performance messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Security log level	Security-related messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
System log level	All the standard scheduler messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Task execution log level	All the task execution messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
ID	The ID of the scheduler.
Created	The date and time when the scheduler was created.
Last modified	The date and time when the scheduler was last modified.

Modified by	By whom the scheduler was modified.
<Custom properties>	Custom properties, if any, are listed here.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.
	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	Refresh the page.
Edit	Edit the selected scheduler.
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**. 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.*

See also:

- *Editing scheduler (page 341)*
- *Connecting tags (page 360)*

Applying a custom property value (page 358)

Scheduler properties

The following property groups are available for schedulers:

Identification

The **Identification** property group contains the basic scheduler properties in the Qlik Sense system.

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: • **Off**: no entries • **Basic**: a limited set of entries	Basic
Service log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Error**: only error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries	Info

Tracing

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

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

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

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

Advanced

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

Property	Description	Default value
Type	If enabled by the property above, the QSS type is set to: • Master: sends the task to a slave QSS within the site. • Slave: receives the task from the master QSS and executes the task. • 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
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

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

Custom properties

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

2.21 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. The QRS also manages the synchronization in multi-node Qlik Sense sites. 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: • **Running** The service is running as per normal. • **Stopped** The service has stopped. • **Disabled** The service has been disabled. > *Click ⓘ in the **Status** column for more detailed information on the status.* See: *Checking the status of Qlik Sense services (page 298)*.
Audit activity log level	Levels: **Off** or **Basic** (a limited set of entries)
Audit security log level	Levels: **Off** or **Basic** (a limited set of entries)
Service log level	Each level from **Error** to **Info** includes more information than the previous level.
Application log level	All the application messages for the repository service are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Audit log level	Detailed, user-based messages are saved to this logger, for example, security rules information. Each level from **Fatal** to **Debug** includes more information than the previous level.

License log level	All the license messages are saved to this logger. For example, token usage and user access allocation. Levels: **Info** or **Debug**
Qlik Management Console (QMC) log level	All the QMC messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log level	All the performance messages for the repository service are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Security log level	All the certificates messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Synchronization log level	All the synchronization information in a multi-node environment are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
System log level	All the standard repository messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
User management log level	All the user sync messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Tags	The QMC 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. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*

Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	Refresh the page.
Edit	Edit the selected repository.
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**. 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.*

See also:

- *Editing repository (page 302)*
- *Connecting tags (page 360)*
- *Applying a custom property value (page 358)*

Repository properties

The following property groups are available for repositories.

Identification

The **Identification** property group contains the basic repository properties in the Qlik Sense system.

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

Tracing

Application log level	All the application messages for the repository service are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
Audit log level	Detailed, user-based messages are saved to this logger, for example, security rules information. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

License log level	All the license messages are saved to this logger. For example, token usage and user access allocation. Use the drop-down to set the verbosity of the logger: • **Info**: fatal, error, warning, and information entries • **Debug**: same as info, but including also debug entries	Info
Qlik Management Console (QMC) log level	All the QMC messages are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
Performance log level	All the performance messages for the repository service are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

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

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

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

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

Tags

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

Custom properties

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

2.22 Sync rules

The **Sync rules** overview lists all the available sync 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 QMC tags that are connected to the sync rule.
Conditions	The conditions of the sync rule.
ID	The ID of the sync rule.
Created	The date and time when the sync rule was created.

Last modified	The date and time when the sync rule was last modified.
Modified by	By whom the sync rule was modified.
▼ ▲	Sort the list ascending or descending. Some columns do not support sorting.
	Type a string to filter on, or, when available, select a predefined value. All rows that match your filter criteria are displayed. You can filter on multiple columns simultaneously to narrow your search. If a filter is applied to a column, is displayed. To remove your criteria, click **Actions** in the table header bar and select **Clear filters and search**. You can combine filtering with searching. See: *Searching and filtering in the QMC (page 29)*
Actions	Options for clearing filter and search, and selecting or deselecting all rows. *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. See: *Searching and filtering in the QMC (page 29)*
	Refresh the page.
Edit	Edit the selected sync rule. When you do not have update rights for the selected items, **Edit** is replaced by **View**.
View	View the selected sync rule. When you do not have update rights for the selected items, **Edit** is replaced by **View**.
Delete	Delete the selected sync rules. If you do not have delete rights for the selected items, **Delete** is disabled.
Create new	Create a new sync rule.
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**. 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.*

See also:

- *Getting to know the sync rules edit page (page 383)*
- *Creating sync rules (page 383)*
- *Previewing how sync rules affect node privileges (page 385)*
- *Editing sync rules (page 387)*
- *Creating sync rules with custom properties (page 389)*
- *Connecting tags (page 360)*

Sync rules properties

The following property groups are available for sync rules.

Identification

The following **Identification** property groups are available.

Name

Property name	Explanation
Name	The name of the rule.

Disabled

Property	Description
Disabled	Select to disable a sync rule.

Description

Property	Description
Description	A text describing what the rule does.

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 sync 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**. You can also use pre-defined functions for conditions to return property values. See *Security rule conventions (page 422)*.
resourcetypevalue	You must provide at least one resource type value, see *Resource filter (Advanced view) (page 181)* for available values.
property	The property name for the resource condition, see *Properties: (page 183)* for available names.
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. *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.@Geographies="Canada")`	The rule will apply to all apps with the custom property Geographies set to Canada.
`resource.resourcetype="App" and !(resource.@Geographies="Canada")`	The rule will apply to all nodes except the nodes with custom property Geographies set to Canada.
With **Resource filter=*** and Conditions field empty	This rule will apply to all resources and all users.

See also:

- *Conditions (Basic view) (page 185)*
- *Operators and functions for conditions (page 426)*

Writing security rules (page 421)

Context (Advanced view)

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

Actions (Basic view)

The sync rule action is always defined as **Sync**.

Resource filter templates (Basic view)

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.

Conditions (Basic view)

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.

See also:

- *Conditions (Advanced view) (page 76)*

Tags

Property	Description
Tags	The available QMC tags are listed to the right. Connected QMC tags are listed to the left.

Sync rules associated items

The following associated items are available for sync rules:

Preview

Preview is available from **Associated items** when you edit sync rules. The preview page shows you a preview of the effects that your rules will have when you apply them.

2.23 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.

See also:

Exporting certificates (page 382)

3 Managing QMC resources

The administration of a Qlik Sense environment includes managing and handling the following:

- License and tokens
- 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 license and tokens

License and tokens

The License Enabling File (LEF) determines the number of tokens available for a Qlik Sense site. You must activate the Qlik Sense site license to get the tokens. Allocate the tokens to the different access types to give the users access to the hub and apps.

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 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.

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.

See also:

- *Allocating user access (page 255)*
- *Deallocating user access (page 255)*
- *Reinstating user access (page 256)*
- *Creating login access (page 256)*
- *Deleting login access (page 260)*

Activating license

The first time you start the Qlik Management Console (QMC), the **Site license properties** page is displayed. All fields are empty and you must enter the license information from the License Enabling 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.
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 SenseLEF 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.

   > ***Failed to apply changes*** *is displayed if any value is incorrect.*

4. Click **OK** to close the dialog.

You have now activated the license and made the tokens available. Next you need to allocate user access to yourself (the preferred access type).

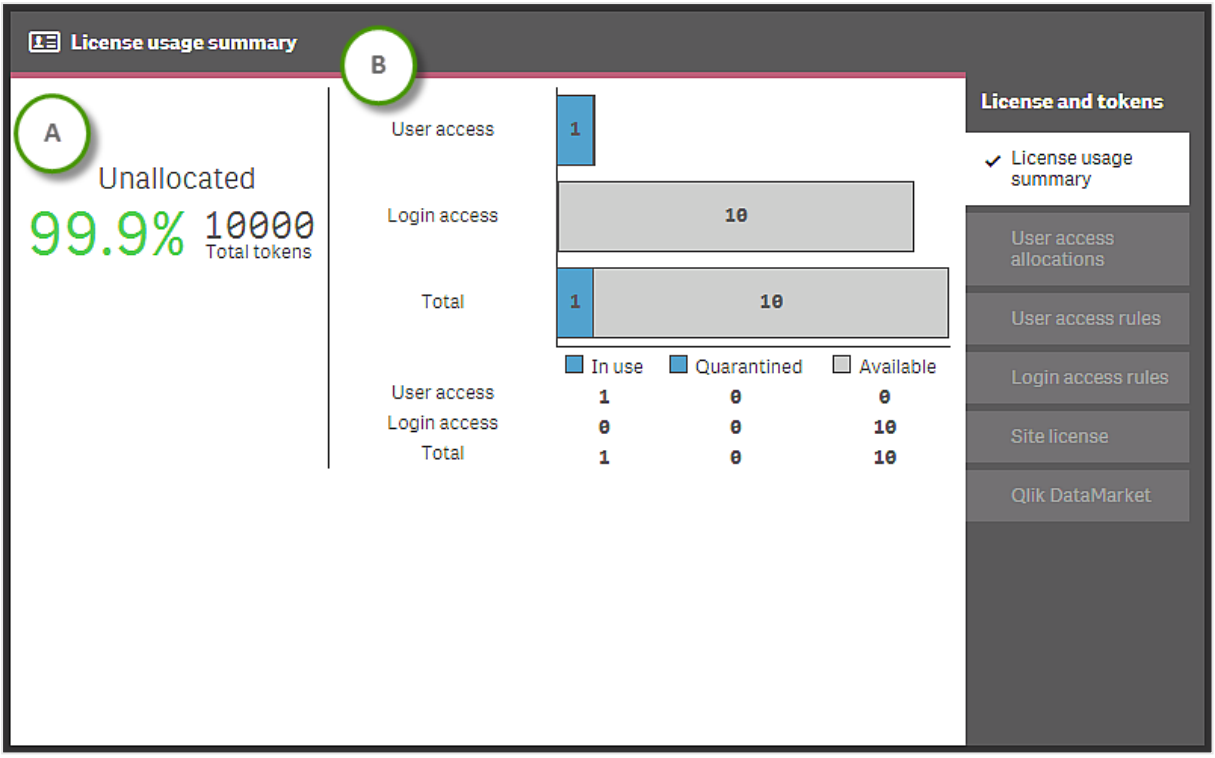
> *You give users access to Qlik Sense by managing the access types: user access or login access, according to which consumption model you prefer for accessing Qlik Sense.*

See also:

- *License and tokens (page 95)*
- *Allocating user access (page 255)*
- *Creating login access (page 256)*

Getting to know the license usage summary page

The **License usage summary** overview shows the token availability and how the tokens are distributed between the different access types. You cannot adjust the token usage from this page. The number of tokens is determined by the license for the Qlik Sense site.



Section (A) shows the amount of unallocated tokens (in percent) and the total number of tokens.

Section (B) shows the access distribution:

- **User access**: the number of tokens that has been allocated to identified users.
- **Login access**: the number of tokens that has been allocated to login access groups.
- **Total**: the sum of the two above.

Status

- **In use**: the number of allocated tokens that are currently in use.
- **Quarantined**: the number of tokens that will be unallocated 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.*

See also:

- *User access allocations (page 96)*
- *Login access rules (page 102)*
- *Site license (page 106)*

Changing license

The license properties can be changed after they have been set for the first time. Updating the LEF 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 and tokens** 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 SenseLEF 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.*

You have now changed the license properties and the number of tokens are updated accordingly.

See also:

- *User access allocations (page 96)*

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 and tokens** 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 **Essential package**. The option **Free** gives you access to a limited data set. The option **Essential package** requires a license and a License Enabling 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 **Essential package**, 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 DataMarket product 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 SenseLEF 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.

You have now activated the license.

See also:

Changing the Qlik DataMarket license (page 193)

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 **Essential package** subscription, or to update the license details, you need to enter the license details and add the License Enabling File (LEF).

Do the following:

1. Select **License and tokens** 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 DataMarket product 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 SenseLEF 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.

You have now changed the license properties.

3.2 Managing apps

You can create an app from the Qlik Sense hub, if you have the appropriate access rights. Apps are published to streams from the QMC, which is a part of Qlik Sense. To publish an app that is created 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.

You can only publish apps that are unpublished:

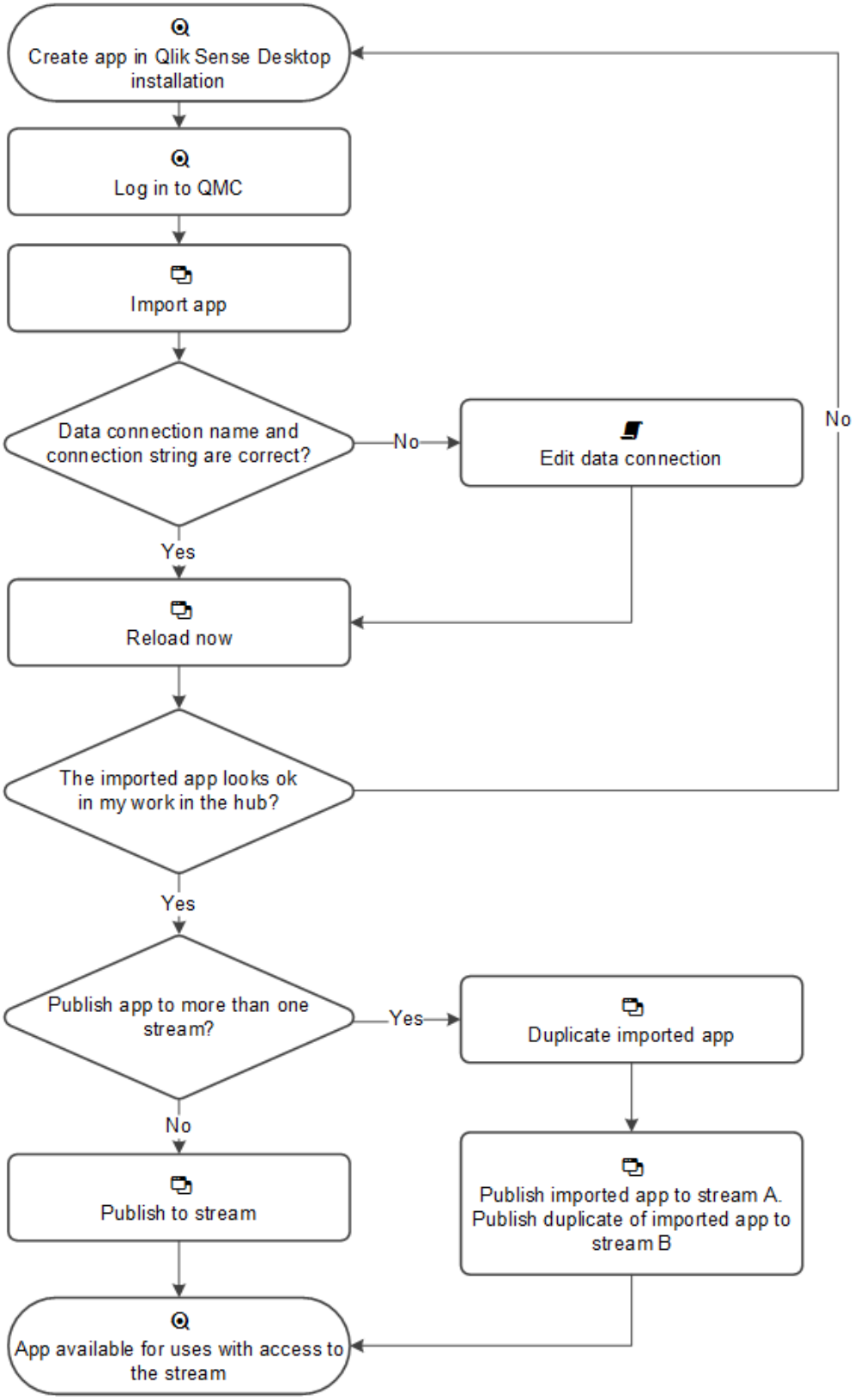
- To publish an app to more than one stream, you must first create a duplicate of the app..
- To republish an app, create a duplicate of the published app, edit the duplicate and publish it.Use the option **Replace existing** to replace a published app.

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 My work 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.*

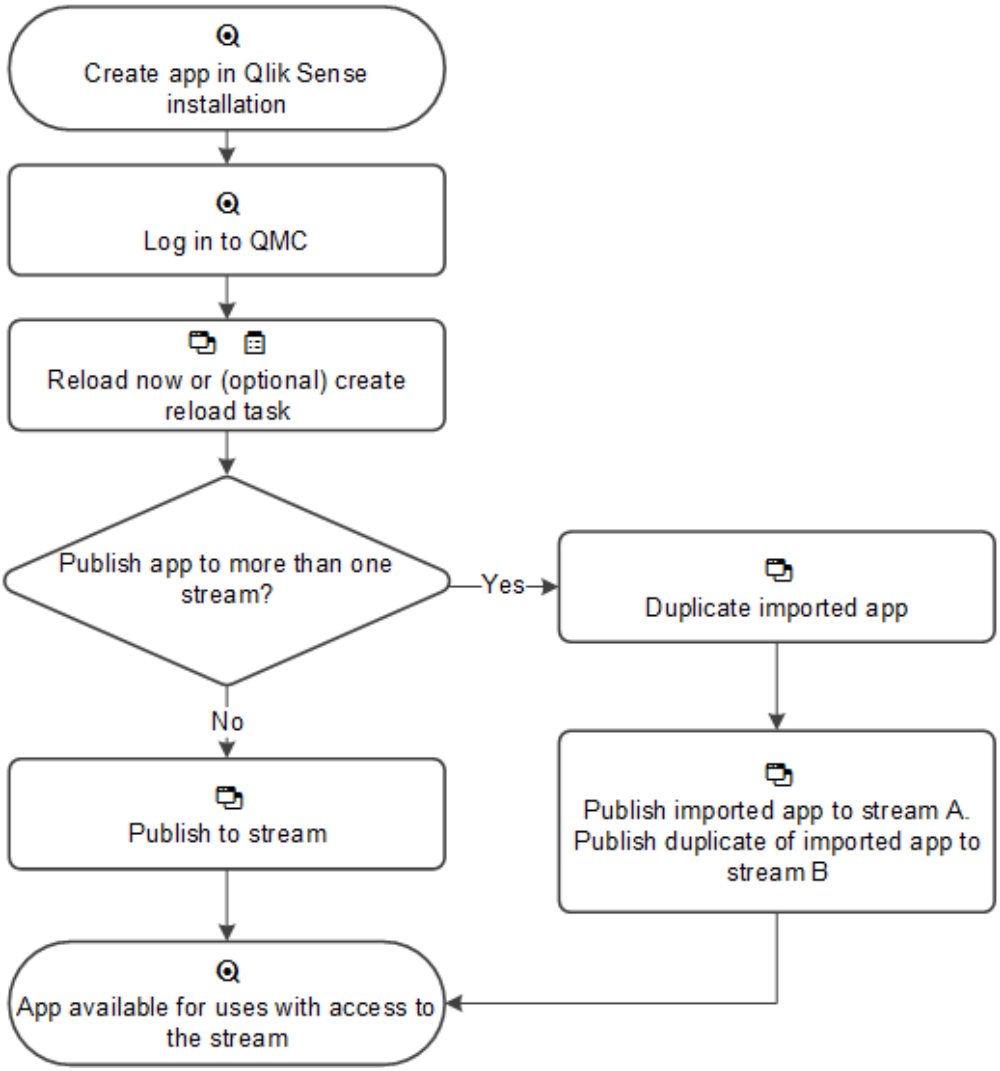
Workflow: Apps developed on aQlik Sense Desktopinstallation

This 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
No
Yes
Reload now
The imported app looks ok in my work in the hub?
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 uses with access to the stream

Workflow: Apps developed on Qlik Sense in a server deployment

This workflow illustrates publishing an app in a Qlik Sense installation:



See also:

- *Editing streams (page 228)*
- *Editing data connections (page 232)*
- *Reloading apps manually (page 217)*
- *Publishing apps (page 201)*
- *Duplicating apps (page 204)*
- *Republishing apps (page 203)*

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**.

   > *There is a maximum limit for simultaneous transports, and if the maximum is reached an error message is displayed.*

   The browse dialog closes and the name of the qvf file is displayed in the **App name** field in the **Import app** dialog.
   If you want to change the name of the app, edit the **App name** field. If the **App name** is not unique, a message is displayed with information on how many apps 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. **Duration** shows you how long the import has been ongoing.
   - Click ⊗ if you want to cancel the import.
     ⚠ and **Aborted** is displayed and the import stops.
   - Click **OK** if you want 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.

You now have imported an app.

Moving apps with ODBC data connections

If you move an app between Qlik Sense sites/Qlik Sense Desktop installations, data connections are included. If the app contains ODBC data connections, you need to make sure that the related ODBC data sources exist on the new deployment as well. The ODBC data sources need to be named and configured

identically, and point to the same databases or files.

See also:

Managing apps (page 194)

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 0.95 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 four status values can be displayed when migrating an app:

- Successful
- Ongoing
- Pending
- Migration failed

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.

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**.
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.

See also:

Importing apps (page 197)

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..

   You can filter a column by using the filtering option: .

2. Select the app or 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.

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

   The **Identification** property group contains the identification information for the for the selected apps.

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.

   The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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.

You have now edited an app or apps.

See also:

- *Resource edit page (page 28)*
- *Apps associated items (page 39)*

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.

   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 have now deleted the apps.

Publishing apps

You can create an app from the Qlik Sense hub, if you have the appropriate access rights. Apps are published to streams from the QMC, which is a part of Qlik Sense. To publish an app that is created 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.

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** 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.

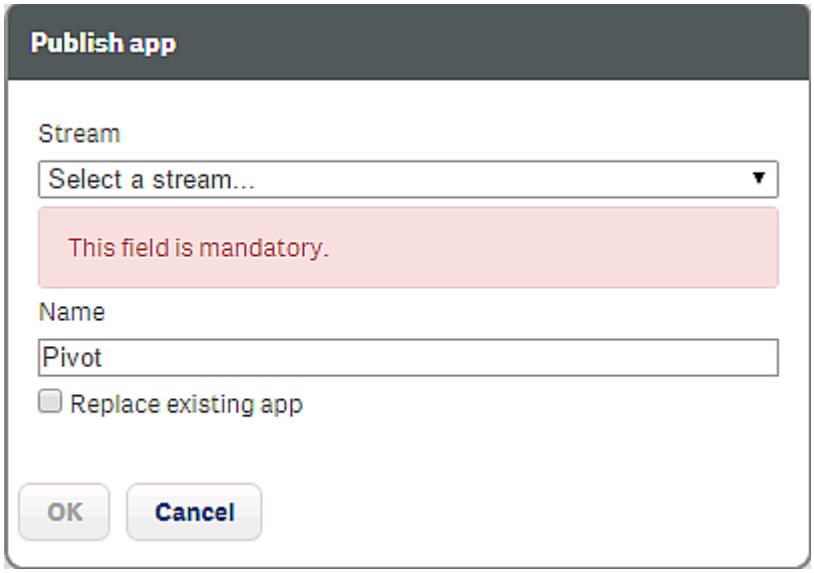
   You can filter a column by using the filtering option: .

2. Select the app or 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.

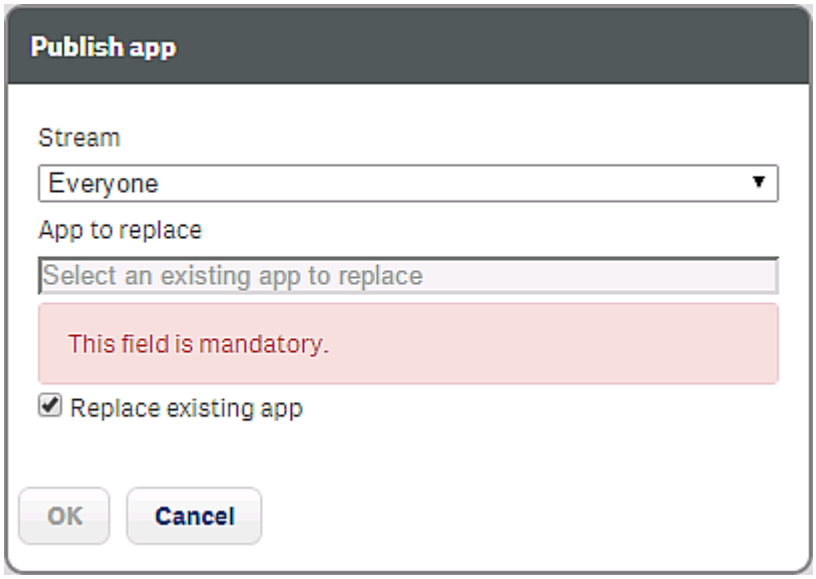
   *The **Publish** button is not displayed if you do not have access to any streams.*

   A dialog window opens.
4. In the **Publish app** dialog:
   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**.



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



A dialog opens.

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

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.

You have now published an app (or several apps) to a stream.

See also:

- *Importing apps (page 197)*
- *Duplicating apps (page 204)*
- *Managing apps (page 194)*
- *Republishing apps (page 203)*

Republishing apps

To republish an app, create a duplicate of the published app, edit the duplicate and publish it.

Do the following:

1. Select **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 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** to replace a published app.

See also:

- *Publishing apps (page 201)*

Replacing apps

You can choose to replace a published app when you publish an app. To do this you use the option **Replace existing** when you publish the app.

See also:

- *Publishing apps (page 201)*

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. Only published and approved content will be included in the export. The exported app is saved in the default download folder of your web browser.

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. **Duration** shows you how long the export has been ongoing. 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 logout 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 ⊗ if you want to cancel the export.
     ⚠ and **Aborted** is displayed and the export stops.
   - Click **OK** if you want to remove a failed item ⚠ .
     The item is removed from the **Ongoing transports** dialog.

   When the export and file download has 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.

You now have exported an app *qvf file* to the default download folder of your web browser.

Moving apps with ODBC data connections

If you move an app between Qlik Sense sites/Qlik Sense Desktop installations, data connections are included. If the app contains ODBC data connections, you need to make sure that the related ODBC data sources exist on the new deployment as well. The ODBC data sources need to be named and configured identically, and point to the same databases or files.

See also:

- *Managing apps (page 194)*
- *Importing apps (page 197)*

Duplicating apps

You can duplicate apps. The duplicate includes all the content that you have reading rights to. Only published and approved content 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..

   You can filter a column by using the filtering option: .

2. Select the app that you want to duplicate, click **More actions** in the far right of 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.

   When you make duplicates of an app a counter is added to the name; <name of original app>(1), <name of original app>(2), <name of original app>(3). If a duplicated app is duplicated once more another counter is added, for example <name of original app>(1)(1), <name of original app>(1)(2), <name of original app>(1)(3).

You have now duplicated an app.

Creating reload tasks

You can create a reload task to 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..

   You can filter a column by using the filtering option: .

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 **Reload task edit** page is displayed.
3. Edit the properties.

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

a. You can change the task name in the **Name** field. By default the name is *Reloadtask of <App name >*.

b. **App name** displays the app you selected from the overview. You can change which app you are creating the task for by clicking the **App name** 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 of selected type 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.

   Clicking undo ↩ in the **Triggers** heading applies to all triggers you are currently editing.

e. Optionally, apply QMC tags.

f. Optionally, apply custom properties.

The **Identification** property group contains the basic reload task properties in the Qlik Sense system. 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>

The **Execution** property group contains the reload task execution properties in the Qlik Sense system.

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

The following properties are available for a scheduled trigger.

Property	Description
Name	The name of the trigger. Mandatory.
Type	The trigger type.
Enabled	The trigger is enabled when selected.
Start	Select when the trigger takes effect by typing the following values: • **Time to start (hh:mm)** and • **Start date (YYYY-MM-DD)**

Property	Description

Schedule	Set the trigger schedule:
	• **Once**.
	• **Hourly**. Set the time period between the executions of the trigger. Edit **Repeat after each** by typing the values for:
	  • **hour(s)** (default is 1)
	  • **minute(s)** (default is 0)
	• **Daily**. Set the time between the executions of the trigger by typing a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	• **Weekly**. Set the time between the executions of the trigger:
	  • Type a value for **Every week(s)** (default is 1) and
	  • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	  *If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*

End	Type values for the following: • **Time to end (hh:mm)** • **End date (YYYY-MM-DD)** Select **Infinite** to create a never ending trigger.

The following properties are available for a task event trigger.

Property	Description
Name	The name of the trigger. Mandatory.
Type	The trigger type.
Enabled	The trigger is enabled when selected.

Property	Description
Time constraint	Defines the time period (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. See: *Creating a task chain (page 286)*
Add task **Task successful** or **Task failed**	Do the following: a. Click **Add task** to add a tasks that will function as a trigger condition. A drop-down list and an empty field is added. b. Click the empty field to add a task. The dialog **Double-click to select** is opened and displays a list of tasks with the following columns: **App name**, **Tags** connected to the task, and **Name**, which is the task name. Click a column heading to sort that column ascending ▼ or descending ▲ . *You can filter a column by using the filtering option:* . c. Double-click the task that will function as a trigger condition. The task is added to the trigger and the dialog is closed. d. Use the drop-down list to select whether the trigger condition is fulfilled on **Task successful** or **Task failed**. Click **Delete** to remove a task from the trigger. *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).* 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 **Select task by double-click** dialog if it has already been added to the trigger. There is a logical AND between

*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 time period is reached, the task that was first completed is no longer considered executed and the end of the time period is recalculated. The trigger then waits for all tasks to be completed within the recalculated time period.*

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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 apply and save your changes.
   Successfully added is displayed at the bottom of the page.

You have now created a new reload task to an app.

See also:

- *Creating a task chain (page 286)*
- *Creating reload tasks from tasks (page 281)*

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..

   You can filter a column by using the filtering option: .

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.

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

   a. You can change the task name in the **Name** field.
   b. **App name** displays the app you selected from the overview. You can change which app you are creating the task for by clicking the **App name** 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 of selected type 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. Apply QMC tags if desired.
   f. Apply custom properties if desired.

Identification

The **Identification** property group contains the basic reload task properties in the Qlik Sense system. 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

The **Execution** property group contains the reload task execution properties in the Qlik Sense

system.

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 trigger

The following properties are available for a scheduled trigger.

Property	Description
Name	The name of the trigger. Mandatory.
Type	The trigger type.
Enabled	The trigger is enabled when selected.
Start	Select when the trigger takes effect by typing the following values: • **Time to start (hh:mm)** and • **Start date (YYYY-MM-DD)**

Property	Description

Schedule	Set the trigger schedule:
	• **Once**.
	• **Hourly**. Set the time period between the executions of the trigger. Edit **Repeat after each** by typing the values for:
	  • **hour(s)** (default is 1)
	  • **minute(s)** (default is 0)
	• **Daily**. Set the time between the executions of the trigger by typing a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	• **Weekly**. Set the time between the executions of the trigger:
	  • Type a value for **Every week(s)** (default is 1) and
	  • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	  *If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*

End	Type values for the following: • **Time to end (hh:mm)** • **End date (YYYY-MM-DD)** Select **Infinite** to create a never ending trigger.

Triggers - Task event trigger

The following properties are available for a task event trigger.

Property	Description
Name	The name of the trigger. Mandatory.
Type	The trigger type.
Enabled	The trigger is enabled when selected.

Property	Description
Time constraint	Defines the time period (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. See: *Creating a task chain (page 286)*
Add task **Task successful** or **Task failed**	Do the following: a. Click **Add task** to add a tasks that will function as a trigger condition. A drop-down list and an empty field is added. b. Click the empty field to add a task. The dialog **Double-click to select** is opened and displays a list of tasks with the following columns: **App name**, **Tags** connected to the task, and **Name**, which is the task name. Click a column heading to sort that column ascending ▼ or descending ▲ . *You can filter a column by using the filtering option:* . c. Double-click the task that will function as a trigger condition. The task is added to the trigger and the dialog is closed. d. Use the drop-down list to select whether the trigger condition is fulfilled on **Task successful** or **Task failed**. Click **Delete** to remove a task from the trigger. *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).* 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 **Select task by double-click** dialog if it has already been added to the trigger. There is a logical AND between

*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 time period is reached, the task that was first completed is no longer considered executed and the end of the time period is recalculated. The trigger then waits for all tasks to be completed within the recalculated time period.*

Tags

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

Custom properties

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

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

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

You have now edited the tasks for apps.

See also:

- *Creating reload tasks (page 205)*
- *Creating reload tasks from tasks (page 281)*

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..

   You can filter a column by using the filtering option: .

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 **Relaod 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**.

You have now deleted the tasks.

See also:

Deleting task (page 295)

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..

   You can filter a column by using the filtering option: .

2. Select the app or apps 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 **App associations** page with the **Tasks** overview is displayed.
4. Select the tasks you want to start and click **Start** in the action bar.
   A dialog is displayed to confirm that your task or tasks are started.

You have now started a task or tasks for an app or apps.

Tasks can also be started by triggers.

See also:

Starting tasks (page 297)

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..

   You can filter a column by using the filtering option: .

2. Select the app or 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.
   The panel to the far left lists your selections.
4. Select the tasks you want to stop and click **Stop** in the action bar.
   A dialog is displayed to confirm that your task or tasks are stopped.

You have now stopped reload tasks for an app or apps.

See also:

Stopping tasks (page 298)

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** in the far right of the action bar and select **Reload now** in the pop-up menu.
   The task to reload the app was successfully started. The status can be viewed in the Task overview if you have access to that section is displayed and a reload task is started. If the task fails you receive the message **Failed to create/start the reload app task. Please try again.**
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**.

   You can filter a column by using the filtering option: .

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.

You have now reloaded an app manually to fully reload the data in an app from the source.

Creating content libraries

Currently, only material in the Default content library is accessible from the Qlik Sense hub.

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 create 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. 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.

   The **Identification** property group contains the identification information for the selected content libraries.

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.

   The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

   The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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 can ungroup them by clicking **Ungroup**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that OR is superior to AND.

Operator	Descriptions and examples
=	This operator is not case sensitive and returns True if the compared expressions are exactly equal. **Example:** `user.name = ”a*”` The user named exactly a* is targeted by the rule.
like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name = ”a*”` All user with names beginning with an a is targeted by the rule.

!=	This operator is not case sensitive and returns True if the attribute values in the compared expressions are equal. **Example:** `user.name=resource.name` All resources with the same name as the user are targeted by the rule.

Successfully added is displayed at the bottom of the page.

You have now created a new content library.

See also:

- *Resource edit page (page 28)*
- *Creating access rights for content libraries (page 224)*

Editing content libraries

Currently, only material in the Default content library is accessible from the Qlik Sense hub.

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.

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

   The **Identification** property group contains the identification information for the selected content libraries.

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.

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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.

You have now edited a content library.

See also:

- *Resource edit page (page 28)*
- *Creating access rights for content libraries (page 224)*

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.

> *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 have now deleted the content libraries and all their library objects.

Uploading objects to content libraries

> *Currently, only material in the Default content library is accessible from the Qlik Sense hub.*

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 file or files you want to import and click **Open**.
   The browse window closes and the file or 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 a upload is queued. The upload starts when less than 4 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.*

You have now uploaded objects to a content library.

Deleting objects from content libraries

You can delete objects from the content libraries that you have delete rights to.

If you want to delete all objects in a content library you can do this by deleting the content library.

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.

You have now deleted the objects.

See also:

Deleting content libraries (page 221)

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.

   You can filter a column by using the filtering option: .

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 can ungroup them by clicking **Ungroup**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that OR is superior to AND.

Operator	Descriptions and examples

=	This operator is not case sensitive and returns True if the compared expressions are exactly equal. **Example:** `user.name = "a*"` The user named exactly a* is targeted by the rule.
like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name = "a*"` All user with names beginning with an a is targeted by the rule.
!=	This operator is not case sensitive and returns True if the attribute values in the compared expressions are equal. **Example:** `user.name=resource.name` All resources with the same name as the user are targeted by the rule.

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.

See also:

- *Editing security rules (page 410)*

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.

   The **Identification** property group contains the basic app object properties.

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

   The property group **Tags** contains the QMC tags that are connected to the app object.

Property	Description
Tags	Click the text box to see the available QMC tags. Start typing to reduce the list. Connected QMC tags are listed under the text box.

   The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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.

You have now edited one or more app objects.

See also:

Resource edit page (page 28)

Deleting app objects

You can delete app objects that you have delete rights to.

Deleting app objects through the QMC only removes them from being visible in the QMC. They are not deleted from the qvf file.

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.

   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 have now deleted the app objects.

3.3 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 in 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 can create streams. Do the following:

1. Select **Streams** 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 ⊕ **Create new** in the action bar.
3. Edit the properties.

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

   The **Identification** property group contains the identification information for the for the selected streams.

Property	Description
Name	The name of the stream.
Owner	The owner of the stream. This property does not exist until the stream is created.

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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 stream.
   The **Create security rule** dialog opens.
5. Create security rules for the stream and click **Apply**, or click **Cancel**.

You have now created a new stream.

See also:

- *Creating access rights for streams (page 230)*
- *Resource edit page (page 28)*

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.

   You can filter a column by using the filtering option: .

2. Select the stream or streams 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.

   If you selected an individual stream you can edit the existing security rules for that stream or add new ones by clicking the ⊕ button.

   If you select several streams, you cannot view, edit or add security rules.

   The **Identification** property group contains the identification information for the for the selected streams.

Property	Description
Name	The name of the stream.
Owner	The owner of the stream. This property does not exist until the stream is created.

   The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

   The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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 apply and save changes.

Successfully updated is displayed at the bottom of the page.

You have now edited the stream or streams.

See also:

Resource edit page (page 28)

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**.

You have now deleted the streams.

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.

   You can filter a column by using the filtering option: .

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. **Example:** `user.name = ”a*”` The user named exactly a* is targeted by the rule.
like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name like ”a*”` All user with names beginning with an a is targeted by the rule.
!=	This operator is not case sensitive and returns True if the values in the compared expressions are not equal. **Example:** `user.name != resource.name` All resources that do not have the same name as the user are targeted by the rule.

6. Optionally, edit the **Advanced** properties and create the **Conditions** for the rule:
   - Add a condition.
   - Use the drop-down to specify the context to which the rule will apply.
7. Click **Apply**.
   The dialog closes and the rule is added to the security rules overview.

> *The security rule results in a corresponding security rule in the **Security rule** overview page.*

You have now created the access rights for the selected stream.

See also:

Editing security rules (page 410)

3.4 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.

Extensions

Extensions can be 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.

The **Identification** property group contains the identification information for the for the selected data connections.

Property	Description
Name	The name of the data connection.
Owner	The user name of the owner of the data connection.
Connection string	The connection string for the data connection. Typically, includes the name of the data source, drivers, and path.
Type	The type of data connection. Standard data connections include ODBC, OLEDB, and Folder.
User ID	The user ID that is used in the connection string.
Password	The password associated with the user ID used in the connection string. *The password is saved encrypted.*

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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.

You have now edited the data connection or connections.

See also:

- *Resource edit page (page 28)*

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.

   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 have now deleted the data connections.

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.

   You can filter a column by using the filtering option: ⊽.

2. Select the data connection that you want to create rules for and click **Edit**.
   The data connection edit page opens.
3. Select **System rules** under **Associated items**.
   The system rules overview is displayed.
4. Click ⊕ **Create new** 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. **Example:** `user.name = "a*"` The user named exactly a* is targeted by the rule.
like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name like "a*"` All user with names beginning with an a is targeted by the rule.
!=	This operator is not case sensitive and returns True if the values in the compared expressions are not equal. **Example:** `user.name != resource.name` All resources that do not have the same name as the user are targeted by the rule.

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.

See also:

- *Editing security rules (page 410)*

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 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 %ProgramData%\Qlik\Sense\Repository\Extensions. The maximum file size is half of the free disk space.*

You have now uploaded the new extension.

Extension names

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 Qlik Sense Workbench.*

See also:

Resource edit page (page 28)

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.

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

2. Select the extension or extensions 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.*

The **Identification** property group contains the basic identification properties in the Qlik Sense system.

Property	Description
Name	The name of the extension is obtained from the file name of the extension definition file (*.qext*) in the uploaded zip file and cannot be modified.
Owner	The user name of the owner of the extension. *This property is only visible when editing an extension.*

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

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

You have now edited an extension or extensions.

> *The web browser caches the extensions for up to six hours. The user can manually clear the cache to access a new version of an extension.*

See also:

- *Resource edit page (page 28)*

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.

   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 have now deleted the extensions.

3.5 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:

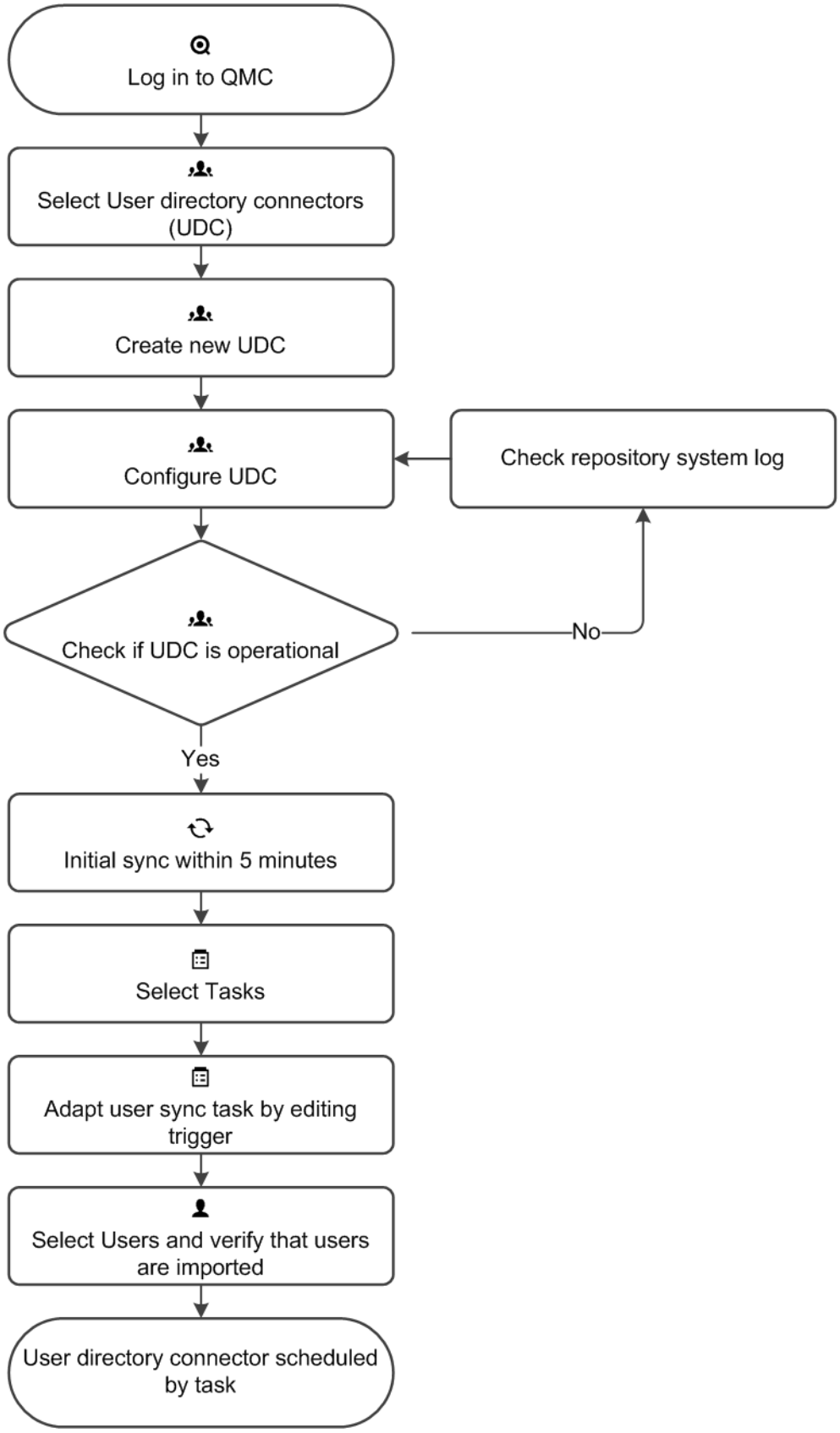
- Creating new user directory connectors
- Synchronizing with user directories
- Managing access types
- Changing ownership of resources
- Removing resources owned by users
- Connecting administrative roles to a user
- Inactivating users
- Deleting users

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 5 minutes. The user directory connector must be configured and operational to function.

If desired you can change the default trigger for the user synchronization task and/or add more triggers.You can synchronize the user data manually from the user directory connectors overview.

This 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

See also:

- *Creating a user directory connector (page 243)*
- *Creating trigger for user sync task - scheduled (page 268)*
- *Synchronizing with user directories (page 254)*
- *ODBC example (page 240)*

ODBC example

Each data source has a different configuration and below is one example of adding an ODBC user directory connector.

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 attributes of the users. The values in the csv files are comma separated. The tables can for example look like this:

   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. Add a new user directory connector, default properties (ODBC) and edit the properties:

   The **Identification** property group contains the basic UDC properties in the Qlik Sense system. 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.

The **User sync settings** property group contains the user sync properties for the user directory connector.

Property	Description	Default value
Fetch user data on first access, then keep in sync	• 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** or **Generic LDAP** if you only want to synchronize a selection of users.	Selected

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

Property	Description	Default value
User directory name	The name of the user directory. Must be unique, otherwise the connector will not be configured.	-
Users table name	The name of the table containing the users.	-
Attributes table name	The name of the table containing the attributes of the users.	-
Visible connection string	The visible part of the connection string that is used to connect to the data source. *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 contains user name and password. *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*

You have now added an ODBC data source and initial synchronization will be performed within 5 minutes (by default).

See also:

- *User directory connectors (page 113)*
- *Creating a user directory connector (page 243)*
- *Synchronizing with user directories (page 254)*

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)))*

See also:

- *Creating a user directory connector (page 243)*
- *Synchronizing with user directories (page 254)*

Creating a user directory connector

You can create a new User Directory Connector (UDC). 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
   - Apache directory search
   - Local network
   - ODBC
   - Access (through ODBC)
   - Excel (through ODBC)
   - SQL (through ODBC)
4. Edit the properties.

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

   The **Identification** property group contains the basic UDC properties in the Qlik Sense system.
   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.

The **User sync settings** property group contains the user sync properties for the user directory connector.

Property	Description	Default value
Fetch user data on first access, then keep in sync	• 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** or **Generic LDAP** if you only want to synchronize a selection of users.	Selected

*Decide how the synchronization is performed by selecting or clearing **Fetch user data on first access, then keep in sync**, in the property group **User sync settings**.*

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

Property	Description	Default value
User directory name *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 AD domain. To support SSL, specify the protocol as LDAPS instead.	ldap://company.domain.com

Property	Description	Default value
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.	-

When a user creates an Active Directory connector that uses LDAPS, the connector will only work when that user (the creator of the UDC) is logged on to the machine and running the Qlik Sense services.
To sync users using LDAPS, you must provide user name and password.

The **Connection** property group contains the Local users connection properties in the Qlik Sense system.

Property	Description	Default value
Sync all domain users	• If not selected, only the users on your local computer will be synchronized. • If selected, all users in the domain that your computer belongs to will be synchronized.	Not selected

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

Property	Description	Default value
User directory name	The name of the user directory. Must be unique, otherwise the connector will not be configured.	-
Users table name	The name of the table containing the users.	-
Attributes table name	The name of the table containing the attributes of the users.	-
Visible connection string	The visible part of the connection string that is used to connect to the data source. *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 contains user name and password. *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

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 AD.	-
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. *If the user synchronization is unsuccessful, try setting the value to no value.*	2000

*Use the **Additional LDAP filter** in the property group **Advanced** to apply a filter that retrieves only a selection of the users.*

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

Property	Description	Default value
Type	The name of the attributes 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 name of the attributes 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 name of the attributes 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.	memberOf
Members of directory entry	The name of the attributes that holds a reference to the direct members of this directory entry. See also the **Group membership** setting, above.	member

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

Property	Description
Tags	*If no QMC tags are available, this property group is empty.* Connected QMC 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*.**The User Directory Connector (UDC) is not configured** is displayed if the **User directory name** is already used or if the field is empty.

See also:

- *Resource edit page (page 28)*
- *ODBC example (page 240)*
- *Using Additional LDAP filter to retrieve specific users (page 242)*

Editing 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.

   You can filter a column by using the filtering option: ⊤.

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.

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

   The **Identification** property group contains the basic UDC properties in the Qlik Sense system. 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.

   The **User sync settings** property group contains the user sync properties for the user directory connector.

Property	Description	Default value
Fetch user data on first access, then keep in sync	• 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** or **Generic LDAP** if you only want to synchronize a selection of users.	Selected

*Decide how the synchronization is performed by selecting or clearing **Fetch user data on first access, then keep in sync**, in the property group **User sync settings**.*

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

Property	Description	Default value
User directory name *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 AD domain. To support SSL, specify the protocol as LDAPS instead.	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.	-

When a user creates an Active Directory connector that uses LDAPS, the connector will only work when that user (the creator of the UDC) is logged on to the machine and running the Qlik Sense services.
To sync users using LDAPS, you must provide user name and password.

The **Connection** property group contains the Local users connection properties in the Qlik Sense system.

Property	Description	Default value
Sync all domain users	• If not selected, only the users on your local computer will be synchronized. • If selected, all users in the domain that your computer belongs to will be synchronized.	Not selected

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

Property	Description	Default value
User directory name	The name of the user directory. Must be unique, otherwise the connector will not be configured.	-
Users table name	The name of the table containing the users.	-
Attributes table name	The name of the table containing the attributes of the users.	-
Visible connection string	The visible part of the connection string that is used to connect to the data source. *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 contains user name and password. *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

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 AD.	-
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. *If the user synchronization is unsuccessful, try setting the value to no value.*	2000

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).

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

Property	Description	Default value
Type	The name of the attributes 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 name of the attributes that holds the emails of a directory entry (user).	mail
Display name	The full name of either a user or a group directory entry.	name

Property	Description	Default value
Group membership	The name of the attributes 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.	memberOf
Members of directory entry	The name of the attributes that holds a reference to the direct members of this directory entry. See also the **Group membership** setting, above.	member

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

Property	Description
Tags	*If no QMC tags are available, this property group is empty.* Connected QMC 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*.**The User Directory Connector (UDC) is not configured** is displayed if the **User directory name** is already used or if the field is empty.

See also:

- *Resource edit page (page 28)*
- *ODBC example (page 240)*
- *Using Additional LDAP filter to retrieve specific users (page 242)*

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.

See also:

Creating a user directory connector (page 243)

Deleting user directory connector and users (optional)

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**.

You have now deleted the user directory connector, and if selected, also the users from the user directory.

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.

   You can filter a column by using the filtering option: ⊽.

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.*

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 **Fetch user data on first access, then keep in sync** 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** or **Generic LDAP** if you only want to synchronize a selection of users.
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**

   You can click ↻ in the top right corner to update the page.

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.

Allocating user access

You allocate user access to an identified user to allow the user to access streams and apps within a Qlik Sense site.

Do the following:

1. Select **License and tokens** 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 ⊕ **Allocate** in the action bar.
   The **Users** dialog opens.

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

   > *Click a column heading to sort that column ascending ▼ or descending ▲ .*

   If you click **Cancel** the dialog is closed and you return to the **User access** overview.
4. Select one or more users in the list and click **Allocate**.

   > ***Allocate** is disabled if the number of tokens available for allocation is not enough for the number of selected users.*

   The dialog is closed and the users are added in the **User access rules** overview table. Also, the information on the **Tokens** page is updated.

You have now allocated user access and the users can access streams and apps.

Deallocating user access

You can deallocate user access from a user to free up tokens.

Do the following:

1. Select **License and tokens** 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.

   You can filter a column by using the filtering option: .

   Click a column heading to sort that column ascending ▼ *or descending* ▲ .

3. Select the user or users that you want to deallocate and click **Deallocate** in the action bar at the bottom of the page.
   A confirmation dialog is displayed.
4. Click **OK** in the dialog to confirm that you want to deallocate user access from the users.
   - The **Status** is changed to **Quarantined** if the user has logged in within the last 7 days.
   - If the user has not logged in within the last 7 days, the user is removed from the overview and the tokens are released.

   Also, the information on the **Tokens** page is updated.

You have now deallocated user access and the users cannot access streams and apps.

Reinstating user access

You can reinstate user access to a user whose token is in quarantine if you do so within 7 days. Do the following:

1. Select **License and tokens** 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.

   You can filter a column by using the filtering option: .

   Click a column heading to sort that column ascending ▼ *or descending* ▲ .

3. Select one or more users with the **Status Quarantined** and click **Reinstate** in the action bar at the bottom of the page.
   The **Status** is changed to **Allocated**. Also, the information on the **Tokens** page is updated.

You have now reinstated user access and the users can access streams and apps.

Creating login access

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 you set the following:

- The number of tokens you want to allocate, providing for a number of login access passes.
- The license rule specifying which users the login access is available for.

Do the following:

1. Select **License and tokens** 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.

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

   The property group **Identification** contains a login access property.

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

   The property group **Allocated tokens** contains a login access property.

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

   When using multiple conditions, you can group two conditions by clicking **Group**. After the conditions have been grouped, you can ungroup them by clicking **Ungroup**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that OR is superior to AND.
   Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.
5. Click **Apply**.
   The **Create license rule** dialog opens.
6. Edit the license rule for the login access:
   a. You can edit the **Identification** properties:

Name	The name of the login access. 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.

*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. **Example:** `user.name = ”a*”` The user named exactly a* is targeted by the rule.
like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name like ”a*”` All user with names beginning with an a is targeted by the rule.
!=	This operator is not case sensitive and returns True if the values in the compared expressions are not equal. **Example:** `user.name != resource.name` All resources that not have the same name as the user are targeted by the rule.

7. Optionally, edit the **Advanced** properties and create the **Conditions** for the rule:
   - Add a condition.
   - Use the drop-down to specify for which context the rule will apply to.
8. Click **Apply** in to create and save the login access.
   The license rule was successfully added to the associated items is displayed at the bottom of the page.

If the number of available tokens is not enough, an error dialog is displayed. Reduce the **Number of tokens** and click **Apply** again.

You have now created a new login access and the rules for the login. The users that the rule specifies can access streams and apps as long as there are remaining login access passes.

See also:

Resource edit page (page 28)

Editing login access

You can edit login access, 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 is available for.

Do the following:

1. Select **License and tokens** 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 **Login access rules** in the panel to the right.
3. Select the login access you want to edit and click **Edit** in the action bar.
4. Edit the properties.

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

   The property group **Identification** contains a login access property.

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

   You can change the name for the login access:

   The property group **Allocated tokens** contains a login access property.

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 dialog 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**.

   The property group **Users** contains a the users associated with the login access.

Property name	Description
Name	The name of the user.
Permitted action	**UseAccessType** is the only permitted value. It means that the user has login access rights.

The property group **System rules** contains the system rules for the login access.

Property name	Description
Name	The name of the rule.
Comment	A comment for the rule.
Resource filter	Shows the resource filter for the rule.
Actions	Shows the actions for the rule.
Status	Shows if the rule is **Enabled** or **Disabled**.

Edit the system rule by selecting a rule and clicking **Edit**. You can also create a new rule by clicking ⊕ **Create new**. Create the user conditions for the security rule. Click ⊕ to add a condition. If you add more than one condition you select **AND** or **OR** in the drop-down list. Click ⊗ to remove a condition.

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.

You have now edited login access and the rules for the login. The users that the rule specifies can access streams and apps as long as there are remaining login access passes.

See also:

Resource edit page (page 28)

Deleting login access

You can delete login access that you have delete rights to, to free up 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 and tokens** 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.

   You can filter a column by using the filtering option: ⊽.

3. Select the login accesses 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.

You have now deleted login access and the users in the login access group cannot access streams and apps.

Creating user access rule

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

Do the following:

1. Select **License and tokens** 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 associated rule** in the action bar.
4. Edit the properties.

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

   The **Identification** property group contains the basic user access rule settings in the Qlik Sense system.

Property name	Description
Name	The name of the user access rule.
Disabled	Select to disable the rule. The rule is enabled by default.
Description	Here you can enter a description for the rule.

   The **Advanced** property group contains the available advanced settings in the Qlik Sense system.

Property name	Description
Resource filter	A definition of the type or types of resources that the rule will be evaluated for.
Conditions	A definition of the resource and/or users that should be met for the rule to apply.
Context	You can specify whether the rule should apply for: **Only in hub**, **Only in QMC**, or **Both in hub and QMC**.

The **Basic** property group contains the basic operators that are available in the Qlik Sense system.

Operator	Descriptions and examples
=	This operator is not case sensitive and returns True if the compared expressions are exactly equal. **Example:** `user.name = ”a*”` The user named exactly a* is targeted by the rule.
like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name like ”a*”` All user with names beginning with an a is targeted by the rule.
!=	This operator is not case sensitive and returns True if the values in the compared expressions are not equal. **Example:** `user.name != resource.name` All resources that not have the same name as the user are targeted by the rule.

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

When using multiple conditions, you can group two conditions by clicking **Group**. After the conditions have been grouped, you can ungroup them by clicking **Ungroup**. The default operator between

conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that OR is superior to AND.
Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

5. Click **Apply** in 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.

You have now created a new user access rule. The users that the rule specifies can have access as long as there are remaining access tokens available.

See also:

Resource edit page (page 28)

Editing user access rule

A user access rule defines which users have access to the available tokens. You can edit existing rules.

Do the following:

1. Select **License and tokens** 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 applicable fields in the **Properties** and **Associated items** tabs:

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

Identification

Property name	Description
Name	The name of the user access rule.
Disabled	When selected, the rule is disabled.
Description	Here you can enter a description for the rule.

Advanced

Property name	Description
Resource filter	A definition of the types of resources that the rule will be evaluated for.
Conditions	A definition of the resource and/or users that needs to be met for the rule to apply.
Context	You can specify whether the rule should apply for: **Only in hub**, **Only in QMC**, or **Both in hub and QMC**.

Basic

Operator	Descriptions and examples
=	This operator is not case sensitive and returns True if the compared expressions are exactly equal. **Example:** `user.name = ”a*”` The user named exactly a* is targeted by the rule.
like	This operator is not case sensitive and returns True if the compared expressions are equal. **Example:** `user.name like ”a*”` All user with names beginning with an a is targeted by the rule.
!=	This operator is not case sensitive and returns True if the values in the compared expressions are not equal. **Example:** `user.name != resource.name` All resources that not have the same name as the user are targeted by the rule.

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

Property	Description
Tags	*If no QMC tags are available, this property group is empty.* Connected QMC 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.

When using multiple conditions, you can group two conditions by clicking **Group**. After the conditions have been grouped, you can ungroup them by clicking **Ungroup**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that OR is superior to AND.
Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.

6. Click **Apply** in 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 unallocated. They have to be unallocated manually.

You have now edited a user access rule. The users that the rule specifies can have access as long as there are remaining access tokens available.

Deleting user access rule

You can delete user access rules that you have delete rights to.

Do the following:

1. Select **License and tokens** 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**.

You have now deleted a user access rule.

If a user access rule is deleted, and there are currently users with tokens allocated by this rule, these tokens are automatically unallocated. They have to be unallocated manually.

See also:

Resource edit page (page 28)

Starting user sync task

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.

   You can filter a column by using the filtering option: .

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 task** overview is displayed.
4. Select the tasks 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.

You have now started one or more user synchronization tasks.

See also:

- *Creating trigger for user sync task - scheduled (page 268)*
- *Starting tasks (page 297)*

Editing user sync task

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.

   You can filter a column by using the filtering option: .

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.

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

   The **Identification** property group contains the basic user sync task properties in the Qlik Sense system.
   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.

   The **Tags** property group contains the available QMC tags in the Qlik Sense system.

Property	Description
Tags	*If no QMC tags are available, this property group is empty.* Connected QMC 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 apply and save your changes.
   Successfully updated is displayed at the bottom of the page.

You have now edited a task or tasks for a user directory connector.

*Triggers for a task are displayed under **Associated items**, where you also can choose to create new triggers.*

See also:

- *Resource edit page (page 28)*
- *Creating trigger for user sync task - scheduled (page 268)*
- *User sync task associated items (page 63)*

Editing task (page 290)

Creating trigger for user sync task - 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.

   You can filter a column by using the filtering option: .

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 new** in the action bar and select **Scheduled** in the drop-down list.
   A dialog is displayed.
5. The following properties are available for a scheduled trigger.

Property	Description
Name	The name of the trigger. Mandatory.
Type	The trigger type.
Enabled	The trigger is enabled when selected.
Start	Select when the trigger takes effect by typing the following values: • **Time to start (hh:mm)** and • **Start date (YYYY-MM-DD)**

Property	Description

Schedule	Set the trigger schedule:
	• **Once**.
	• **Hourly**. Set the time period between the executions of the trigger. Edit **Repeat after each** by typing the values for:
	  • **hour(s)** (default is 1)
	  • **minute(s)** (default is 0)
	• **Daily**. Set the time between the executions of the trigger by typing a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	• **Weekly**. Set the time between the executions of the trigger:
	  • Type a value for **Every week(s)** (default is 1) and
	  • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	  *If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*

End	Type values for the following: • **Time to end (hh:mm)** • **End date (YYYY-MM-DD)** Select **Infinite** to create a never ending trigger.

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

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**.

You have now created a new scheduled trigger for a task.

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.

   You can filter a column by using the filtering option: .

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.
   The following properties are available for a scheduled trigger.

Property	Description
Name	The name of the trigger. Mandatory.
Type	The trigger type.
Enabled	The trigger is enabled when selected.
Start	Select when the trigger takes effect by typing the following values: • **Time to start (hh:mm)** and • **Start date (YYYY-MM-DD)**

Property	Description

Schedule	Set the trigger schedule:
	• **Once**.
	• **Hourly**. Set the time period between the executions of the trigger. Edit **Repeat after each** by typing the values for:
	  • **hour(s)** (default is 1)
	  • **minute(s)** (default is 0)
	• **Daily**. Set the time between the executions of the trigger by typing a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	• **Weekly**. Set the time between the executions of the trigger:
	  • Type a value for **Every week(s)** (default is 1) and
	  • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	  *If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*

End	Type values for the following: • **Time to end (hh:mm)** • **End date (YYYY-MM-DD)** Select **Infinite** to create a never ending trigger.

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

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.

You have now edited a trigger for a task.

Stopping user sync task

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.

   You can filter a column by using the filtering option: .

2. Select the user directory connector that you want to start a task 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 task** overview is displayed.
4. Select the tasks 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.

You have now stopped one or more user synchronization tasks.

See also:

Stopping tasks (page 298)

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.

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

   The property group **Identification** contains the basic user properties in the Qlik Sense system.

Property	Description
Name	The name of the user.

Property	Description
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.
Admin roles	The QMC administration roles associated with the user.

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. 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.

You have updated the users.

See also:

- *Default administration roles (page 369)*
- *Managing admin roles for a user (page 276)*
- *Inactivating users (page 274)*
- *Editing items owned by users (page 278)*

Deleting user sync task

You can delete user synchronization tasks that you have delete rights to from the user directory connector's association page.

You can also delete 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.

   You can filter a column by using the filtering option: ⊽.

2. Select the User directory connector that you want to delete tasks from and click **Edit** in the action bar.
3. Select **Tasks** under **Associated items**.
   The **User synchronization task** overview is displayed.
4. Select the tasks you want to delete.
5. Click **Delete** in the action bar.
   A **Delete** dialog is displayed.
6. Click **OK**.

You have now deleted the tasks.

See also:

Deleting task (page 295)

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.

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.

   You can filter a column by using the filtering option: .

2. Select the users that you want to inactivate.
3. Click **Edit** in the action bar.
   The **User edit** page opens.
4. Select **Blocked**.
   Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.
5. Click **Apply** in the action bar to apply and save your changes.

You have now inactivated the selected users.

See also:

Deleting users (page 275)

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**.

You have now deleted the users.

See also:

- *Inactivating users (page 274)*
- *Deleting user directory connector and users (optional) (page 253)*

Creating a root administrator user

The first user that is accessing the Qlik Management Console (QMC) and adding the server license obtains the role root administrator (RootAdmin) for the Qlik Sense system. This user has full access rights for all resources in the site: security rules, streams, nodes and so on. Additional users can be assigned as RootAdmin if needed or assigned to 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**.*

See also:

- *Starting the QMC (page 20)*

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.

*You can edit users that have access rights to a stream from the **Streams** overview. Simply select the stream from the Streams overview, click **Users** from the property groups, select the user or users and then click **Edit**.*

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 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.

   > *As 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.*

   Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.
6. Click **Apply** in the action bar to apply and save your changes.

You have now made changes to the user admin roles.

See also:

- *Default administration roles (page 369)*

Changing ownership of resources

By default the owner is the creator of the resource. The ownership can be changed. The **Owner** property is available in the **Properties** section when you choose to edit a resource.

Do the following:

1. From a resource overview, select the resource that you want to change owner of and click **Edit**.
2. Type 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 cannot assign the ownership to a user who does not exist in the Qlik Sense system.
4. Click **Apply** to change owner.
   Successfully updated is displayed.

You now have changed the owner of the resource.

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.

You can now view all the items owned by the user.

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.

You have now edited an item owned by the user.

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.

   You can filter a column by using the filtering option: .

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 sync and security rules associated with that resource are deleted automatically.
7. Click **OK**.

You have now deleted the items.

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.

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.

The QMC is delivered with a set of predefined administration roles. Each role is associated with security rules tailored for specific purposes as described in the following table.

Property	Description
RootAdmin	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.
AuditAdmin	Has read access to all resource names, and for users also read access to user directory name and user directory ID. Has read rights on the Monitoring apps stream.
ContentAdmin	Has create, read, update and delete rights for all resources except nodes, engines, repositories, schedulers, proxies, virtual proxies, and syncs. Has read and publish rights on the Monitoring apps stream.

Property	Description
DeploymentAdmin	Has create, read, update and delete rights for apps, tasks, users, licenses, nodes, repositories, schedulers, proxies, virtual proxies, and engines. Has read rights on the Monitoring apps stream.
SecurityAdmin	Same as ContentAdmin but with create, read, update and delete rights for proxies and virtual proxies, and no access rights on tasks. Has read rights on server node configuration. Has read and publish rights on the Monitoring apps stream.

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 QMC content admin roles (page 439)*

See also:

- *Managing admin roles for a user (page 276)*
- *Providing users with access using user types (page 280)*

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:

- User properties and/or
- 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 444)*

See also:

- *Providing administrators with access using roles (page 279)*

3.6 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.

See also:

- *Creating reload tasks (page 205)*
- *Creating trigger for user sync task - scheduled (page 268)*

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.

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

   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 of selected type 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 QMC tags.
   f. Optionally, apply custom properties.

The **Identification** property group contains the basic reload task properties in the Qlik Sense system. 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>

The **Execution** property group contains the reload task execution properties in the Qlik Sense system.

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

The following properties are available for a scheduled trigger.

Property	Description
Name	The name of the trigger. Mandatory.
Type	The trigger type.
Enabled	The trigger is enabled when selected.
Start	Select when the trigger takes effect by typing the following values: • **Time to start (hh:mm)** and • **Start date (YYYY-MM-DD)**

Property	Description

Schedule	Set the trigger schedule:
	• **Once**.
	• **Hourly**. Set the time period between the executions of the trigger. Edit **Repeat after each** by typing the values for:
	  • **hour(s)** (default is 1)
	  • **minute(s)** (default is 0)
	• **Daily**. Set the time between the executions of the trigger by typing a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	• **Weekly**. Set the time between the executions of the trigger:
	  • Type a value for **Every week(s)** (default is 1) and
	  • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	  *If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*

End	Type values for the following: • **Time to end (hh:mm)** • **End date (YYYY-MM-DD)** Select **Infinite** to create a never ending trigger.

The following properties are available for a task event trigger.

Property	Description
Name	The name of the trigger. Mandatory.
Type	The trigger type.
Enabled	The trigger is enabled when selected.

Property	Description
Time constraint	Defines the time period (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. See: *Creating a task chain (page 286)*
Add task **Task successful** or **Task failed**	Do the following: a. Click **Add task** to add a tasks that will function as a trigger condition. A drop-down list and an empty field is added. b. Click the empty field to add a task. The dialog **Double-click to select** is opened and displays a list of tasks with the following columns: **App name**, **Tags** connected to the task, and **Name**, which is the task name. Click a column heading to sort that column ascending ▼ or descending ▲ . *You can filter a column by using the filtering option:* . c. Double-click the task that will function as a trigger condition. The task is added to the trigger and the dialog is closed. d. Use the drop-down list to select whether the trigger condition is fulfilled on **Task successful** or **Task failed**. Click **Delete** to remove a task from the trigger. *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).* 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 **Select task by double-click** dialog if it has already been added to the trigger. There is a logical AND between

*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 time period is reached, the task that was first completed is no longer considered executed and the end of the time period is recalculated. The trigger then waits for all tasks to be completed within the recalculated time period.*

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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 apply and save your changes.
   Successfully added is displayed at the bottom of the page.

You have now created a new reload task to an app.

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.

See also:

- *Creating reload tasks (page 205)*
- *Creating reload tasks from tasks (page 281)*
- *Viewing task chains (page 289)*

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.

See also:

- *Creating reload tasks (page 205)*
- *Creating reload tasks from tasks (page 281)*
- *Viewing task chains (page 289)*

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 task

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.

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

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.

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

   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

The **Identification** property group contains the basic reload task properties in the Qlik Sense system. 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>

The **Execution** property group contains the reload task execution properties in the Qlik Sense system.

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

The following properties are available for a scheduled trigger.

Property	Description
Name	The name of the trigger. Mandatory.
Type	The trigger type.
Enabled	The trigger is enabled when selected.

Property	Description
Start	Select when the trigger takes effect by typing the following values: • **Time to start (hh:mm)** and • **Start date (YYYY-MM-DD)**

Schedule	Set the trigger schedule:
	• **Once**.
	• **Hourly**. Set the time period between the executions of the trigger. Edit **Repeat after each** by typing the values for:
	  • **hour(s)** (default is 1)
	  • **minute(s)** (default is 0)
	• **Daily**. Set the time between the executions of the trigger by typing a value for **Every day(s)** (default is 1). For example, type 2 to repeat the trigger every second day.
	• **Weekly**. Set the time between the executions of the trigger:
	  • Type a value for **Every week(s)** (default is 1) and
	  • Select one or more days under **On these weekdays** to determine which days the trigger is repeated (on the weeks you have specified). For example, type 3 and select **Mon** to repeat the trigger on Mondays every third week.
	• **Monthly**. Select one or more days under **On these days** to define the days when the trigger is repeated every month.
	  *If you have selected **Monthly** and want to be sure that a trigger is repeated every month, you need to select a day no later than the 28th.*

End	Type values for the following: • **Time to end (hh:mm)** • **End date (YYYY-MM-DD)** Select **Infinite** to create a never ending trigger.

The following properties are available for a task event trigger.

Property	Description
Name	The name of the trigger. Mandatory.

Property	Description
Type	The trigger type.
Enabled	The trigger is enabled when selected.
Time constraint	Defines the time period (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. See: *Creating a task chain (page 286)*
Add task **Task successful** or **Task failed**	Do the following: a. Click **Add task** to add a tasks that will function as a trigger condition. A drop-down list and an empty field is added. b. Click the empty field to add a task. The dialog **Double-click to select** is opened and displays a list of tasks with the following columns: **App name**, **Tags** connected to the task, and **Name**, which is the task name. Click a column heading to sort that column ascending ▼ or descending ▲ . *You can filter a column by using the filtering option:* . c. Double-click the task that will function as a trigger condition. The task is added to the trigger and the dialog is closed. d. Use the drop-down list to select whether the trigger condition is fulfilled on **Task successful** or **Task failed**. Click **Delete** to remove a task from the trigger. *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).* 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 **Select task by double-click** dialog if it has already been added to the trigger. There is a logical AND between

> *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 time period is reached, the task that was first completed is no longer considered executed and the end of the time period is recalculated. The trigger then waits for all tasks to be completed within the recalculated time period.*

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

User synchronization task properties

The **Identification** property group contains the basic user sync task properties in the Qlik Sense system.
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

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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 apply and save your changes.
   Successfully updated is displayed at the bottom of the page.

You have now edited a task.

See also:

- *Resource edit page (page 28)*
- *Editing reload tasks (page 210)*
- *Editing user sync task (page 266)*

Deleting task

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 have now deleted the tasks.

You can also delete a task from the association page when you edit an app or a user directory connector.

See also:

- *Deleting reload tasks (page 215)*
- *Deleting user sync task (page 273)*

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.

   You can filter a column by using the filtering option: .

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.*

See also:

- *Editing task (page 290)*

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.

   You can filter a column by using the filtering option: .

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 have now disabled the tasks.

You can also disable a task from the properties tab when you edit the task.

See also:

Editing task (page 290)

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 or task 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.

You have now started one or more task.

Tasks can also be started by triggers.

See also:

- *Managing tasks and triggers (page 281)*
- *Viewing task chains (page 289)*
- *Starting reload tasks (page 216)*
- *Starting user sync task (page 266)*

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.

You have now stopped the tasks.

3.7 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.

See also:

- *Creating virtual proxy (page 324)*

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 ⓘ 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.

See also:

- *Editing nodes (page 311)*

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 Planning Qlik Sense deployments 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 Installation Guide

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 Qlik Management Console (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 be in the format `node2.domain.com`.

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 field, an asterisk (*) is displayed next to the property name, to indicate that the property value will be changed. Clicking **Revert** in the action bar resets all field values while clicking ↩ next to a field only resets that specific field 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 for 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 synchronization process begins. When finished, the **Certificate setup** dialog displays that the service was successfully unlocked.

   The first synchronization can take a few minutes to complete and during this time the services are not accessible. If you have several large applications on the central node, the synchronization may take several minutes to complete.

   If the synchronization is not successful, the certificate setup dialog displays that it failed to install the Qlik Sense certificate package. Please try again or check the log for details.

4. When the synchronization has completed, restart the services you installed on the new node.

The node is now added and operational.

Editing repository

You can edit the 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 repository or repositories 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.

   The **Identification** property group contains the basic repository properties in the Qlik Sense system. All fields are mandatory and must not be empty.

Property	Description	Default value
Node	The repository name.	Inherits the node name.

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

Tracing

Application log level	All the application messages for the repository service are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
Audit log level	Detailed, user-based messages are saved to this logger, for example, security rules information. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
License log level	All the license messages are saved to this logger. For example, token usage and user access allocation. Use the drop-down to set the verbosity of the logger: • **Info**: fatal, error, warning, and information entries • **Debug**: same as info, but including also debug entries	Info

Qlik Management Console (QMC) log level	All the QMC messages are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
Performance log level	All the performance messages for the repository service are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

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

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

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

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

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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.

You have now made repository edits.

See also:

Resource edit page (page 28)

Creating node

You can create a node.

When you create a node its associated services are also created and they inherit the node name: repository, engine, 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.

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

   The **Identification** property group contains the basic node properties in the Qlik Sense system. 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 **Node purpose** property group contains the basic node properties in the Qlik Sense system.

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 buttons in the Hub to create apps and the My Work section are not displayed to the user.
- 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.

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).
Proxy	The Qlik Sense Proxy Service (QPS).
Scheduler	The Qlik Sense Scheduler Service (QSS).

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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.

See also:

- *Creating virtual proxy (page 324)*
- *Adding load balancing (page 321)*

Editing nodes

You can edit nodes.

Do the following:

1. Select **Nodes** 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 node 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.*

   The **Identification** property group contains the basic node properties in the Qlik Sense system.

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 **Node purpose** property group contains the basic node properties in the Qlik Sense system.

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 buttons in the Hub to create apps and the My Work section are not displayed to the user.
- 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.

The **Services activation** property group contains the available services activation properties in the Qlik Sense system.
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).
Proxy	The Qlik Sense Proxy Service (QPS).
Scheduler	The Qlik Sense Scheduler Service (QSS).

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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.

You have now edited the node.

See also:

Resource edit page (page 28)

Redistributing 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.

   You can filter a column by using the filtering option: .

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.

*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.*

When you delete a node, its services are also deleted: proxy, engine, and scheduler. 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.

   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 have now deleted the nodes and their resources.

Editing proxies

You can edit a proxy that you have update rights to.

1. Select **Proxies** 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 proxies 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.

   The **Identification** property group contains the basic proxy properties in the Qlik Sense system. All fields are mandatory and must not be empty.

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

The **Ports** property group contains the proxy ports properties in the Qlik Sense system.

Property	Description	Default value
Service listen port HTTPS (default)	The secure listen port for the proxy, which by default manages all Qlik Sense communication. *Make sure that port 443 is available for the Qlik Sense Proxy Service (QPS) to use because the port is sometimes used by other software, for example, web servers.*	443
Authentication listen port HTTPS (default)	The secure listen port for the default (internal) authentication module.	4244
Kerberos authentication	Select to enable Kerberos authentication.	Not selected
REST API listen port	The listen port for the proxy API.	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 is allowed. Then the QMC address is *https://<QPS server name>:Service listen port HTTP/qmc* (where *https* can be replaced by *http*). By default the QMC address is *https://<QPS server name>/qmc*. *If you change the property **Allow HTTP**, please know that all web browser bookmarks (that Qlik Sense users or QMC admin users have created) will not be valid anymore.* *The **Service listen port HTTP** and **Authentication listen port HTTP** need to be set when **Allow HTTP** is checked.*	False (not allowed)
Service listen port HTTP	The unencrypted listen port, used when HTTP connection is allowed.	80
Authentication listen port HTTP	The unencrypted authentication listen port, used when HTTP connection is allowed.	4248

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

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 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

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

Tracing

Performance log interval (minutes)	The interval of performance logging.	5 minutes
Audit log level	More detailed, user-based messages are saved to this logger, for example, proxy calls. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
Performance log level	All the performance messages are saved to this logger. For example, performance counters and number of connections, streams, sessions, tickets, web sockets and load balancing information. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

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

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

The **Security** property group contains the proxy security properties in the Qlik Sense system.

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. *To be valid, the certificate must contain a private key.*

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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**.

   The **Virtual proxies** property group contains a list of associated 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.

   When you apply the changes the proxy must be restarted. Sessions handled by this proxy are ended and the users are logged out.

   Successfully updated is displayed at the bottom of the page.

You have now made proxy edits.

See also:

Resource edit page (page 28)

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.

Do the following:

1. Select **Virtual proxies** 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 virtual proxy 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.

   You can apply a filter to a column by clicking .

   Click a column heading to sort that column ascending ▼ *or descending* ▲ .

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.
   Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.
7. Click **Apply** in the action bar.
   A confirmation dialog is displayed telling you that the proxy must be restarted, sessions will be ended and users logged out.
8. Click **OK**.
   Successfully updated is displayed at the bottom of the page.

You have now added load balancing.

See also:

- *Creating virtual proxy (page 324)*
- *Editing virtual proxy (page 331)*

Configuring load balancing to isolate development nodes

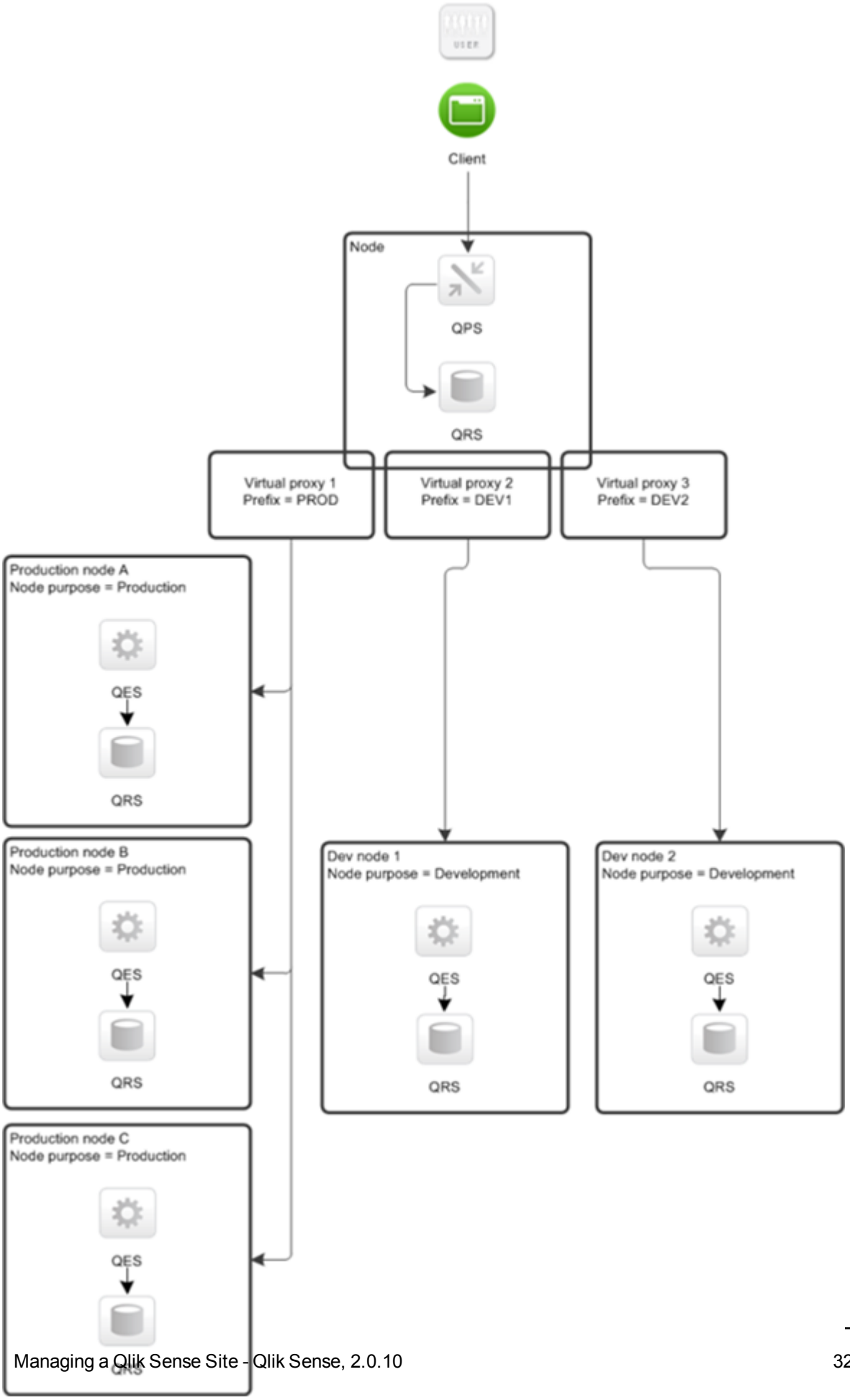
When you install multiple engines and virtual proxies, you must add load balancing to the new nodes and virtual proxies. It is only on the central node that load balancing is automatically added. You can configure a proxy so that it only talks to its local engine or to a subset of the engines, which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

It is recommended that you use separate development nodes when performing selective synchronization 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.


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
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.

See also:

- *Creating virtual proxy (page 324)*
- *Editing nodes (page 311)*
- *Adding load balancing (page 321)*
- *Configuring sync rules (page 383)*

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.

   You can filter a column by using the filtering option: .

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**.

You have now deleted the load balancing for the selected proxies.

Creating 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.

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.

The **Identification** property group contains the basic virtual proxy properties in the Qlik Sense system.
All fields are mandatory and must not be empty.

Property	Description	Default value
Description	The description of the virtual proxy.	Blank
Prefix	The path name in the proxy's URI that defines each additional path. Example: *https://[node]/[prefix]/* You can only use characters that can be part of a URI path. You can use slashes (/), but the prefix cannot begin nor end with a slash. Hash signs (#) cannot be used. Uniform Resource Identifier (URI): Generic Syntax	Blank
Session inactivity timeout (minutes)	The maximum period of time with inactivity before timeout. After this, the session is invalid and the user is logged out from the system.	30 minutes
Session cookie header name	The name of the HTTP header used for the session cookie. This value is blank by default and you must enter a value. *It can be useful to include the value of the **Prefix** property above as a suffix in the cookie name.*	Blank

The **Authentication** property group contains the authentication method properties for the virtual proxies in the Qlik Sense system.

Property	Description	Default value
Anonymous access mode	How to handle anonymous access: • **No anonymous user** • **Allow anonymous user** • **Always anonymous user**	No anonymous user
Authentication method	• **Ticket**: a ticket is used for authentication. • **Header authentication static user directory**: allows static header authentication, where the user directory is set in the QMC. • **Header authentication dynamic user directory**: allows dynamic header authentication, where the user directory is fetched from the header. • **SAML**: SAML2 is used for authentication.	Ticket
Header authentication header name	The name of the HTTP header that identifies users, when header authentication is allowed. Mandatory if you allow header authentication (by selecting either **Header authentication static user directory** or **Header authentication dynamic user directory** for the **Authentication method** property). *Header authentication only supports US-ASCII (UTF-8 is not supported).*	Blank

Property	Description	Default value
Header authentication static user directory	The name of the user directory where additional information can be fetched for header authenticated users. Mandatory if you allow static header authentication (by selecting **Header authentication static user directory** for the **Authentication method** property).	Blank
Header authentication dynamic user directory	Mandatory if you allow dynamic header authentication (by selecting **Header authentication dynamic user directory** for the **Authentication method** property). The pattern you supply must contain '$ud', '$id' and a way to separate them. **Example setting and matching header:** `$ud\\$id` – matches USERDIRECTORY\userid (backslashes must be escaped with an additional \) `$id@$ud` – matches userid@USERDIRECTORY ($id and $ud can be in any order) `$ud:::$id` – matches USERDIRECTORY:::userid	Blank
Windows authentication pattern	The chosen authentication pattern for logging in. If the User-Agent header contains the Windows authentication pattern string, Windows authentication is used. If there is no matching string, form authentication is used.	Windows
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)

Property	Description	Default value
SAML host URI	The server name that is exposed to the client. This name is used by the client for accessing Qlik services, such as the QMC. The server name does not have to be the same as the machine name, but in most cases it is. You can use either http:// or https:// in the URI. To be able to use http://, you must select **Allow HTTP** on the edit page of the proxy that the virtual proxy is linked to. Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property).	Blank
SAML entity ID	ID to identify the service provider. The ID must be unique. Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property).	Blank
SAML metadata IdP	The metadata from the IdP is used to configure the service provider, and is essential for the SAML authentication to work. A common way of obtaining the metadata is to download it from the IdP website. Click the browse button and open the IdP metadata .xml file for upload. To avoid errors, you can click **View content** and verify that the file has the correct content and format. The configuration is incomplete without metadata.	

Property	Description	Default value
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. See: *I do not know the name of a mandatory SAML attribute (page 459)*	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'. See: *I do not know the name of a mandatory SAML attribute (page 459)*	Blank
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'.	

The **Load balancing** property group contains the load balancing properties for the virtual proxies in the Qlik Sense system.

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

The **Advanced** property group contains the advanced properties for the virtual proxies in the Qlik Sense system.

Property	Description	Default value
Extended security environment	Enabling this setting will send the following information about the client environment in the security header: OS, device, browser, and IP. If not selected, the user can run the same engine session simultaneously on multiple devices.	Blank
Session cookie domain	By default the session cookie is valid only for the machine that the proxy is installed on. This (optional) property allows you to increase its validity to a larger domain. Example: `company.com`	Blank (default machine)

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

Websocket origin 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.	Blank

The **Integration** property group contains the integration properties for the virtual proxies in the Qlik Sense system.

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)

The property group **Tags** contains the available QMC tags in the Qlik Sense system.

Property	Description
Tags	*If no QMC tags are available, this property group is empty.* Click the text box to be display a list of the available QMC tags. Start typing to reduce the list. Connected tags are displayed under the text box.

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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.

You now have created a new virtual proxy.

See also:

Resource edit page (page 28)

Editing 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.

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:

The **Identification** property group contains the basic virtual proxy properties in the Qlik Sense system.
All fields are mandatory and must not be empty.

Property	Description	Default value
Description	The description of the virtual proxy.	Blank
Prefix	The path name in the proxy's URI that defines each additional path. Example: *https://[node]/[prefix]/* You can only use characters that can be part of a URI path. You can use slashes (/), but the prefix cannot begin nor end with a slash. Hash signs (#) cannot be used. Uniform Resource Identifier (URI): Generic Syntax	Blank
Session inactivity timeout (minutes)	The maximum period of time with inactivity before timeout. After this, the session is invalid and the user is logged out from the system.	30 minutes
Session cookie header name	The name of the HTTP header used for the session cookie. This value is blank by default and you must enter a value. *It can be useful to include the value of the **Prefix** property above as a suffix in the cookie name.*	Blank

The **Authentication** property group contains the authentication method properties for the virtual proxies in the Qlik Sense system.

Property	Description	Default value
Anonymous access mode	How to handle anonymous access: • **No anonymous user** • **Allow anonymous user** • **Always anonymous user**	No anonymous user
Authentication method	• **Ticket**: a ticket is used for authentication. • **Header authentication static user directory**: allows static header authentication, where the user directory is set in the QMC. • **Header authentication dynamic user directory**: allows dynamic header authentication, where the user directory is fetched from the header. • **SAML**: SAML2 is used for authentication.	Ticket
Header authentication header name	The name of the HTTP header that identifies users, when header authentication is allowed. Mandatory if you allow header authentication (by selecting either **Header authentication static user directory** or **Header authentication dynamic user directory** for the **Authentication method** property). *Header authentication only supports US-ASCII (UTF-8 is not supported).*	Blank

Property	Description	Default value
Header authentication static user directory	The name of the user directory where additional information can be fetched for header authenticated users. Mandatory if you allow static header authentication (by selecting **Header authentication static user directory** for the **Authentication method** property).	Blank
Header authentication dynamic user directory	Mandatory if you allow dynamic header authentication (by selecting **Header authentication dynamic user directory** for the **Authentication method** property). The pattern you supply must contain '$ud', '$id' and a way to separate them. **Example setting and matching header:** `$ud\\$id` – matches USERDIRECTORY\userid (backslashes must be escaped with an additional \) `$id@$ud` – matches userid@USERDIRECTORY ($id and $ud can be in any order) `$ud:::$id` – matches USERDIRECTORY:::userid	Blank
Windows authentication pattern	The chosen authentication pattern for logging in. If the User-Agent header contains the Windows authentication pattern string, Windows authentication is used. If there is no matching string, form authentication is used.	Windows
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)

Property	Description	Default value
SAML host URI	The server name that is exposed to the client. This name is used by the client for accessing Qlik services, such as the QMC. The server name does not have to be the same as the machine name, but in most cases it is. You can use either http:// or https:// in the URI. To be able to use http://, you must select **Allow HTTP** on the edit page of the proxy that the virtual proxy is linked to. Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property).	Blank
SAML entity ID	ID to identify the service provider. The ID must be unique. Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property).	Blank
SAML metadata IdP	The metadata from the IdP is used to configure the service provider, and is essential for the SAML authentication to work. A common way of obtaining the metadata is to download it from the IdP website. Click the browse button and open the IdP metadata .xml file for upload. To avoid errors, you can click **View content** and verify that the file has the correct content and format. The configuration is incomplete without metadata.	

Property	Description	Default value
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. See: *I do not know the name of a mandatory SAML attribute (page 459)*	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'. See: *I do not know the name of a mandatory SAML attribute (page 459)*	Blank
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'.	

The **Load balancing** property group contains the load balancing properties for the virtual proxies in the Qlik Sense system.

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

The **Advanced** property group contains the advanced properties for the virtual proxies in the Qlik Sense system.

Property	Description	Default value
Extended security environment	Enabling this setting will send the following information about the client environment in the security header: OS, device, browser, and IP. If not selected, the user can run the same engine session simultaneously on multiple devices.	Blank
Session cookie domain	By default the session cookie is valid only for the machine that the proxy is installed on. This (optional) property allows you to increase its validity to a larger domain. Example: `company.com`	Blank (default machine)

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

Websocket origin 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.	Blank

The **Integration** property group contains the integration properties for the virtual proxies in the Qlik Sense system.

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)

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

Property	Description
Tags	*If no QMC tags are available, this property group is empty.* Click the text box to be display a list of the available QMC tags. Start typing to reduce the list. Connected tags are displayed under the text box.

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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**.

Node	The proxy name.
Status	One of the following statuses is displayed: • **Running** The service is running as per normal. • **Stopped** The service has stopped. • **Disabled** The service has been disabled. *Click ⓘ in the **Status** column for more detailed information on the status.* See: *Checking the status of Qlik Sense services (page 298)*.
Service listen port HTTPS (default)	The secure listen port for the proxy, which by default manages all Qlik Sense communication. *Make sure that port 443 is available for the Qlik Sense Proxy Service (QPS) to use because the port is sometimes used by other software, for example, web servers.*

Allow HTTP	Status values: **Yes** or **No**. **Yes**: Unencrypted communication is allowed. This means that both https (secure communication) and (http) unencrypted communication is allowed.
Service listen port HTTP	The unencrypted listen port, used when HTTP connection is allowed.
Authentication listen port HTTPS (default)	The secure listen port for the default (internal) authentication module.
Kerberos authentication	Status values: **Yes** or **No**. **Yes**: Kerberos authentication is enabled.
Authentication listen port HTTP	The unencrypted authentication listen port, used when HTTP connection is allowed.
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.
Keep-alive timeout (seconds)	The maximum timeout period for a single HTTP request before closing the connection. Protection against denial-of-service attacks. This means that if an ongoing request exceeds this period, Qlik Sense proxy will close the connection. Increase this value if your users work over slow connections and experience closed connections.
Max header size (bytes)	The maximum total header size.
Max header lines	The maximum number of lines in the header.
Audit activity log level	Levels: **Off** or **Basic** (a limited set of entries)
Audit security log level	Levels: **Off** or **Basic** (a limited set of entries)
Service log level	Each level from **Error** to **Info** includes more information than the previous level.
Audit log level	More detailed, user-based messages are saved to this logger, for example, proxy calls. Each level from **Fatal** to **Debug** includes more information than the previous level.

Performance log level	All the performance messages are saved to this logger. For example, performance counters and number of connections, streams, sessions, tickets, web sockets and load balancing information. Each level from **Fatal** to **Debug** includes more information than the previous level.
Security log level	All the certificates messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
System log level	All the standard proxy messages are saved to this logger. Each level from **Fatal** to **Debug** includes more information than the previous level.
Performance log interval (minutes)	The interval of performance logging.
REST API listen port	The listen port for the proxy API.
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.
	You can combine filtering with searching. *Searching and filtering in the QMC (page 29)*
Edit	Click **Edit** in the action bar and edit the selected proxy.
Unlink	Click to unlink a proxy service from the selected proxy. *A virtual proxy must be linked to a proxy service in order to work.*
Link	Click to 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.
   Successfully updated is displayed at the bottom of the page.

You now have edited a virtual proxy.

See also:

- *Resource edit page (page 28)*
- *SAML authentication (page 377)*

Deleting virtual proxy

You can delete a virtual proxy 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.

   You can filter a column by using the filtering option: .

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**.

You have now deleted a virtual proxy.

Editing scheduler

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.

   You can filter a column by using the filtering option: .

2. Select the scheduler or schedulers 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.

The **Identification** property group contains the basic scheduler properties in the Qlik Sense system. All fields are mandatory and must not be empty.

Property	Description	Default value
Node	The scheduler name.	Inherits the node name.

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: • **Off**: no entries • **Basic**: a limited set of entries	Basic
Service log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Error**: only error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries	Info

Tracing

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

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

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

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

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

Property	Description	Default value
Type	If enabled by the property above, the QSS type is set to: • Master: sends the task to a slave QSS within the site. • Slave: receives the task from the master QSS and executes the task. • 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
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

The **Tags** property group contains the available QMC tags in the Qlik Sense system.

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

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) 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.

You have now made scheduler edits.

See also:

Resource edit page (page 28)

Editing 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.

   You can filter a column by using the filtering option: .

2. Select the engine or engines 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.

   The **Identification** property group contains the basic engine properties in the Qlik Sense system.

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

   The **Apps** property group contains engine properties in the Qlik Sense system.

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 timeout (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
Working folder	A scheduled reload will search for files in this directory when relative paths are used to define file location.	%ProgramData%\Qlik\Sense\Apps

Property	Description	Default value
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

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

Property	Description	Default value
Listen ports	The listen port used by Qlik Sense Engine Service (QES) for communication with the Qlik Sense web clients. Click ⊕ to add more ports. Click ⊗ to remove a port.	4747
Allow data lineage	Save the data lineage (that is, the origin of the data) when executing a load script that loads data into Qlik Sense.	Selected
Min memory usage (%)	The minimum memory capacity used by Qlik Sense.	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: • **Hard max limit**: never use more memory than defined by the property above. • **Ignore max limit**: use as much memory as necessary, regardless of the **Max memory usage (%)** setting. • **Soft max limit**: use more memory than defined by the**Max memory usage (%)** setting, if necessary and available.	Hard max limit
CPU throttle (%)	The amount of CPU capacity used by Qlik Sense. Range: 0 – 100 %	0 (that is, no throttling)

Property	Description	Default value
Standard mode	When selected, standard mode is used. If cleared, legacy mode is used. For security reasons, Qlik Sense in standard mode does not support absolute or relative paths in the data load script or functions and variables that expose the file system. *Disabling standard mode can create a security risk by exposing the file system.*	Selected

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: • **Off**: no entries • **Basic**: a limited set of entries	Basic
Service log level	Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Error**: only error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries	Info

Tracing

Performance log interval (minutes)	The number of minutes in-between performance logging entries.	5

System log level	All the standard engine messages are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
Performance log level	All the performance messages are saved to this logger (by default updated default every five minutes). The log contains, for example, the number of active users, the number of open sessions, and the CPU load. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info

QIX performance log level	All the QIX protocol performance messages are saved to this logger. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Off
Audit log level	More detailed, user based, messages are saved to this logger, for example, when the user makes a selection in an app. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Off

Session log level	All the session messages are saved to this logger when a client session is terminated, for example, user information, machine ID, IP address and port number. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Info
Traffic log level	All the traffic messages are saved to this logger, for example, all JSON-messages to and from the engine. Use the drop-down to set the verbosity of the logger: • **Off**: no entries • **Fatal**: only fatal entries • **Error**: same as fatal, but also including error entries • **Warning**: same as error, but also including warning entries • **Info**: same as warning, but also including information entries • **Debug**: same as info, but also including debug entries	Off

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

The **Tags** property group contains the available tags in the Qlik Sense system.

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.

The **Custom properties** property group contains the custom properties in the Qlik Sense system. When a custom property has been activated for a resource, you can use the drop-down 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) and you must make a custom property available for this resource type before it will be displayed here.

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

You have now made engine edits.

See also:

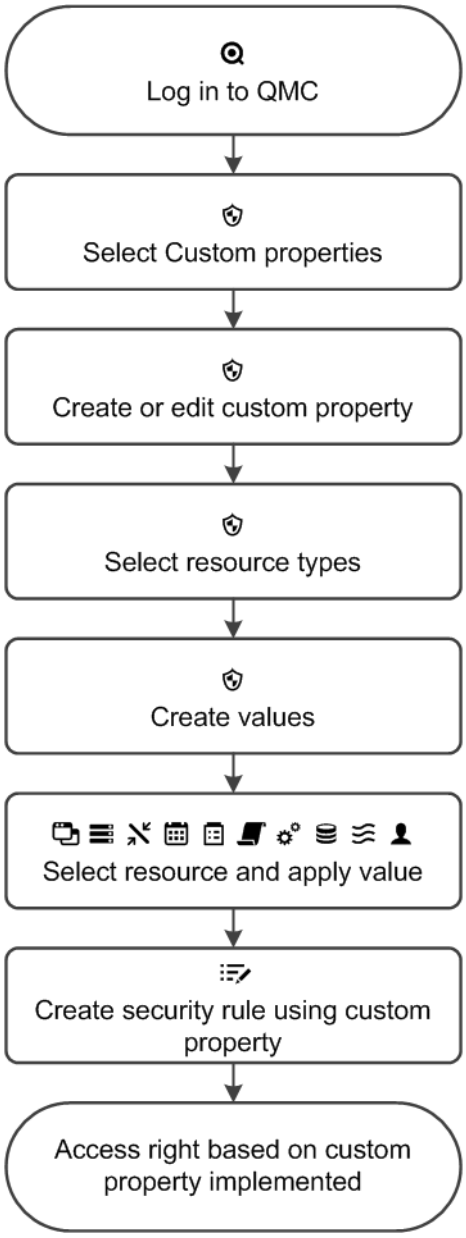
Resource edit page (page 28)

3.8 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 these values can be used 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:



See also:

- *Creating sync rules with custom properties (page 389)*
- *Security rules example: Creating QMC organizational admin roles (page 441)*
- *Security rules example: Applying Qlik Sense access rights for user types (page 444)*
- *Creating a custom property (page 355)*
- *Applying a custom property value (page 358)*
- *Editing a custom property (page 356)*

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.

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

   The **Identification** property group contains the name of the custom property.

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).

   The **Resource types** property group contains the resources that the custom property can be used on.

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

   The **Values** property group contains values that you create for the custom property.

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 have now created a new custom property and can use its values on resources and in security rules.

See also:

- *Resource edit page (page 28)*
- *Applying a custom property value (page 358)*
- *Creating security rules (page 399)*

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.

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

2. Select one custom property and click **Edit** in the action bar at the bottom of the page.
3. Edit the properties.

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

   The **Identification** property group contains the name of the custom property.

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).

The **Resource types** property group contains the resources that the custom property can be used on.

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

The **Values** property group contains values that you create for the custom property.

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.

You have now edited a custom property and can use its values on resources and in security rules.

See also:

🗋 *Resource edit page (page 28)*

- *Applying a custom property value (page 358)*
- *Creating security rules (page 399)*

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.

   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 have now deleted the custom properties.

Applying a custom property value

To be able to use a custom property value in the security rules, you must first apply the custom property value 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.

   You can filter a column by using the filtering option: .

2. Select one or more resources and click **Edit**.
3. Select **Custom properties** from the **Properties** section and select the value that you want to apply in the drop-down list next to the custom property.

   *If **Custom properties** is not available in the properties panel to the right, you must first make a custom property available for the resource. You do this when you create (or edit) a custom property.*

   Click **Apply** to save your changes. If a mandatory field is empty, **Apply** is disabled.
4. Click **Apply** in the action bar to apply the value.
   Successfully added is displayed at the bottom of the page.

You have now applied a custom property value, and you can use it when creating security rules for the resource.

See also:

- *Creating a custom property (page 355)*
- *Creating security rules (page 399)*

3.9 Using QMC tags

You create QMC 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 (page 359)

Connecting tags (page 360)

Disconnecting tags (page 361)

Searching and filtering in the QMC (page 29)

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.

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

   The property group **Identification** contains the basic tag properties in the Qlik Sense system.

Property	Description
Name	The name of the QMC tag. The name must be unique.

   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 apps that the tag is connected to.

Property	Description
App objects	The app objects that the tag is connected to.
Security rules	The security rules that the tag is connected to.
Extensions	The extensions that the tag is connected to.
Content libraries	The content libraries that the tag is connected to.
Data connections	The data connections that the tag is connected to.
Nodes	The nodes that the tag is connected to.
Engines	The engines that the tag is connected to.
Proxies	The proxies that the tag is connected to.
Virtual proxies	The virtual proxies that the tag is connected to.
Repositories	The repositories that the tag is connected to.
Schedulers	The schedulers that the tag is connected to.
Streams	The streams that the tag is connected to.
Users	The users that the tag is connected to.
User directory connectors	The user directories that the tag is connected to.
Reload tasks	The reload tasks that the tag is connected to.
User synchronization tasks	The user synchronization tasks that the tag is connected to.

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 tag.
   Successfully added new tag is displayed at the bottom of the page. A new button (**Add another**), appears and can be used to create another tag.

You have created a new tag.

See also:

- *Resource edit page (page 28)*

Connecting tags

You can connect a tag to a resource. Do the following:

1. Select a resource type (for example, **Apps**) on theQMC 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.

See also:

Creating tags (page 359)

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 theQMC 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.

You have now removed the connection between the tag and the resource.

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.

   You can filter a column by using the filtering option: .

2. Select the tags 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.

   The property group **Identification** contains the basic tag properties in the Qlik Sense system.

Property	Description
Name	The name of the QMC tag. The name must be unique.

   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 apps that the tag is connected to.
App objects	The app objects that the tag is connected to.
Security rules	The security rules that the tag is connected to.
Extensions	The extensions that the tag is connected to.
Content libraries	The content libraries that the tag is connected to.
Data connections	The data connections that the tag is connected to.
Nodes	The nodes that the tag is connected to.
Engines	The engines that the tag is connected to.
Proxies	The proxies that the tag is connected to.
Virtual proxies	The virtual proxies that the tag is connected to.
Repositories	The repositories that the tag is connected to.
Schedulers	The schedulers that the tag is connected to.
Streams	The streams that the tag is connected to.
Users	The users that the tag is connected to.

Property	Description
User directory connectors	The user directories that the tag is connected to.
Reload tasks	The reload tasks that the tag is connected to.
User synchronization tasks	The user synchronization tasks that the tag is connected to.

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.

You have now edited a tag or tags.

See also:

Resource edit page (page 28)

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.

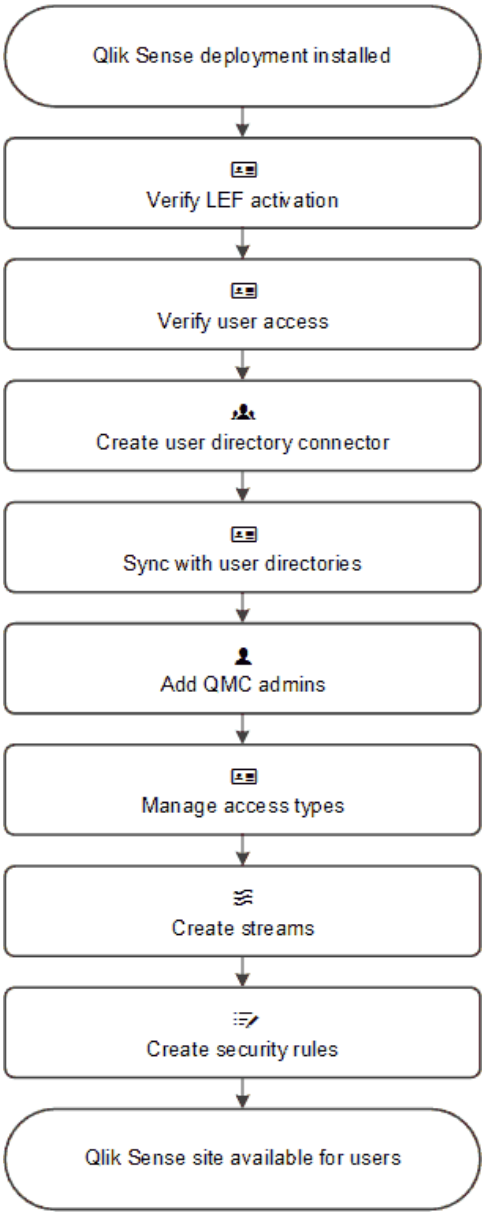
   You can filter a column by using the filtering option: .

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

You have now deleted the tags.

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:



Do the following:

1. If not performed during the installation, activate the license. This will:
   - Make you the root admin for the site.
   - Provide tokens that can be used on access types.
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 (**User access** or **Login access**) 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.

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**.*

See also:

- *Activating license (page 188)*
- *Creating login access (page 256)*
- *Setting up a user directory connector and schedule by task (page 238)*
- *Synchronizing with user directories (page 254)*
- *Adding root admin and admin users (page 367)*
- *Allocating user access (page 255)*
- *Creating login access (page 256)*
- *Creating streams (page 227)*
- *Writing security rules (page 421)*
- *Managing apps (page 194)*

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 not published 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.

See also:

🗋 *Providing administrators with access using roles (page 279)*

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.

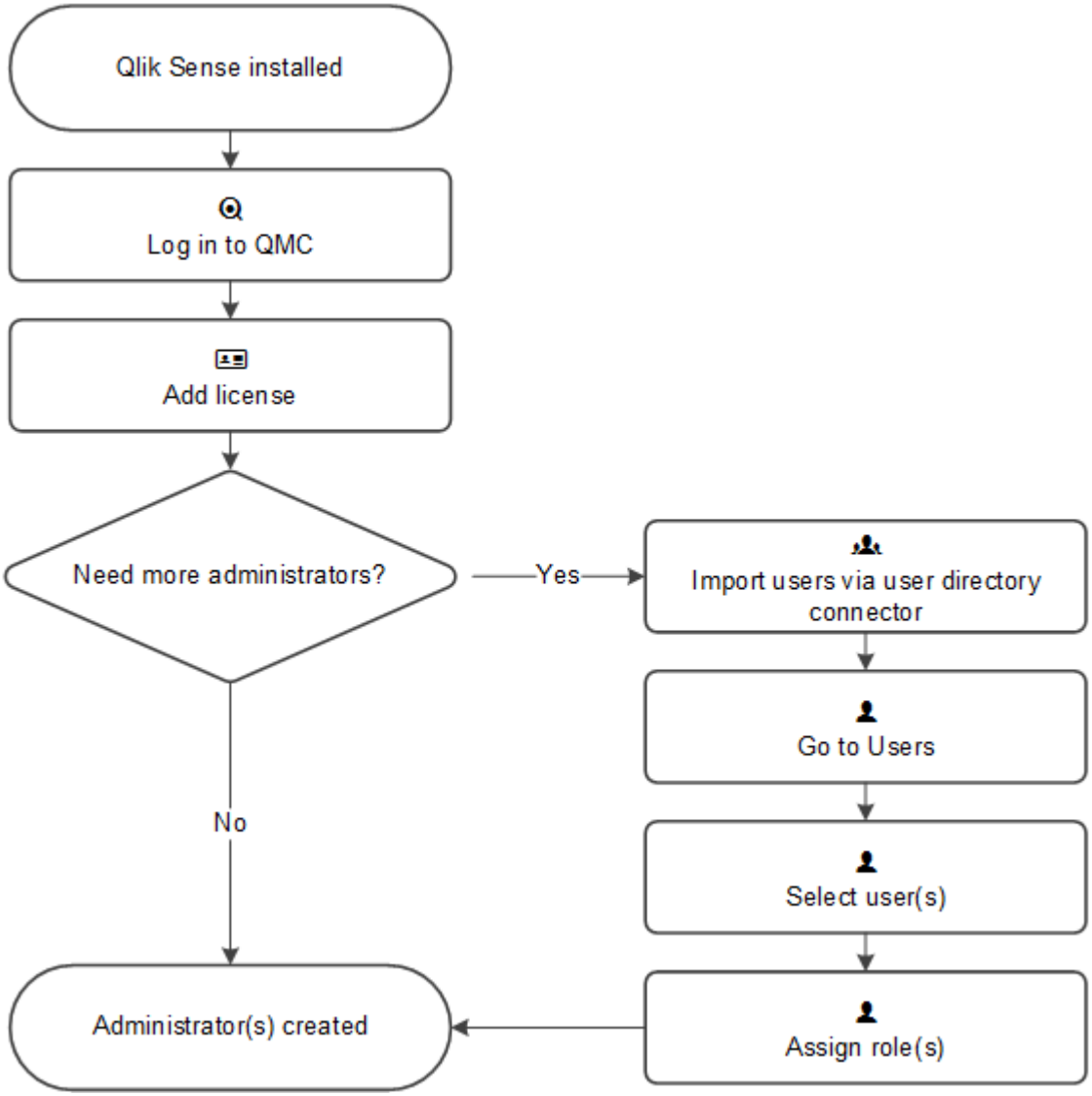
See also:

- *Adding root admin and admin users (page 367)*
- *Authentication (page 371)*
- *Changing proxy certificate (page 380)*
- *Creating virtual proxy (page 324)*
- *Using custom properties (page 353)*
- *Designing access control (page 391)*
- *Writing security rules (page 421)*
- *Security rules examples (page 439)*

Adding root admin and admin users

The first user that is accessing the Qlik Management Console (QMC) and adding the server license obtains the role root administrator (RootAdmin) for the Qlik Sense system. This user has full access rights for all resources in the site: security rules, streams, nodes and so on. Additional users can be assigned as RootAdmin if needed or assigned to other admin roles with other administrative rights.

This workflow illustrates adding QMC administrators:



Setup workflow for root administrator (RootAdmin)

Do the following:

1. Verify that Qlik Sense is installed.
2. Login to Qlik Management Console (QMC) using the Windows account 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 admin user (page 369)*.

The root administrator role is now created.

Setup workflow admin user

Do the following:

1. Login as root administrator (RootAdmin).
2. Import users with 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 should have administrative rights and click **Edit**.
5. Assign the role using the **Admin roles** attribute by clicking ⊕ and entering the name of the administration role in the text box that appears.

   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.

As 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 as described in the following table.

Property	Description
RootAdmin	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.
AuditAdmin	Has read access to all resource names, and for users also read access to user directory name and user directory ID. Has read rights on the Monitoring apps stream.

Property	Description
ContentAdmin	Has create, read, update and delete rights for all resources except nodes, engines, repositories, schedulers, proxies, virtual proxies, and syncs. Has read and publish rights on the Monitoring apps stream.
DeploymentAdmin	Has create, read, update and delete rights for apps, tasks, users, licenses, nodes, repositories, schedulers, proxies, virtual proxies, and engines. Has read rights on the Monitoring apps stream.
SecurityAdmin	Same as ContentAdmin but with create, read, update and delete rights for proxies and virtual proxies, and no access rights on tasks. Has read rights on server node configuration. Has read and publish rights on the Monitoring apps stream.

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

The QMC looks for changes in the user roles definitions every 20 seconds.
The following table displays an overview of the default QMC administrator roles (in addition to the RootAdmin) and which parts of the QMC they can manage.

QMC	SecurityAdmin	DeploymentAdmin	ContentAdmin	AuditAdmin
Apps	x	x	x	
Content libraries	x		x	
Data connections	x		x	
App objects	x		x	
Streams	x		x	
Tasks		x	x	
Users	x	x	x	
Audit	x	x	x	x
Security rules	x			
Custom properties	x	x	x	
License and tokens		x		
Extensions			x	
Tags	x	x	x	x
User directory connectors		x		

QMC	SecurityAdmin	DeploymentAdmin	ContentAdmin	AuditAdmin
Nodes		x		
Engines		x		
Proxies	x	x		
Virtual proxies	x	x		
Schedulers		x		
Repositories		x		
Sync rules		x		
Certificates	x	x		
Reload tasks		x	x	
User sync task		x	x	
Triggers		x	x	

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.

Do the following:

1. Select **Virtual proxies** 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 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 would like a user to enter as anonymous and then be able to switch to a user account.
   - Select **Always anonymous user** if all users always should be anonymous.

The default value is **No anonymous user** and the Qlik Sense users must supply the user identity and credentials.

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

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

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 and tokens** on the QMC start page or from the **Start** ▼ drop-down menu to display the overview.
2. Click on **Login access rules**.
3. Select a rule to edit and click **Edit** in the action bar.
4. Click on **License rules** in **Associated items**.
5. Select the license rule 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.

   The **Authentication** property group contains the authentication method properties for the virtual proxies in the Qlik Sense system.

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

Property	Description	Default value
Header authentication header name	The name of the HTTP header that identifies users, when header authentication is allowed. Mandatory if you allow header authentication (by selecting either **Header authentication static user directory** or **Header authentication dynamic user directory** for the **Authentication method** property). *Header authentication only supports US-ASCII (UTF-8 is not supported).*	Blank
Header authentication static user directory	The name of the user directory where additional information can be fetched for header authenticated users. Mandatory if you allow static header authentication (by selecting **Header authentication static user directory** for the **Authentication method** property).	Blank

Property	Description	Default value
Header authentication dynamic user directory	Mandatory if you allow dynamic header authentication (by selecting **Header authentication dynamic user directory** for the **Authentication method** property). The pattern you supply must contain ‘$ud’, ‘$id’ and a way to separate them. **Example setting and matching header:** `$ud\\$id` – matches USERDIRECTORY\userid (backslashes must be escaped with an additional \) `$id@$ud` – matches userid@USERDIRECTORY ($id and $ud can be in any order) `$ud:::$id` – matches USERDIRECTORY:::userid	Blank
Windows authentication pattern	The chosen authentication pattern for logging in. If the User-Agent header contains the Windows authentication pattern string, Windows authentication is used. If there is no matching string, form authentication is used.	Windows
Authentication module redirect URI	When using an external authentication module, the clients are redirected to this URI for authentication.	Blank (default module, that is Windows authentication Kerberos/NTLM)

Property	Description	Default value
SAML host URI	The server name that is exposed to the client. This name is used by the client for accessing Qlik services, such as the QMC. The server name does not have to be the same as the machine name, but in most cases it is. You can use either http:// or https:// in the URI. To be able to use http://, you must select **Allow HTTP** on the edit page of the proxy that the virtual proxy is linked to. Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property).	Blank
SAML entity ID	ID to identify the service provider. The ID must be unique. Mandatory if you allow SAML authentication (by selecting **SAML** for the **Authentication method** property).	Blank
SAML metadata IdP	The metadata from the IdP is used to configure the service provider, and is essential for the SAML authentication to work. A common way of obtaining the metadata is to download it from the IdP website. Click the browse button and open the IdP metadata .xml file for upload. To avoid errors, you can click **View content** and verify that the file has the correct content and format. The configuration is incomplete without metadata.	

Property	Description	Default value
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. See: *I do not know the name of a mandatory SAML attribute (page 459)*	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'. See: *I do not know the name of a mandatory SAML attribute (page 459)*	Blank
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'.	

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.

You have set the authentication method.

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 IdP has enabled SSO, the user can access several service provider sites and applications without having to log in at each site.

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

Wikipedia: SAML 2.0

See also:

Wikipedia: Security Assertion Markup Language

Oasis SAML wiki: SAML v2.0 Standard

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 virtual proxy (page 324)*

   > *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 metadata IdP**). 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 Metadata IdP**.
   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.

See also:

- *SAML authentication (page 377)*
- *I do not know the name of a mandatory SAML attribute (page 459)*
- *Authentication methods (page 372)*

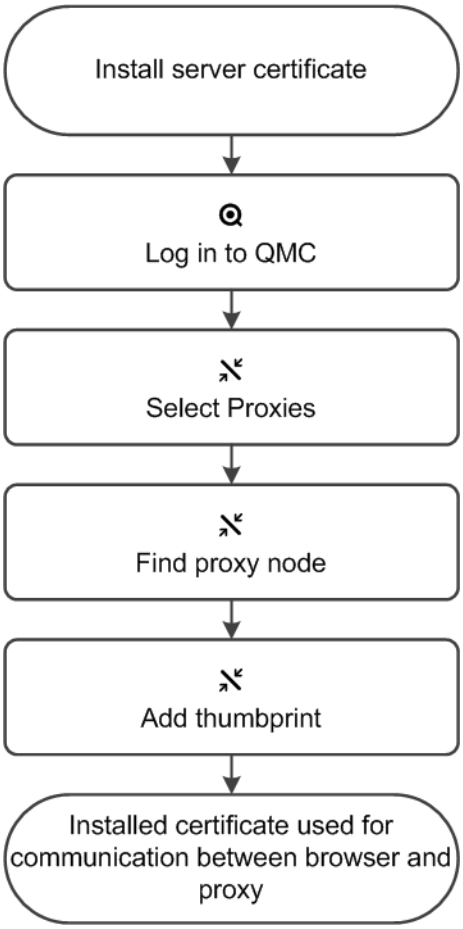
Changing proxy certificate

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.

This flow describes changing proxy certificate:



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.*

2. Log into the (QMC).
3. Select **Proxies** 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:* .

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.

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

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

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*.

Exporting certificates

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.

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*.

   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 all exported certificates.

   > *Certificates that are to be used in the Qlik Deployment Console (QDC) must be password protected.*

   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.*

5. 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**.

You have now exported the certificates.

4.3 Configuring sync 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 synchronizes the central repository database and the local repository databases.

You set up rules for the synchronization of Qlik Sense apps.

Getting to know the sync rules edit page

You can define new rules or edit existing rules from the **Security rules** page. Select **Security rules** or **Sync rules** on the QMC start page or from the **Start** ▼ drop-down menu. Select a rule and click **Edit** to open the edit page.

The following views are available under **Properties**:

- **Identification**: Displays the name of the rule and whether the rule is disabled. You can add a description.
- **Advanced**: Enables you to define all aspects of the security rule in a text based rule editor.
- **Basic**: Enables you to select target resources, attributes, and actions from drop-down lists.

*You can choose to hide or display the basic view under **Properties**.*

There is a dynamic relationship between the **Basic** and the **Advanced** views, so that updates made in one view are automatically updated in the other view.

- **Tags**: Enables you to add tags to your rule.

Under **Associated items**, you can select **Preview** to view the access rights that your rule will create and the users they will apply to.

Creating sync rules

*If you define a rule without specifying at least one **Resource** or **User** condition, your rule will apply to all resources and/or users as indicated by **(ALL)** next to the condition heading.*

You can create sync rules.

Do the following:

1. Select **Sync rules** on the QMC start page or from the **Start** ▼ drop-down menu.
2. Click ⊕ **Create new** in the action bar.
3. Under **Identification**, give the rule a name and a description.
4. Click **Disabled** if you do not want to enable the rule at this time.
5. In the **Basic** view, select the type of actions you want to create a rule for.
6. Select a resource condition in the drop-down lists.
   For example selecting the resource condition `name` and setting `name` equal to *MyApp* means that the rule applies to the app named *MyApp* while setting it equal to *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 can ungroup them by clicking **Ungroup**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that OR is superior to AND.*

> *Changing the **Create rule from template** selection automatically clears all **Actions**, and changes the **Advanced > Conditions** text box accordingly.*

Resource

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.

Property name	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.

7. Click the **Preview** tab under **Associated items** to view the access rights that your rule will create and the resources they apply to.

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

8. Click **Apply** in the action bar to create and save the rule or click **Cancel** to discard changes. **Successfully added** is displayed at the bottom of the page.

You have now created a new sync rule.

See also:

- *Resource edit page (page 28)*
- *Creating streams (page 227)*
- *Writing security rules (page 421)*
- *Security rule conventions (page 422)*

Previewing how sync rules affect node privileges

The **Preview** under **Associated items** on the **Sync rule edit** page is similar to the search results page in the **Audit** page. The **Preview** shows the node access rights to resources according to the sync rule properties that you define.

Inactive users are not shown.

Do the following:

1. On the **Sync rule edit** page, define the properties and click **Preview**.
   The results are displayed in **Grid** mode by default, but you can toggle between the **List** and **Grid** views.
   By default, the first round of query results are presented for 10 resources and 20 users. To see more click **See more items** at the bottom of the page.

2. Select a property to filter the results on from one or more of the drop-down lists above the search results.
   The list or grid is automatically filtered according to your selections.
   The default selection for all properties, with the exception of **Display**, is **All**. Next to **All** you see the number of available property items, if any.
3. Select further properties to filter on as required.

   *You can see the number of resources that the query returned in the drop-down filter that has the resource's name. To reset the filtering, set all the properties to **All**.*

4. In **Grid** display mode the types of access that apply to each resource and user are shown using a set of icons.
   See: *Audit properties (page 69)*.

5. In **Grid** display mode, clicking on an item in the matrix opens the **Applicable rules** window.
   The **Applicable rules** window includes a series of tabs each containing more details on the rules, resources, and users associated with the user and resource you selected. The rules are color coded.

Color	Description
Green	Successful validation of the rule.
Yellow	Successful validation of the rule. But the rule is disabled.
Red	Invalid rule due to invalid conditions in the system rule setup.

   Click **Edit** to go to the Edit view of the selected resource or **OK** to close the window.

   Items that can be clicked on are highlighted in green when you move the cursor over them.

6. In **Grid** display mode, selecting an **Action** to filter on shows you the number of rules that exist per resource and user.
   Click on a number to open the **Applicable rules** window for more details on those rules.
7. In **List** display mode, clicking on an item opens a separate window with more details on the selected item.
   Click **Edit** to go to the edit view of the selected resource or **OK** to close the window.

You have now previewed and filtered a sync rule.

See also:

Audit properties (page 69)

Editing sync rules

You can edit sync rules that you have update rights to.

Do the following:

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

   You can filter a column by using the filtering option: .

2. Select the rule you want to edit.
3. Click **Edit** in the action bar.
4. Edit the applicable fields for the rule.

   *You can change the text in the **Resource** text box of the **Advanced** view, but this will not affect the resource type selection.*

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

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.

Property name	Description
owner.environment.ip	Owner property associated with the app. See corresponding owner property for description.
owner.environment.os	Owner property associated with the app. See corresponding owner property for description.
owner.environment.secureRequest	Owner property associated with the app. See corresponding owner property for description.
owner.name	The user name of the owner of the resource.
owner.userDirectory	The user directory of the owner of the resource.
owner.userId	The user id of the owner of the resource.
stream.@<customproperty>	Owner property associated with the app. See corresponding owner property for description.
stream.name	The name of the associated stream.

5. Click **Disabled** if you do not want to enable the rule at this time.
6. Click the **Preview** tab to view the access rights that your rule will create and the resources they apply to.

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

7. Click **Apply** in the action bar to save the edited rule or click **Cancel** to discard changes. **Successfully updated** is displayed at the bottom of the page.

You have now edited a sync rule.

See also:

- *Resource edit page (page 28)*
- *Creating security rules (page 399)*
- *Previewing how security rules affect user privileges (page 409)*
- *Creating streams (page 227)*

Deleting sync rules

You can delete sync rules that you have delete rights to.

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

Do the following:

1. Select **Sync 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**.

You have now deleted the selected sync rules.

Creating sync rules with custom properties

Your company has a number of multi-node Qlik Sense installations that are spread out geographically across several countries. You need to create synchronization rules for all of your nodes.

You can set sync rules on individual nodes. However, given the multi-node scenario it will be easier to manage synchronization if you group nodes. Here you can consider grouping nodes by country, by function or both.

The following example will show how you can group nodes by both geography and function. Let's assume that you have one multi-node installation per geography. Here you want to create sync rules to synchronize each department 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 Geographies.
   a. Apply the custom property to the **Resource types Nodes**.
   b. Create the following values for the custom property Geographies: *USA*, *Canada*, and *Mexico*.
2. Add the custom property Geographies and Departments to the appropriate nodes.

   *In this example the nodes with names including *F001 are located in Canada, *F002 in the USA and *F003 in Mexico.*

   a. Select the appropriate nodes in the **Nodes** overview (using multi-select).
   b. For example, set custom property **Geographies** to *Canada* and set the property **Departments** to *Sales*.
   c. Repeat for all geographies and departments.
3. Create a sync rule that enables *Sales* nodes to synchronize apps in the sales streams on the **Central** node.

a. Create a sync rule for **Resource** *App* and **Resource type** *resource.stream.@department* = *Sales*.
   This means that the sync rule will apply to all apps in streams that have the custom property **Departments** set to the value *Sales*.
b. Set the Node access conditions to @Geographies = Canada and @Departments = Sales.
   This means that the sync rule will only apply to nodes with the custom properties **Geographies** set to *Canada* and **Departments** set to *Sales*.
c. Repeat for all geographies and departments.

You have now made it possible to administer node synchronization using geographies and departments.

5 Designing access control

There are concepts that are fundamental to understanding how to design access control in Qlik Sense. The following sections describe these concepts together with the conventions, rule syntax and editor with which you build and activate your attribute-based security rules.

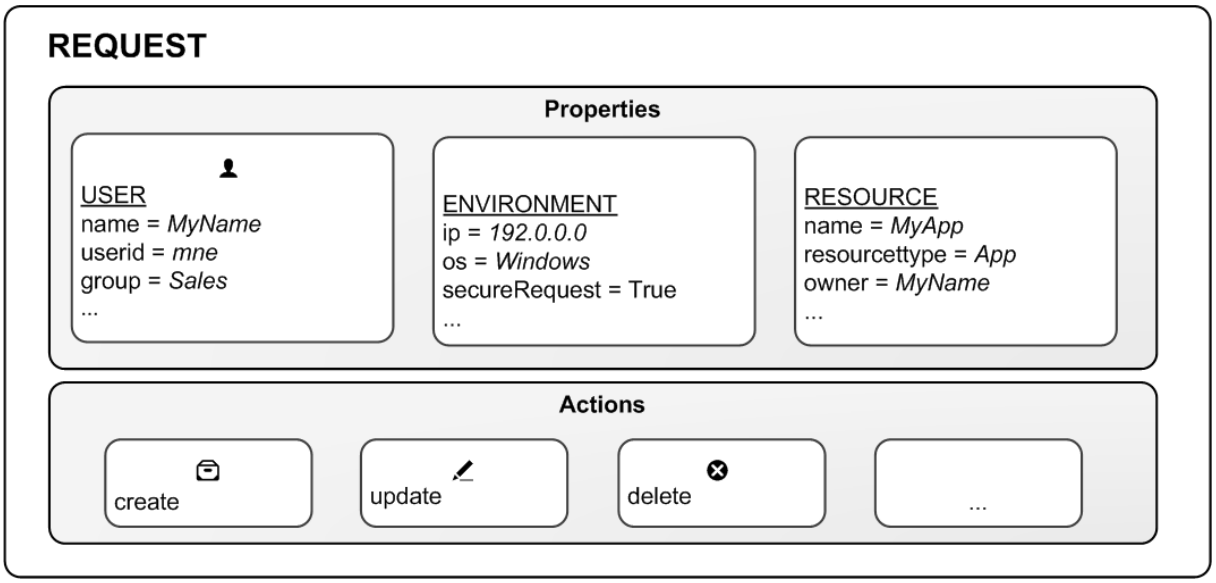
- Access control is property-based
- Security rules are inclusive by design

5.1 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:

- **User** making the request
- **Environment** the request is made from
- **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 QMC's 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 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

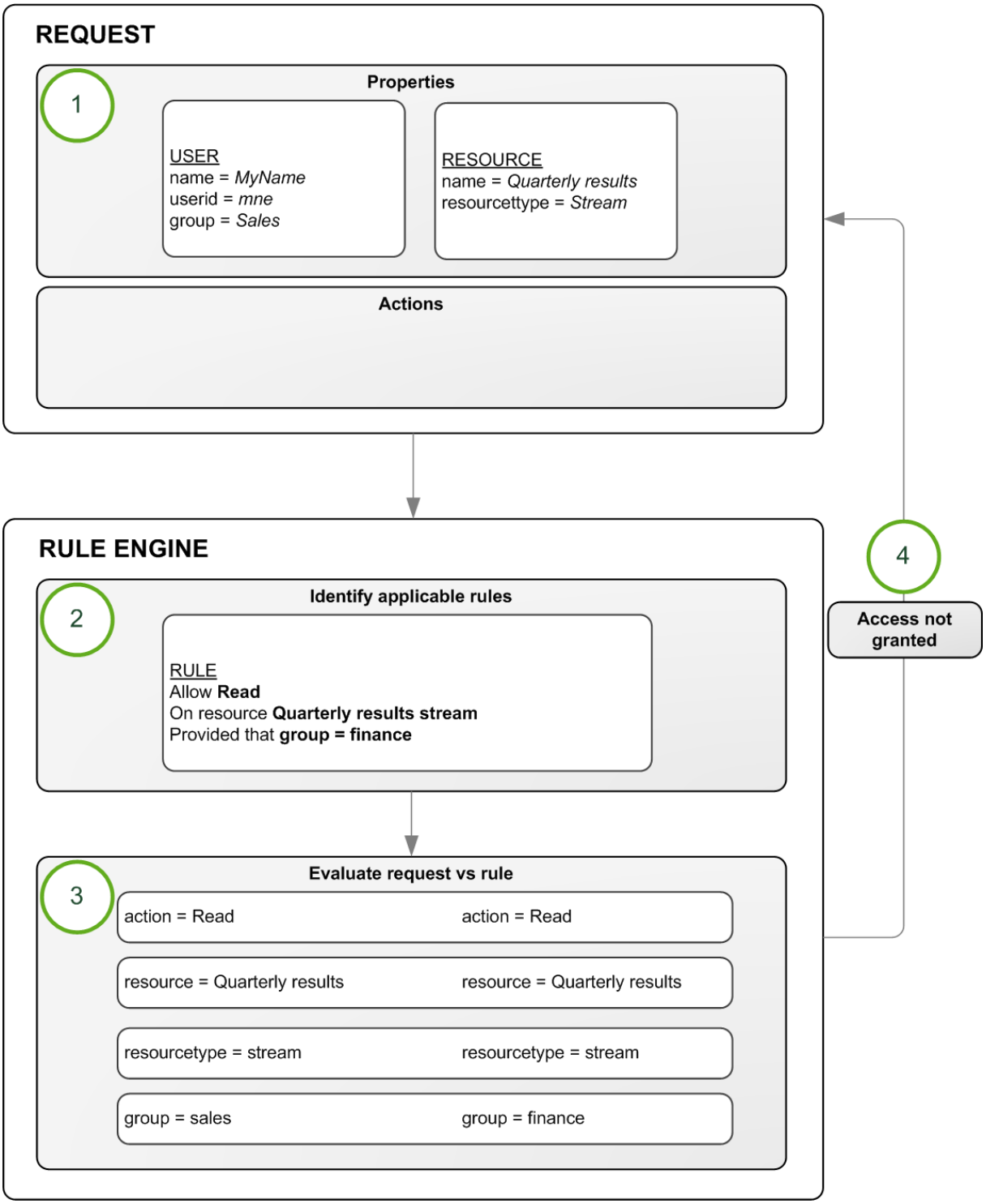
Example: One property-value pair in conditions:

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:

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 of the QMC 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.*

See also:

- *Security rules evaluation (page 394)*
- *Writing security rules (page 421)*

5.2 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
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
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		

See also:

- *Property-based access control (page 391)*
- *Writing security rules (page 421)*
- *Auditing access control (page 452)*
- *Previewing rules (page 455)*

Defining customized roles in the QMC (page 279)

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 68)*.

You can also preview the effects of a rule.

See: *Previewing how security rules affect user privileges (page 409)*.

Example 1:

In the example *One property-value pair in conditions: (page 392)* 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
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 OR office=UK	group=Management	User has read access to the stream
Evaluates to	FALSE	TRUE	TRUE
Resulting access for Sales director	**Provide** read access		

5.3 Getting to know the security rules edit page

You can define new rules or edit existing rules from the **Security rules** page. Select **Security rules** or **Sync rules** on the QMC start page or from the **Start** ▼ drop-down menu. Select a rule and click **Edit** to open the edit page.

The following views are available under **Properties**:

- **Identification**: Displays the name of the rule and whether the rule is disabled. You can add a description.
- **Advanced**: Enables you to define all aspects of the security rule in a text based rule editor.
- **Basic**: Enables you to select target resources, attributes, and actions from drop-down lists.

*You can choose to hide or display the basic view under **Properties**.*

There is a dynamic relationship between the **Basic** and the **Advanced** views, so that updates made in one view are automatically updated in the other view.

- **Tags**: Enables you to add tags to your rule.

Under **Associated items**, you can select **Preview** to view the access rights that your rule will create and the users they will apply to.

Creating security rules

You can create security rules.

> *If you define a rule without specifying at least one **Resource** or **User** condition, your rule will apply to all resources and/or users as indicated by **(ALL)** next to the condition heading.*

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.
   This opens the **Security rule edit** page.
3. In the **Identification** view, select the type of resource you want to create a rule for from the **Create rule from template** drop-down list.

   > *Changing the **Create rule from template** selection automatically clears all **Actions**, and changes the **Advanced > Conditions** text box accordingly.*

   Resource

Property	Security rule will be applied to
Unspecified	Access rules
App access	Apps
App object access	Objects The Objects' objectTypes, for example: sheet, story, bookmark, measure, or dimension.
Content library access	Content libraries
Data connection access	Data connections
Extension access	Extensions
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 sync task access	User synchronization tasks

For example, if you create an **App access rule** 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*.

> *When using a wildcard (*), you must use the "`like`" operator, instead of "=".*

4. 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 can ungroup them by clicking **Ungroup**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that OR is superior to AND.

   Resource condition

Property name	Available in	Description
@<customproperty>	App, App.Object, DataConnection, ReloadTask, ServerNodeConfiguration, Stream, Task	The custom property associated with the resource.
resource.@<customproperty>	App.Object, ReloadTask	The custom property associated with the resource.
app.name	App.Object, ReloadTask	The name of the associated app.
app.owner.@<customproperty>	ReloadTask	The custom property associated to the stream of an app. See the corresponding owner property for a description.
app.owner.email	ReloadTask	Owner property associated with the app. See the corresponding owner property for a description.
app.owner.environment.browser	ReloadTask	Owner property associated with the app. See corresponding owner property for description.

Property name	Available in	Description
app.owner.environment.context	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.device	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.ip	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.os	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.secureRequest	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.group	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.name	ReloadTask	The user name of the owner of the resource.
app.owner.userDirectory	ReloadTask	The user directory of the owner of the resource
app.owner.userId	ReloadTask	The user id of the owner of the resource
app.stream.@<customproperty>	App.Object, ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.stream.name	App.Object, ReloadTask	The name of the associated stream.

Property name	Available in	Description
category	SystemRule	The system rule category: License, Security or Sync.
description	User	The description of the owner retrieved from the user directory.
email	User	The email addresses that are available from the connected user directories.
environment.browser	User	Security rule will be applied to the type of browser. Supported browsers: Chrome, Firefox, Safari, MSIE or Unknown. **Example 1:** Define browser and version: Firefox 22.0 Chrome 33.0.1750.154 *If the browser information contains a slash (/), replace it with a space.* **Example 2:** Use the wildcard (*) to include all versions of the browser: environment.browser like Chrome*

Property name	Available in	Description
environment.context	User	Security rule will be applied only to the Qlik Sense environment that the call originates from. Available preset values: ManagementAccess or AppAccess.
environment.device	User	Security rule will be applied to the type of device. Available preset values: iPhone, iPad or Default.
environment.ip	User	Security rule will be applied to an IP number.
environment.os	User	Security rule will be applied to the type of operating system. Available preset values: Windows, Linux, Mac OS X or Unknown.
environment.secureRequest	User	Security rule will be applied to the type of request. Available preset values: SSL True or False.
group	User	The group memberships of the owner retrieved from the user directory.
roles	User	A role that is associated with the user.
name	App, App.Object, DataConnection, Extension, License.LoginAccessType, ReloadTask, ServerNodeConfiguration, Stream, User, UserDirectory, UserSyncTask, SystemRule,	The name of the resource or user.

Property name	Available in	Description
objectType	App.Object	The type of app object. Available preset values: story, masterobject, properties, sheet, dimension.
owner.@<customproperty>	App, App.Object, DataConnection, Extension, Stream	The custom property associated with the owner of the resource.
owner.description	App, DataConnection, Extension, Stream	The description of the owner retrieved from the user directory.
owner.email	App, App.Object, DataConnection, Extension, Stream	The email of the owner retrieved from the user directory.
owner.environment.browser	App, App.Object, DataConnection, Extension, Stream	The browser environment of the owner of the resource.
owner.environment.context	App, App.Object, DataConnection, Extension, Stream	Security rule will be applied only to the Qlik Sense environment that the call originates from. Available preset values: ManagementAccess or AppAccess.
owner.environment.device	App, App.Object, DataConnection, Extension, Stream	The device environment of the owner of the resource.
owner.environment.ip	App, App.Object, DataConnection, Extension, Stream	The IP environment of the owner of the resource.
owner.environment.os	App, App.Object, DataConnection, Extension, Stream	The OS environment of the owner of the resource.
owner.environment.secureRequest	App, App.Object, DataConnection, Extension, Stream	Indicates if the sent request is encrypted or not, that is using SSL or not (True or False).

Property name	Available in	Description
owner.group	App, App.Object, DataConnection, Extension, Stream	The group memberships of the owner retrieved from the user directory.
owner.name	App, App.Object, DataConnection, Extension, Stream	The user name of the owner of the resource.
owner.userDirectory	App, App.Object, DataConnection, Extension, Stream	The user directory of the owner of the resource
owner.userId	App, App.Object, DataConnection, Extension, Stream	The user id of the owner of the resource.
published	App.Object	The status of the app object.
resourceFilter	SystemRule	The existing resource definitions (from the Resource column in the security rules overview).
ruleContext	SystemRule	Specifies where the rule is to be applied: **Both in hub and QMC**, **Only in hub**, or **Only in QMC**.
stream.@<customproperty>	App	The custom property associated with the stream.
stream.name	App	The name of the associated stream.
type	SystemRule, DataConnection	The type of security rule or data connection.
userid	User	A user's ID.
userdirectory	User	The name of a user directory.
userDirectory.name	UserSyncTask	The name of the user directory connection that the user sync task applies to.

Property name	Available in	Description
userDirectory.userDirectoryName	UserSyncTask	The name of the user directory that the user directory connector is connected to.
userDirectoryName	UserDirectory	The name of the user directory connection in the QMC.

*For some resources (for example, environment.browser), you need to select **Extended security environment** in the proxy settings.*

5. Select the applicable **Actions** to assign access rights to the user for the resource.

   Action properties

Property name	Description
Create	Create resource
Read	Read resource
Update	Update resource
Delete	Delete resource
Export	Be able to export a resource to a new format, for example Excel
Publish	Be able to publish a resource to a stream
Change owner	Be able to change the owner of a resource
Change role	Be able to change user role
Export data	Be able to export data from an object

6. 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 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.
email	The email addresses that are available from the connected user directories.
group	The group memberships of the owner retrieved from the user directory.
environment.browser	Security rule will be applied to the type of browser. Supported browsers: Chrome, Firefox, Safari, MSIE or Unknown. **Example 3:** Define browser and version: Firefox 22.0 Chrome 33.0.1750.154 *If the browser information contains a slash (/), replace it with a space.* **Example 4:** Use the wildcard (*) to include all versions of the browser: environment.browser = Chrome*
environment.context	Security rule will be applied only to the Qlik Sense environment that the call originates from. Available preset values: ManagementAccess or AppAccess.

Property	Description
environment.device	Security rule will be applied to the type of device. Available preset values: iPhone, iPad or Default.
environment.ip	Security rule will be applied to an IP number.
environment.os	Security rule will be applied to the type of operating system. Available preset values: Windows, Linux, Mac OS X or Unknown.
environment.secureRequest	Security rule will be applied to the type of request. Available preset values: SSL True or False.

7. In the **Identification** property, give the security rule a name in the **Name** text box.
   Name properties

Property	Description
Name	The name of the rule.

8. Click **Disabled** if you do not want to enable the rule at this time.
9. In the **Advanced** view, select where the rule should be applied from the **Context** drop-down list.
   Context properties

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

10. Click the **Preview** tab to view the access rights that your rule will create and the users they apply to.
    See: *Previewing how security rules affect user privileges (page 409)*

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

11. Click **Apply** in the action bar to create and save the rule or click **Cancel** to discard changes.
    Successfully added is displayed at the bottom of the page.

You have now created a new security rule.

See also:

- *Writing security rules (page 421)*

- *Security rules examples (page 439)*
- *Operators and functions for conditions (page 426)*
- *Security rules properties (page 73)*
- *Creating streams (page 227)*
- *Allocating user access (page 255)*
- *Security rule conventions (page 422)*
- *Overlapping rules (page 397)*

Previewing how security rules affect user privileges

The **Preview** under **Associated items** in the **Security rule** edit page is similar to the search results page in the **Audit** page. The **Preview** shows the user access rights to resources as defined by the security rule that you are defining on the security rules edit page.

> *Inactive users are not shown.*

Do the following:

1. Define a rule on the **Security rule edit** page and click **Preview** under **Associated items**.
   The results are displayed in **Grid** mode by default, but you can toggle between the **List** and **Grid** views.

   > *By default, the first round of query results are presented for 10 resources and 20 users. To see more click **See more items** at the bottom of the page.*

   Could not determine a distinct resource for preview, please use the audit tool instead is displayed if the system cannot return a result.

2. Select a property to filter the results on from one or more of the drop-down lists above the search results.
   The list or grid is automatically filtered according to your selections.
   The default selection for all properties, with the exception of **Display**, is **All**. Next to **All** you see the number of available property items, if any.
3. Select further properties to filter on as required.

   > *You can see the number of resources that the query returned in the drop-down filter that has the resource's name. To reset the filtering, set all the properties to **All**.*

4. In **Grid** display mode the types of access that apply to each resource and user are shown using a set of icons.
   See: *Audit properties (page 69)*.

5. In **Grid** display mode, clicking on an item in the matrix opens the **Applicable rules** window.
   The **Applicable rules** window includes a series of tabs each containing more details on the rules, resources, and users associated with the user and resource you selected. The rules are color coded.

Color	Description
Green	Successful validation of the rule.
Yellow	Successful validation of the rule. But the rule is disabled.
Red	Invalid rule due to invalid conditions in the system rule setup.

   Click **Edit** to go to the Edit view of the selected resource or **OK** to close the window.

   Items that can be clicked on are highlighted in green when you move the cursor over them.

6. In **Grid** display mode, selecting an **Action** to filter on shows you the number of rules that exist per resource and user.
   Click on a number to open the **Applicable rules** window for more details on those rules.
7. In **List** display mode, clicking on an item opens a separate window with more details on the selected item.
   Click **Edit** to go to the edit view of the selected resource or **OK** to close the window.
8. Click **Edit rule** to edit the rule you are previewing.

You have now filtered a security rule preview.

See also:

- *Audit properties (page 69)*
- *Audit (page 68)*

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.

*Rules that are specific to streams and data connections can be created and changed from the **Streams** and **Data connections** pages.*

Do the following:

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

   You can filter a column by using the filtering option: ⊽.

2. Select the rule you want to edit.
3. Click **Edit** in the action bar.
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 can ungroup them by clicking **Ungroup**. The default operator between conditions is OR. You can change this in the operator drop-down list. Multiple conditions are grouped so that OR is superior to AND.*

   Resource

Property	Security rule will be applied to
Unspecified	Access rules
App access	Apps
App object access	Objects The Objects' objectTypes, for example: sheet, story, bookmark, measure, or dimension.
Content library access	Content libraries
Data connection access	Data connections
Extension access	Extensions
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 sync task access	User synchronization tasks

   Resource condition

Property name	Available in	Description
@<customproperty>	App, App.Object, DataConnection, ReloadTask, ServerNodeConfiguration, Stream, Task	The custom property associated with the resource.
resource.@<customproperty>	App.Object, ReloadTask	The custom property associated with the resource.
app.name	App.Object, ReloadTask	The name of the associated app.
app.owner.@<customproperty>	ReloadTask	The custom property associated to the stream of an app. See the corresponding owner property for a description.
app.owner.email	ReloadTask	Owner property associated with the app. See the corresponding owner property for a description.
app.owner.environment.browser	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.context	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.device	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.ip	ReloadTask	Owner property associated with the app. See corresponding owner property for description.

Property name	Available in	Description
app.owner.environment.os	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.environment.secureRequest	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.group	ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.owner.name	ReloadTask	The user name of the owner of the resource.
app.owner.userDirectory	ReloadTask	The user directory of the owner of the resource
app.owner.userId	ReloadTask	The user id of the owner of the resource
app.stream.@<customproperty>	App.Object, ReloadTask	Owner property associated with the app. See corresponding owner property for description.
app.stream.name	App.Object, ReloadTask	The name of the associated stream.
category	SystemRule	The system rule category: License, Security or Sync.
description	User	The description of the owner retrieved from the user directory.
email	User	The email addresses that are available from the connected user directories.

Property name	Available in	Description
environment.browser	User	Security rule will be applied to the type of browser. Supported browsers: Chrome, Firefox, Safari, MSIE or Unknown. **Example 1:** Define browser and version: Firefox 22.0 Chrome 33.0.1750.154 *If the browser information contains a slash (/), replace it with a space.* **Example 2:** Use the wildcard (*) to include all versions of the browser: environment.browser like Chrome*
environment.context	User	Security rule will be applied only to the Qlik Sense environment that the call originates from. Available preset values: ManagementAccess or AppAccess.
environment.device	User	Security rule will be applied to the type of device. Available preset values: iPhone, iPad or Default.
environment.ip	User	Security rule will be applied to an IP number.

Property name	Available in	Description
environment.os	User	Security rule will be applied to the type of operating system. Available preset values: Windows, Linux, Mac OS X or Unknown.
environment.secureRequest	User	Security rule will be applied to the type of request. Available preset values: SSL True or False.
group	User	The group memberships of the owner retrieved from the user directory.
roles	User	A role that is associated with the user.
name	App, App.Object, DataConnection, Extension, License.LoginAccessTyp e, ReloadTask, ServerNodeConfiguration, Stream, User, UserDirectory, UserSyncTask, SystemRule,	The name of the resource or user.
objectType	App.Object	The type of app object. Available preset values: story, masterobject, properties, sheet, dimension.
owner.@<customproperty>	App, App.Object, DataConnection, Extension, Stream	The custom property associated with the owner of the resource.
owner.description	App, DataConnection, Extension, Stream	The description of the owner retrieved from the user directory.

Property name	Available in	Description
owner.email	App, App.Object, DataConnection, Extension, Stream	The email of the owner retrieved from the user directory.
owner.environment.browser	App, App.Object, DataConnection, Extension, Stream	The browser environment of the owner of the resource.
owner.environment.context	App, App.Object, DataConnection, Extension, Stream	Security rule will be applied only to the Qlik Sense environment that the call originates from. Available preset values: ManagementAccess or AppAccess.
owner.environment.device	App, App.Object, DataConnection, Extension, Stream	The device environment of the owner of the resource.
owner.environment.ip	App, App.Object, DataConnection, Extension, Stream	The IP environment of the owner of the resource.
owner.environment.os	App, App.Object, DataConnection, Extension, Stream	The OS environment of the owner of the resource.
owner.environment.secureRequest	App, App.Object, DataConnection, Extension, Stream	Indicates if the sent request is encrypted or not, that is using SSL or not (True or False).
owner.group	App, App.Object, DataConnection, Extension, Stream	The group memberships of the owner retrieved from the user directory.
owner.name	App, App.Object, DataConnection, Extension, Stream	The user name of the owner of the resource.
owner.userDirectory	App, App.Object, DataConnection, Extension, Stream	The user directory of the owner of the resource

Property name	Available in	Description
owner.userId	App, App.Object, DataConnection, Extension, Stream	The user id of the owner of the resource.
published	App.Object	The status of the app object.
resourceFilter	SystemRule	The existing resource definitions (from the Resource column in the security rules overview).
ruleContext	SystemRule	Specifies where the rule is to be applied: **Both in hub and QMC**, **Only in hub**, or **Only in QMC**.
stream.@<customproperty>	App	The custom property associated with the stream.
stream.name	App	The name of the associated stream.
type	SystemRule, DataConnection	The type of security rule or data connection.
userid	User	A user's ID.
userdirectory	User	The name of a user directory.
userDirectory.name	UserSyncTask	The name of the user directory connection that the user sync task applies to.
userDirectory.userDirectoryName	UserSyncTask	The name of the user directory that the user directory connector is connected to.
userDirectoryName	UserDirectory	The name of the user directory connection in the QMC.

Action properties

Property name	Description
Create	Create resource
Read	Read resource
Update	Update resource
Delete	Delete resource
Export	Be able to export a resource to a new format, for example Excel
Publish	Be able to publish a resource to a stream
Change owner	Be able to change the owner of a resource
Change role	Be able to change user role
Export data	Be able to export data from an object

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 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.
email	The email addresses that are available from the connected user directories.
group	The group memberships of the owner retrieved from the user directory.

Property	Description
environment.browser	Security rule will be applied to the type of browser. Supported browsers: Chrome, Firefox, Safari, MSIE or Unknown. **Example 3:** Define browser and version: Firefox 22.0 Chrome 33.0.1750.154 *If the browser information contains a slash (/), replace it with a space.* **Example 4:** Use the wildcard (*) to include all versions of the browser: environment.browser = Chrome*
environment.context	Security rule will be applied only to the Qlik Sense environment that the call originates from. Available preset values: ManagementAccess or AppAccess.
environment.device	Security rule will be applied to the type of device. Available preset values: iPhone, iPad or Default.
environment.ip	Security rule will be applied to an IP number.
environment.os	Security rule will be applied to the type of operating system. Available preset values: Windows, Linux, Mac OS X or Unknown.
environment.secureRequest	Security rule will be applied to the type of request. Available preset values: SSL True or False.

Name properties

Property	Description
Name	The name of the rule.

Context properties

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

5. Click the **Preview** tab to view the access rights that your rule will create and the users they apply to. See: *Previewing how security rules affect user privileges (page 409)*

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

6. Click **Apply** in the action bar to save the edited rule or click **Cancel** to discard changes. **Successfully updated** is displayed at the bottom of the page.

You have now edited a security rule.

> *Updates to the security rules will not immediately take effect in a client if the client has more 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.*

See also:

- *Creating security rules (page 399)*
- *Creating streams (page 227)*
- *Security rules examples (page 439)*

Deleting security rules

You can delete security rules that you have delete rights to.

> *If a resource is deleted, all sync 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**.

You have now deleted the selected security rules.

5.4 Writing security rules

Security rules are written in the security rules editor.

> *You can specify where a security rule should apply: **Both in hub and QMC**, **Only in hub** or **Only in QMC**. This is done using the **Context** property when creating or editing a security rule. For example, the RootAdmin rule applies in the QMC only as the RootAdmin would otherwise have access, and see, all content in Qlik Sense.*

The following describes:

- The security rule editor
- Security rule conventions
- Security rule examples

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**.

The security rules editor has several properties. You can create basic security rules, or use the **Conditions** field in the **Advanced** section to edit the rule details and create more advanced security rules, or you can write the rule directly in the **Conditions** text box.

> *If you create rules using the **Advanced** section, note that you will need to specify the **Actions** in the **Basic** section.*

> *Rules that are specific to streams and data connections can be created and changed from the **Streams** and **Data connections** pages.*

When do I use the **Basic** section?

The **Basic** section provides an efficient way to either create:

- Rules that apply to one resource type only
- The base for more advanced rules

Creating rules for one resource type only

Using the **Create rule from template** drop down (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 432)*.

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. See *Functions for conditions (page 424)*.

Backtracking between the **Advanced** and **Basic** sections

To enable synchronization between the **Basic** and **Advanced** sections (so called backtracking), extra parenthesis 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.

Security rule conventions

In general a rule can read as a sentence:

```
"Allow the requester to [action] the [resource] provided that
[conditions]."
```

This section describes the action, resource, conditions, and other properties that can be used to build a rule.

You can create rules for users that are not yet in the system or resources that do not yet exist in the system. This enables you to proactively create rules. However, the rules cannot evaluate until the users are authenticated in the system or the resources, such as apps, actually exist.

Reading the security rule syntax notation

The security rules syntax notation is as follows:

- words written outside brackets in regular text are mandatory (required).
- words or characters written in **bold** outside or inside brackets are mandatory.
- words written in *italic* inside brackets are optional.
- words in green in the syntax descriptions are links to further information on the syntax.

Security rule properties

Name

A name to identify the security rule. (MANDATORY)

Disabled

Select to disable the security rule. The effect of disabled rules can still be evaluated using the preview or the audit tool. (OPTIONAL)

Description

A short description of the intention with the rule. (OPTIONAL)

Resource filter

A mandatory definition of the type or types of resources that the security rule will be evaluated for. (MANDATORY)

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

Context

You can specify whether the security rule should apply: **Both in hub and QMC**, **Only in hub** or **Only in QMC**.

Actions

A mandatory definition of the actions that the user will be allowed to perform on the resources if the rule evaluates to True. (MANDATORY)

```
action [, action]
```

Tags

You can add QMC tags to the security rule. (OPTIONAL)

Conditions for security rules

Define resource and/or user conditions that should be met for the rule to apply. (OPTIONAL).

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 **User** condition, your rule will apply to all resources and/or users as indicated by **(ALL)** next to the condition heading.*

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

Functions for conditions

The QMC includes several predefined functions that can be used to return property values from targeted resources.

IsAnonymous

Boolean function for user conditions that returns True if the user requesting access has logged in as anonymous. Otherwise returns False.

```
user.IsAnonymous()
```

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.

```
resource.HasPrivilege("action")
```

IsOwned

Boolean function **for resource conditions** that returns True if the specified resource has an owner. Otherwise returns False.

```
resource.IsOwned()
```

Empty()

Boolean function for resource conditions that returns True if the specified resource has no connections. Otherwise returns False.

> *In practice this function is only valid in situations where resource filter is set to App_* as apps are the only resource that can be connected with multiple resources (in this case streams).*

```
resource.Streams.Empty()
```

Operators for conditions

AND

This operator compares two expressions and returns True only if both evaluate to True.

```
(EXPRESSION) && (EXPRESSION)
(EXPRESSION) and (EXPRESSION)
```

OR

This operator compares two expressions and returns True if one or both evaluate to True.

```
(EXPRESSION) || (EXPRESSION)
```

```
(EXPRESSION) or (EXPRESSION)
```

EQUAL

This operator is not case sensitive and returns True if the compared expressions are equal. The full list does not have to match when a value used in an expression exists in a list.

```
(EXPRESSION) = (EXPRESSION)
```

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.

```
(EXPRESSION) == (EXPRESSION)
```

NOTEQUAL

This operator is not case sensitive and returns True if the compared expressions are not equal. The full list does not have to match when a value used in an expression exists in a list.

```
(EXPRESSION) != (EXPRESSION)
```

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.

```
(EXPRESSION) !== (EXPRESSION)
```

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.

```
!(EXPRESSION)
```

LIKE

The security rules editor supports the regular expression operator "like". This operator is not case sensitive.

```
(EXPRESSION) like (EXPRESSION)
```

MATCHES

The security rules editor supports the regular expression operator "matches". This operator is case sensitive and returns only results that exactly match your expression.

```
(EXPRESSION) matches (EXPRESSION)
```

See also:

- *Properties (page 438)*
- *Defining resource filters (page 432)*
- *Previewing how security rules affect user privileges (page 409)*

Operators and functions for conditions

The QMC includes several predefined functions that can be used to return property values from targeted resources.

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 not case sensitive and returns True if the compared expressions are 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 = "uk"** in the access request.	`resource.@org = "UK"` evaluates to True because the operator is not case sensitive.
Given that **@org = "UK"** in the access request.	`resource.@org = "UK"` evaluates to True.
Given that **@org = "United Kingdom"** in the access request.	`resource.@org = "UK"` evaluates to False.
`resource.groups = user.groups`	Evaluates to True if the properties for the groups are the same, irrespective of case. Otherwise False.

LIKE

The security rules editor supports the regular expression operator "like". This operator is not case sensitive.

For more information, see applicable javascript documentation.

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. *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 = "UK"** in access request	`!(resource.@org = "UK")` evaluates to False.
Given that **@org = "US"** in access request	`!(resource.@org = "UK")` evaluates to True.

MATCHES

The security rules editor supports the regular expression operator "matches". This operator is case sensitive and returns only results that exactly match your expression.

For more information see applicable javascript documentation.

Syntax:

```
(EXPRESSION) matches (EXPRESSION)
```

Examples and results:

Example	Result
`resource.name matches ".*yAp.*"`	Evaluates all resources with names containing "*yAp*" to True.
`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 not case sensitive and returns True if the compared expressions are 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 = "uk"** in the access request	`resource.@org != "UK"` evaluates to False because the operator is not case sensitive.
Given that **@org = "UK"** in the access request	`resource.@org != "UK"` evaluates to False.
Given that **@org = "United Kingdom"**in the access request	`resource.@org != "UK"` evaluates to True.
`resource.groups = user.groups`	Evaluates to False if the properties of the groups are the same irrespective of case. Otherwise True.

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 = "united States"** in the access request	`resource.@org == "United States"` evaluates to False because the operator is case sensitive.
Given that **@org = "United States"**in the access request	`resource.@org == "United States"` evaluates to True
Given that **@org = "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 = "united States"**in the access request	`resource.org !== "United States"` evaluates to True because the operator is case sensitive.
Given that**org = "United States"** in the access request	`resource.org !== "United States"` evaluates to False.
Given that **org = "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: `*` **Conditions:** `resource.resourcetype = "App"` `and resource.Stream.HasPrivilege("read")` **Action:** `read`	The user will be given read access to the app provided that the user has read privileges to the stream that the resource is published to.

See also:

- *Conditions (Advanced view) (page 76)*
- *Security rule conventions (page 422)*

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_*` **Conditions:** `user.IsAnonymous()` **Action:** `read`	Anonymous users are allowed to read streams.
Resource filter: `Stream_*` **Conditions:** `!user.IsAnonymous()` **Action:** `read, publish`	All users that are **not anonymous** (notice the NOT operator, !, in front of the condition) are allowed to read and publish streams. Anonymous users will have no access to streams.

See also:

- *Conditions (Advanced view) (page 76)*
- *Security rule conventions (page 422)*

Empty

Boolean function for resource conditions that returns True if the specified resource has no connections. Otherwise returns False.

Syntax:

```
resource.resourcetype.Empty()
```

Examples and results:

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

See also:

- *Conditions (Advanced view) (page 76)*
- *Security rule conventions (page 422)*

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: `*` **Conditions:** `resource.IsOwned() and resource.owner = user` **Action:** `read, export, publish`	The owner of a resource should be able to read, export and publish his / her resources. Here the conditions specify that the resource must be owned and the owner must be the requesting user for the rule to apply. *This is the definition of the OwnerNonModificationActions rule, a custom rule supplied with the QMC. Complements the Owner rule that provides resource owners with all actions provided that the resource is not published to a stream.*

See also:

- *Conditions (Advanced view) (page 76)*
- *Security rule conventions (page 422)*

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 rules either in the Audit page, the Security rules overview or 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: **Resource*** `App*` **Conditions*** `resource.resourcetype="App" and ( )`
`Stream_88ee46c6-5e9a-41a7-a66a-f5d8995454ec`	The rule applies to the stream with the specified GUID.

Defining multiple resource types

Type the names of the resource types you want to apply the rule to in the Resource filter field. You can write explicit resource names that include the resource GUID or use wildcards to imply all resources of a specific type.

> *If you define a rule without specifying at least one **Resource** or **User** condition, your rule will apply to all resources and/or users as indicated by **(ALL)** next to the condition heading.*

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.

See also:

- *Resource filter (Advanced view) (page 74)*
- *Available resource filters (page 434)*

Security rule conventions (page 422)

Available resource filters

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

Resource filter	Filter will target	Used in Security rule
*	All resources	Owner QMC, RootAdmin, ServiceAccount
App*	All resources with the resource type beginning with "App"	ContentAdmin, DeploymentAdmin, SecurityAdmin, Stream
App_*	All App resources	CreateApp, DeploymentAdminAppAccess, ExportAppData
AppAccessType_*	All AppAccessType resources	DeploymentAdmin
AppAccessUsage_*	All AppAccessUsage resources	DeploymentAdmin
AppBookmark_*	All AppBookmark resources	CreateAppComponents, ReadAppComponents
AppCalendar_*	All AppCalendar resources	CreateAppComponents, ReadAppComponents
App.Data_*	All App.Data resources	CreateAppComponents QMC,
App.DataSegment_*	All App.Data resources	ReadAppDataSegments, UpdateAppDataSegments
AppGroup_*	All AppGroup resources	CreateAppComponents, ReadAppComponents
App.Object_*	All App.Object resources	OwnerCanEditPrivateObjectsInPublished Apps
AppProperties_*	All AppProperties resources	CreateAppComponents, ReadAppComponents
AppScript_*	All AppScript resources	CreateAppComponents, ReadAppComponents
App.Sheet_*	All App.Sheet resources	CreateAppComponents
AppSlide_*	All AppSlide resources	CreateAppComponents, ReadAppComponents
AppSlideItem_*	All AppSlideItem resources	CreateAppComponents, ReadAppComponents

Resource filter	Filter will target	Used in Security rule
AppSnapshot_*	All AppSnapshot resources	CreateAppComponents, ReadAppComponents
App.Story_*	All App.Story resources	CreateAppComponents
AppUndo_*	All AppUndo resources	CreateAppComponents, ReadAppComponents
AppVariable_*	All AppVariable resources	CreateAppComponents, ReadAppComponents
CompositeEvent_*	All CompositeEvent resources	ContentAdmin
ContentLibrary_*	All ContentLibrary resources	ContentAdmin
CustomProperty*	All CustomProperty resources	ContentAdmin, DeploymentAdmin, SecurityAdmin
DataConnection_*	All DataConnection resources	ContentAdmin, DataConnection, SecurityAdmin, FolderDataConnection
Engine*	All resources with names beginning with "Engine"	DeploymentAdmin
Extension_*	All Extension resources	Extension
FileReference_*	The FileReference resource	ReadFileReference
License_*	All License resources	AuditAdminQmcSections, ContentAdminQmcSections, DeploymentAdmin, DeploymentAdminQmcSections, SecurityAdminQmcSections
License*	All License resources	DeploymentAdmin
LoadbalancingSelectList	The LoadbalancingSelectList resource	DeploymentAdminQmcSections
LoginAccessUsage_*	All LoginAccessUsage resources	DeploymentAdmin
Proxy*	All resources with names beginning with "Proxy"	DeploymentAdmin, SecurityAdmin
QmcSection_AccessRule	The QmcSectionAccessRule resource	SecurityAdminQmcSections
QmcSection_App	The QmcSectionApp resource	ContentAdminQmcSections, DeploymentAdminQmcSections, SecurityAdminQmcSections
QmcSection_App.Object	The QmcSectionApp.Object resource	SecurityAdminQmcSections, ContentAdminQmcSections

Resource filter	Filter will target	Used in Security rule
QmcSection_ App.Sheet	The QmcSectionApp.Sheet resource	ContentAdminQmcSections, SecurityAdminQmcSections
QmcSection_ App.Story	The QmcSectionApp.Story resource	ContentAdminQmcSection, SecurityAdminQmcSections
QmcSection_Audit	The QmcSectionAudit resource	AuditAdminQmcSections, ContentAdminQmcSections, SecurityAdminQmcSections
QmcSection_ Certificates	The QmcSectionCertificate resource	DeploymentAdminQmcSections, SecurityAdminQmcSections
QmcSection_ CompositeEvent	The QmcSectionCompositeEvent resource	ContentAdminQmcSections
QmcSection_ ContentLibrary	The QmcSectionContentLibrary resource	SecurityAdminQmcSections, ContentAdminQmcSections
QmcSection_ CustomPropertyDefiniti on	The QmcSectionCustomPropertyDefin ition resource	ContentAdminQmcSections, DeploymentAdminQmcSections, SecurityAdminQmcSections
QmcSection_ DataConnection	The QmcSectionDataConnection resource	ContentAdminQmcSections, SecurityAdminQmcSections
QmcSection_ EngineService	The QmcSectionEngineService resource	DeploymentAdminQmcSections
QmcSection_Event	The QmcSectionEvent resource	ContentAdminQmcSections
QmcSection_Extension	The QmcSection_Extension resource	ContentAdminQmcSections
QmcSection_License*	The QmcSectionLicense resource	DeploymentAdminQmcSections
QmcSection_ ProxyService	The QmcSectionProxyService resource	DeploymentAdminQmcSections, SecurityAdminQmcSections
QmcSection_ ReloadTask	The QmcSectionReloadTask resource	ContentAdminQmcSections
QmcSection_ RepositoryService	The QmcSectionRepositoryService resource	DeploymentAdminQmcSections
QmcSection_ SchedulerService	The QmcSectionSchedulerService resource	DeploymentAdminQmcSections
QmcSection_ SchemaEvent	The QmcSectionSchemaEvent resource	ContentAdminQmcSections

Resource filter	Filter will target	Used in Security rule
QmcSection_ ServerNodeConfiguration	The QmcSectionServerNodeConfiguration resource	DeploymentAdminQmcSections
QmcSection_Stream	The QmcSectionStream resource	ContentAdminQmcSections, SecurityAdminQmcSections
QmcSection_SyncRule	The QmcSectionSyncRule resource	DeploymentAdminQmcSections
QmcSection_ SystemRule	The QmcSectionSystemRule resource	SecurityAdminQmcSections
QmcSection_Tag	The QmcSectionTag resource	AuditAdminQmcSections, ContentAdminQmcSections, SecurityAdminQmcSections
QmcSection_Task	The QmcSectionTask resource	ContentAdminQmcSections, DeploymentAdminQmcSections
QmcSection_ Templates	The QmcSectionTemplates resource	DeploymentAdminQmcSections, SecurityAdminQmcSections
QmcSection_Token	The QmcSectionToken resource	DeploymentAdminQmcSections
QmcSection_User	The QmcSectionUser resource	ContentAdminQmcSections, DeploymentAdminQmcSections, SecurityAdminQmcSections
QmcSection_ UserAccessType	The QmcSectionUserAccessType resource	
QmcSection_ UserDirectory	The QmcSectionUserDirectory resource	DeploymentAdminQmcSections
QmcSection_ UserSyncTask	The QmcSectionUserSyncTask resource	ContentAdminQmcSections
QmcSection_ VirtualProxyConfig	The QmcSectionVirtualProxyConfig resource	DeploymentAdminQmcSections, SecurityAdminQmcSections
ReloadTask_*	All ReloadTask resources	ContentAdmin, DeploymentAdmin
Repository*	All resources with names beginning with "Repository"	DeploymentAdmin
ServiceStatus_*	All ServiceStatus resources	DeploymentAdminQmcSections
Scheduler*	All resources with names beginning with "Scheduler"	DeploymentAdmin
SchemaEvent_*	All SchemaEvent resources	ContentAdmin, DeploymentAdmin

Resource filter	Filter will target	Used in Security rule
ServiceStatus_*	All ServiceStatus resources	DeploymentAdmin
ServerNodeConfiguration_*	All ServerNodeConfiguration resources	DeploymentAdmin
StaticContentReference_*	All StaticContentReference resources	Content library content, Content library manage content, Extension static content, Installed static content
Stream_*	All stream resources	ContentAdmin, SecurityAdmin
Stream_de5e4a31-c08d-48ed-8aec-85a9ea190850	The Everyone stream that has the GUID de5e4a31-c08d-48ed-8aec-85a9ea190850	StreamEveryone, StreamEveryoneAnonymous
SystemRule_*	All ServiceStatus resources	ContentAdminRulesAccess, DeploymentAdminRulesAccess, SecurityAdmin
TableDefinition*	All resources with names beginning with "TableDefinition"	ContentAdmin, DeploymentAdmin
TempContent_*	All TempContent resources	Temporary content
Tag_*	All Tag resources	AuditAdmin, ContentAdmin, DeploymentAdmin, SecurityAdmin
User*	All resources with names beginning with "User"	ContentAdmin, DeploymentAdmin, SecurityAdmin
UserAccessType_*	All UserAccessType resources	DeploymentAdmin
UserAccessUsage_*	All UserAccessUsage resources	DeploymentAdmin
UserSyncTask_*	All UserSyncTask resources	ContentAdmin, DeploymentAdmin
VirtualProxy*	All resources with names beginning with "VirtualProxy"	DeploymentAdmin, SecurityAdmin

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 connections, or you can define your own customized properties. See *Custom properties (page 439)*.

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 392)*, 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 data connections 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.

Examples:

- *Security rules example: Applying Qlik Sense access rights for user types (page 444)*
- *Creating sync rules with custom properties (page 389)*

5.5 Security rules examples

The following examples describe using and writing security rules for a number of scenarios. For more examples of properties and functions, see the syntax descriptions in *Security rule conventions (page 422)*.

Security rules example: Creating QMC content admin roles

In this example, you organize the administration of access rights for streams and their contents by:

- Creating an administrator for each stream
- Providing each administrator with full access rights to the stream and apps, sheets, and stories in the stream

You can do this by creating security rules for each individual user, but it is easier to apply security rules based on an admin role. Since there is no default administrator role for streams, you have to create one. This is done by defining a rule and then applying it to a user role.

In the example, you create an administrator for the Stream 1 stream, but the following steps can be applied to any stream.

Procedure

Do the following:

1. Select **Security rules** and click ⊕ **Create new**.
2. Type a name for the security rule in the **Name** field.
3. The resource filter for the rule should be set to filter on streams and their apps, sheets, stories, and tasks.
   In the **Advanced** section, fill in the **Resource filter** field with text as per Security rule code.
4. You now need to set the conditions to specify the resources that the rule applies to, and the user role that the rule defines.
   In the **Advanced** section, fill in the **Conditions** field with text as per Security rule code.
5. Set the actions that the rule should provide for the specified resources.
   In the **Basic** section, select the **Actions** as per Security rule code.
6. Click **Apply**.
7. You need to assign the role to the user who will be the stream administrator.
   Go to QMC > **Users**.
8. Select the user and click **Edit**.
9. Click ⊕ under **Admin roles** and select *Stream1Admin*.
10. Click **Apply**.

You have now created an administrator role for the stream named Stream1Admin.

Security rule code

The following is the security rule code for this example, with explanatory comments:

Field	Code	Comments
Resource filter	`Stream_*, App_*, App.Object_*, ReloadTask_*`	Specifically filters on resource types Stream, App, AppObjects and ReloadTasks *Alternatively you could write `App*` instead of `App_*, App.Object_*` as using the wildcard (*) without the underscore (_). This implies all resource types beginning with App will be targeted.*

Field	Code	Comments

Conditions	`user.roles = "Stream1Admin" and ((resource.resourcetype="Stream" and resource.name="Stream 1") or (resource.resourcetype="App" and resource.stream.name="Stream 1") or (resource.resourcetype="App.Object" and resource.objectType="sheet" and resource.app.stream.name="Stream 1") or (resource.resourcetype="ReloadTask" and resource.app.stream.name="Stream 1"))`	`user.roles = "Stream1Admin" and`
		The conditions that follow define the user role Stream1Admin which will be available in Users > Roles.
		
		`((resource.resourcetype="Stream" and resource.name="Stream 1") or`
		The rule will apply to streams with the name Stream1 only. The double parenthesis at the beginning is due to the preceding AND statement.
		
		`(resource.resourcetype="App" and resource.stream.name="Stream 1") or`
		The rule applies to all apps in Stream 1.
		
		Not specifying resource.stream.name means that you give access to all apps.
		
		`(resource.resourcetype="App.Object" and resource.objectType="sheet" and resource.app.stream.name="Stream 1") or`
		The rule applies to all sheets in Stream 1.
		
		`(resource.resourcetype="ReloadTask" and resource.app.stream.name="Stream 1"))`
		The rule applies to all reload tasks in Stream 1. The double parenthesis at the end is due to the AND statement in conjunction with the `user.roles` condition.

Actions	`create, read, update, delete, export, publish, changeOwner, changeRole, exportData`	The actions will be granted provided that the conditions are met.

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** per Security rule code.
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. Select **Apps**, *Ctrl*+click to select more than one app 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 resource.@Department=user.@Department and (resource.resourcetype="App" or (resource.resourcetype="ReloadTask" or resource.resourcetype="App.Object") or resource.resourcetype="SchemaEvent" or resource.resourcetype="CompositeEvent" or resource.resourcetype="Tag")`	The rule will apply to all users that have the user role set to `DepartmentAdmin` .
Actions	`create, read, update, delete, publish`	The actions will be granted provided that the conditions are met.

Field	Code	Comments
Context	**Only in QMC**	The rule is only valid when you use the QMC.

Security rules example: Applying Qlik Sense access rights for user types

In this example, you set access rights according to user types. Your development department comprises the following user types:

- Developer: is allowed to create apps, sheets, stories, objects and can use and create data connections.
- Contributor: is allowed to create stories and sheet towards 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, DataConnection.

You set access rights according to user types by using security rules in the following main steps:

1. Define each type of user in such a way that makes it possible to apply rules to each type of user 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 type of activity.

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** per Security rule code.
   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 types apps.

Field	Code	Comments

Conditions	`!user.IsAnonymous() and (user.@usertype="Developer")`	`!user.IsAnonymous()`
		This condition uses the security rules function `IsAnonymous` that can be used to evaluate if the user is logged in as anonymous. In this case, if the user is logged in as Anonymous the rule will NOT apply.
		`(user.@usertype="Developer")`
		The rule will apply to all users that have the custom property `@usertype` set to `Developer`.
		Alternatively, if you have a user directory with a corresponding group you can use that instead of custom properties. In this case the condition could look like this: `user.group="Developer"`.

Action	`create`	The specified actions will be provided to 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 types App.Object.
Conditions	`resource.App.HasPrivilege("read") and !user.IsAnonymous() and (user.@usertype="Developer" or user.@usertype="Contributor")`	`resource.App.HasPrivilege("read") and` This condition uses a security rules function HasPrivelege that can be used to evaluate access rights for resourcetypes. In this instance the function evaluates if the resourcetype user is allowed to perform the action update on the resource sheet. This means that Contributors will be allowed to create objects for sheets that he or she owns.
Actions	`create`	The specified actions will be granted provided the conditions are met.

Security rule code for "Data connections"

Field	Code	Comments
Resource filter	`DataConnection_*`	Specifically filters on data connections.

Field	Code	Comments

Conditions	`resource.resourcetype = "DataConnection" and (user.@usertype="Developer")`	`resource.resourcetype = "DataConnection" and`
		The rule will apply to resources of the type DataConnection.
		`user.@usertype="Developer"`
		The rule will apply to users with the custom property `@usertype` set to "Developer".

Actions	`create`	Create action will be granted provided that the conditions are met.

Security rules example: Recreating document admin by creating QMC app admin

In this example, you recreate a Qlik Sense 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.

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.

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.
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.
4. Set the actions that the rule should provide.
   In the **Basic** section, fill in the **Actions** field with text as per Security rule code.

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>="<Value1a>")`	`resource.resourcetype="Stream"`
		The rule applies to streams.
		`(user.environment.<Attribute1>="<Value1a>")`
		The rule applies to the users where the attribute equals the value.

Actions	`read`	Read actions will be granted provided that the conditions are met.

6 Auditing access control

The QMC includes the following audit tools that enable you to review and preview access rights and the security rules that provide them:

- Audit page: Verify that access rights comply with your company's security policies.
- Preview page: See the effects that a new or edited rule will have without disrupting your system.

The auditing tools enable you to view the rules that apply to a resource. This means that you can verify access rights, identify overlapping security rules and ultimately streamline your security rule architecture.

> *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 in 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 them 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 **Resources** drop-down list and set `name = Quarterly reports`.
3. Click **Audit**.
   The results view to the right shows a grid. The rows of the grid show user IDs, while the columns show the streams (in this case only the stream Quarterly reports).
   For each user, the grid shows symbols that correspond to the access rights that the user has to the stream.
   Finance users should have Read and Other 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. This means that a user missing from the list has no access to the resource.

   > *The list will always include the RootAdmin user since that user has full access. Depending on the selected resource, the other Admin roles will also show in the grid.*

4. Click a cell in the grid (do not click on an admin user) corresponding to a user belonging to the Finance

department.
The **Applicable rules** dialog 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 rules:

- Stream_read_Quarterly reports
- Stream_publish_Quarterly reports

5. Click on a cell in the grid (do not click on an admin user) corresponding to a user belonging to the Sales department.
The **Applicable rules** dialog 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 rules:
   - Stream_read_Quarterly reports

See also:

- *Audit (page 68)*
- *Defining an audit query (page 453)*
- *Viewing and filtering audit query results (page 454)*

6.1 Defining an audit query

You can query for security or sync rules.

Do the following:

1. Select the type of audit that you want to perform by clicking either the **Security rules** or **Sync rules** radio button.
2. Select the type of resource you want to audit from the **Resources** drop-down list.
By default the **name** property with a wild card search criteria appear in both the **Resources** and the **Users** drop-down lists. This means that the query returns all resources of the selected type.

   > *You must select a type of resource and at least one Resource and User condition in your query; otherwise your query cannot return any results.*

   The number of items that match your criteria are shown in parenthesis next to the property heading. The matching items for each type of condition are independent of each other.
3. Change the query conditions as required or click ⊕ to add further resource and/or user conditions to your query.
4. Use the context drop-down list to specify whether the security rule is used **Both in hub and QMC**, **Only in hub** or **Only in QMC**.

5. You can enter environment conditions for your query in the **Client environment filter** text field. For example: *OS=Windows; IP=10.88.3.35*.
6. Click **Audit** to perform the query.
   The results view is automatically updated with the results, if any, of your query.

You have now defined an audit query.

See also:

- *Viewing and filtering audit query results (page 454)*
- *Audit (page 68)*

6.2 Viewing and filtering audit query results

You can filter the query results using the drop-down property lists.

> *You can only view security rules that you have access rights to read.*

Do the following:

1. Define a query and click **Audit** as appropriate.
   The query results are shown in the right hand side of the **Audit** page.
   The results are displayed in **Grid** mode by default, but you can toggle between the **List** and **Grid** views.

   > *Inactive users are not shown.*

2. Select a property to filter the results on from one or more of the drop-down lists above the search results.
   The list or grid is automatically filtered according to your selections.
   The default selection for all properties, with the exception of **Display**, is **All**. Next to **All** you see the number of available property items, if any.
3. Select further properties to filter on as required.

   > *You can see the number of resources that the query returned in the drop-down filter that has the resource's name. To reset the filtering, set all the properties to **All**.*

4. In **Grid** display mode the types of access that apply to each resource and user are shown using a set of icons.
   See: *Audit properties (page 69)*.
5. In **Grid** display mode, clicking on an item in the matrix opens the **Applicable rules** window.

The **Applicable rules** window includes a series of tabs each containing more details on the rules, resources, and users associated with the user and resource you selected. The rules are color coded.

Color	Description
Green	Successful validation of the rule.
Yellow	Successful validation of the rule. But the rule is disabled.
Red	Invalid rule due to invalid conditions in the system rule setup.

Click **Edit** to go to the Edit view of the selected resource or **OK** to close the window.

> *Items that can be clicked on are highlighted in green when you move the cursor over them.*

6. In **Grid** display mode, selecting an **Action** to filter on shows you the number of rules that exist per resource and user.
   Click on a number to open the **Applicable rules** window for more details on those rules.
7. In **List** display mode, clicking on an item opens a separate window with more details on the selected item.
   Click **Edit** to go to the edit view of the selected resource or **OK** to close the window.

You have now filtered a list and viewed the details of one or more items.

See also:

- *Audit properties (page 69)*
- *Defining an audit query (page 453)*
- *Audit (page 68)*

6.3 Previewing rules

The **Preview** page enables you to view the effects that your access or sync rules will have when you apply and enable them in your Qlik Sense system.

The preview page is similar to the audit page except that there is no search view. Instead the **Results** view is preloaded with filter settings that correspond to the security rule you are creating or editing.

To preview a rule, create or edit the rule as per normal and then click **Preview** under **Associated items**.

See also:

- *Previewing how security rules affect user privileges (page 409)*
- *Previewing how sync rules affect node privileges (page 385)*

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.

A Windows dialog is displayed when I try to browse to the QMC

Possible cause

You are using Windows Server 2012.

Proposed action

In the Windows dialog, log in and browse to the QMC.

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

Restart 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 software.

Possible cause

The required port is not available, because the port is used by another software, for example, 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.

7.2 Troubleshooting - Managing QMC resources

This section describes problems that can occur when managing QMC resources.

Error message: **400 Bad request**

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 Sense services are not allowed to communicate.
- You are trying to access a resource that you are not granted access to, according to the rule engine in the repository.

Proposed action

Remove any unused root certificates. See also the following Microsoft help documentation:

- Clients cannot make connections if you require client certificates on a Web site or if you use IAS in Windows Server 2003
- 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.

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']

Reload is not working

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*.

A task is not executed

Possible cause

The task status is not **Success**.

Proposed action

On the tasks overview page in the QMC, click ⓘ in the status column to display a summary of the execution steps.

You can also check the log file at this location: *%ProgramData%\Qlik\Sense\Log\Scheduler*.

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 254)*

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*.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 no value.

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.

An app is not migrated

An app is not migrated 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 want to change the default user account

I want to change the default Windows user account, that is used to run Qlik Sense.

Proposed action

Modify the Qlik Sense installation.

Do the following:

1. Open the **Control Panel** and select **Uninstall a program**.
2. Select Qlik Sense from the list of programs and click **Change**.
3. Select **Modify** in the Qlik Sense setup dialog.

The Windows user account can also be changed manually. This is done by modifying the user account that is used to run the Qlik Sense services and the user account that is used to access the folder where the Qlik Sense logs are stored. The default path to the Qlik Sense log folder is *%ProgramData%\Qlik\Sense\Log\<Service>*.

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 proxy certificate (page 380)*

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.

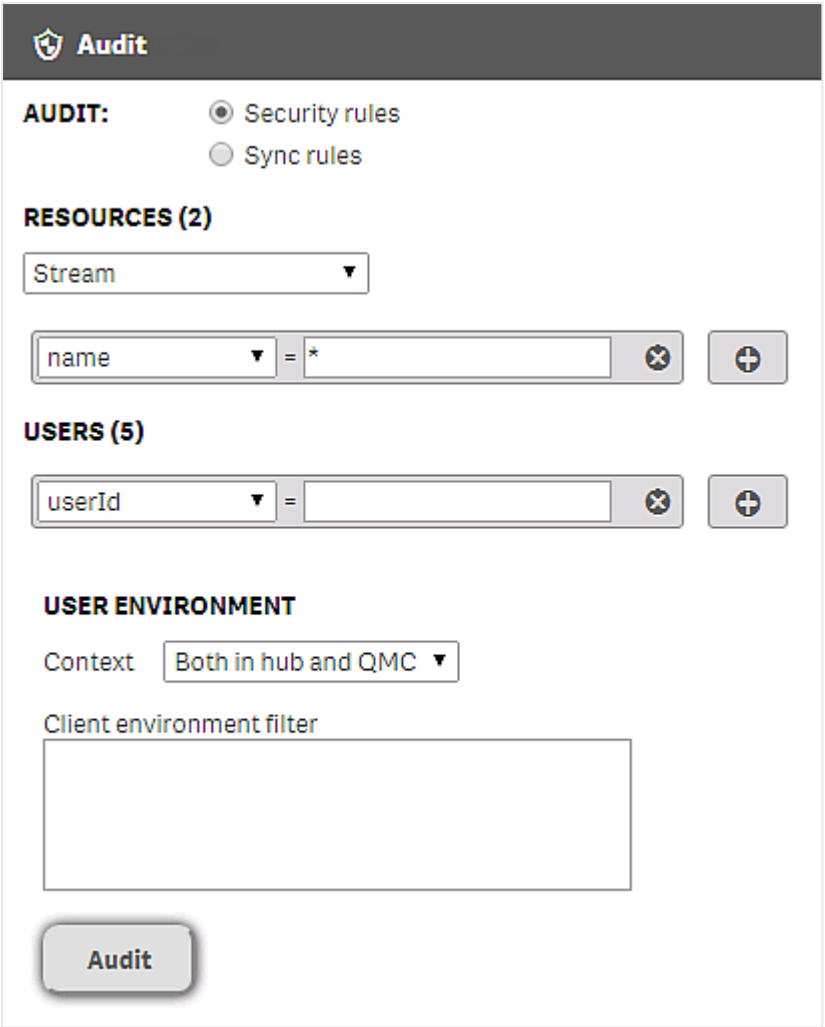
I suspect that a user can access a stream that should not be accessible

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.



See also:

- *Defining an audit query (page 453)*
- *Editing security rules (page 410)*