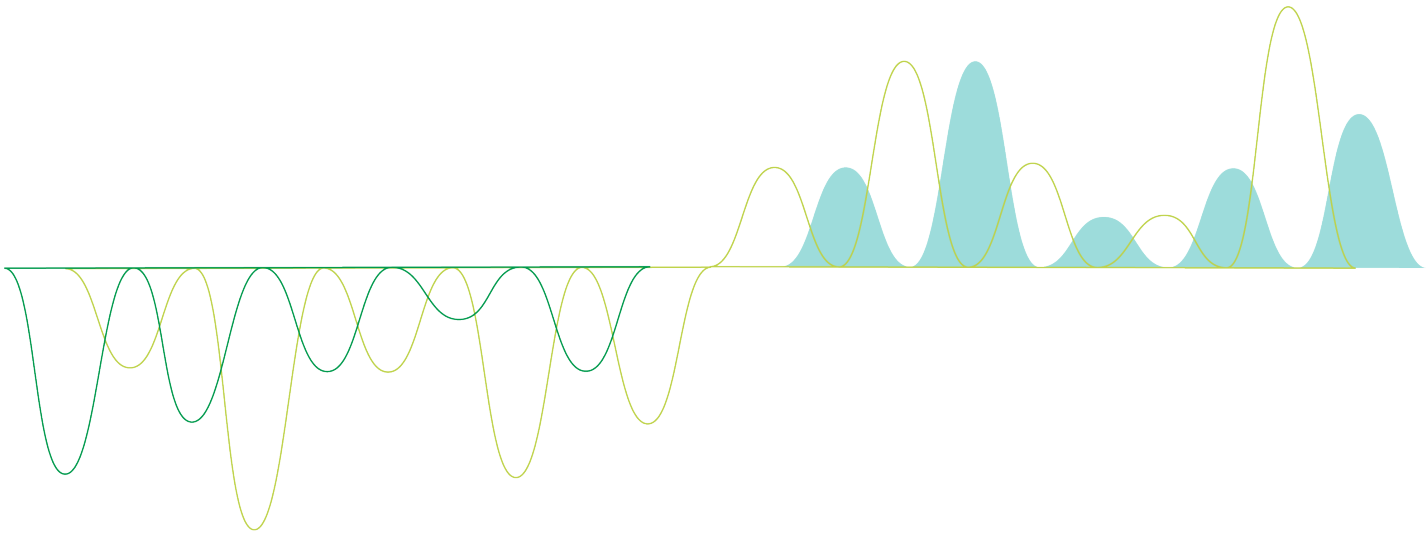
Administer Qlik Sense Enterprise on Kubernetes

Qlik Sense®
November 2019



Contents

Contents

1 Management console

The management console is used for managing licenses, user assignments, manage spaces, themes, and extensions in cloud editions of Qlik Sense. The management console should not be confused with the Qlik Management Console (QMC), which is used for managing Qlik Sense Enterprise on Windows. Only users with Tenant Admin role have access to the management console.

You access the management console by adding */console* to your tenant address: *https://<your tenant address>/console*, or by using the navigation link **Administration** under user profile in the hub.

Currently, the management console supports a fully enabled Qlik Cloud Services deployment, or a single deployment of Qlik Sense Enterprise on Kubernetes.

Here you can find an overview of the main sections that compose the management console.

1.1 Licenses

The license/user allocation section has three tabs: **Overview**, **Assigned users**, and **License key**.

Overview

Overview shows basic information about the license. In the Overview tab you can also add a license if needed.

License item	Description
Professional	**Consumed**: number of users with professional access. **Total**: Total availability of professional access.
Analyzer	**Consumed**: number of users with analyzer access. **Total**: Total availability of analyzer access.
Analyzer capacity (minutes)	**Consumed**: amount of minutes spent. **Total**: Total amount of minutes available per month. Overage is required after the total amount has been spent. **Overage**. Overage can either be limited, to the amount stated, or unlimited. For more information about analyzer capacity, see Analyzer capacity license.

Expires	Date of license expiration.
Quotas	
Shared spaces	**Consumed**: number of shared spaces. **Quota limit**: Quota limit can either be limited, to the amount stated, or unlimited.
In-memory app size	Maximum app memory size.

Assigned users

Assigned users shows information about users and license types. There are also buttons for removing assignments and assigning analyzer or professional access.

License item	Description
Name	Name of user.
User ID	Unique ID for the user.
IdP subject	User identifier in the identity provider (IdP). This value is needed when adding new users from the IdP user database.
License	License type assigned to the user: professional, analyzer, or analyzer capacity (also known as analyzer time).
Status	When the number of allocated assignments is larger than defined by the license, some users will be excluded. The users will then no longer have access to the hub or the management console. The **Status** column for the users will show *Excluded*. Those who most recently were assigned access will be excluded. They will remain excluded until the number of allocations matches the number defined by the license. If more access assignments are made available, or if the admin removes access for others, access will be reallocated to excluded users.

See also:

Assigning access to users (page 16)

License key

In the License key tab you can change a license if needed. To change the license: paste the license key in the text box and click **Submit**.

1.2 Users

The users page displays all the users that have logged into the tenant. If a user has a certain role (tenant admin), it is displayed in the roles field.

Use the search to find users. Use the buttons for assigning and removing tenant admins. For each user in the table, you also have a button to the far right where you can assign and remove the tenant admin role.

User status

The following are the available user statuses.

Status	Description	Status can be changed to
active	User is fully registered and can consume according to the assigned license.	disabled
disabled	User license is removed and that user cannot access their account or use the product.	active

1.3 Spaces

The spaces section has two tabs:

- **Overview** shows the current number of shared and managed spaces, and the creation date of the latest space.
- **Spaces** shows a table with space name, space type, space owner, description of the space, and the space creation date. You also have buttons for deleting a space, changing the owner, editing the space, and creating a new space.

The following are the space types:

- Personal spaces: In personal spaces, only the owner can edit apps, that is, you cannot co-develop in personal spaces. You can share apps outside your space, but only for viewing.
- Shared spaces: Shared spaces allow for easy co-development of apps within a closed group of users. What actions you can perform with an app in a space is determined by permissions and your license. With a professional license you can create a shared space in the hub. You can then add new members to your shared space and assign them permissions.
- Managed spaces: Managed spaces enable governed access to apps. Managed spaces are restricted to members. Permissions are assigned to members when they are added to a managed space. Permissions define what members can access in a space. Apps that you develop in a personal or shared space can be published to a managed space. Only space owners and target app consumers

can open apps in a managed space. Other users can open apps if they have viewing permissions. Managed spaces can only be created by tenant administrators.

See also:

Managing spaces in the management console (page 29)

Working in shared spaces (page 21)

1.4 Schedules

With scheduling, you can view and delete reload schedules for apps in your system. From the hub users can edit existing and create new reload schedules.

Property	Description
App	Name of the app the reload task is assigned to.
Last execution	Displays when the task was last executed.
Next execution	Displays when the task is scheduled to be executed next.
State	Displays if the reload task is enabled, disabled, completed, or failed.
Status	Shows whether the schedule is enabled or disabled.

See also:

Managing reload schedules (page 19)

1.5 Events

In the events section, you can follow up on events in your system and get information about the event type and the user who initiated the event.

Property	Description
Date	Date and time in UTC format.
Source	Source of the event information. See examples.
Event type	Type of event. See examples.
User	User initiating the event. If the user name cannot be displayed, the user ID is displayed instead. Click the arrow to the far right to display additional information from the source or event.

In the table, sort by using the arrows in the properties header and filter by using the funnel. There are buttons for refreshing and resetting after filtering.

Examples of sources:

- com.qlik/licenses
- com.qlik/engine
- com.qlik/edge-auth

Examples of events:

- app.created
- user-session.begin
- assignment.added
- assignment.revoked

1.6 Themes

In the **Themes** page of the management console, the following properties are shown.

Property	Description
Name	This is the metadata name contained in the QEXT file, which is different from the QEXT filename.
Description	Short description of the theme.
Tags	Tags for filtering.
Author	Creator of the theme.
QEXTfilename	Identifier that must be unique. Filename of the theme definition file. Different from the name of the theme.
QEXTversion	Metadata version contained in the QEXT file.
Published	Date of publishing.

In the table, sort by using the arrows in the properties header. Filter by using the **Tags** drop-down menu, or by selecting the tags in the table.

See also:

Managing themes (page 32)

1.7 Extensions

Extensions only are available in Qlik Sense Enterprise on Kubernetes and not in Qlik Sense Enterprise on Cloud Services.

In the **Extensions** page of the management console, the following properties are shown.

Property	Description
Name	This is the metadata name contained in the QEXT file, which is different from the QEXT filename.
Description	Short description of the extension.
Tags	Tags for filtering.
Author	Creator of the extension.
QEXTfilename	Identifier that must be unique. Filename of the extension definition file. Different from the name of the extension.
QEXTversion	Metadata version contained in the QEXT file.
Published	Date of publishing.

In the table, sort by using the arrows in the properties header. Filter by using the **Tags** drop-down menu, or by selecting the tags in the table.

See also:

Managing extensions (page 33)

1.8 API keys

An API key is a unique identifier used for authentication of a user, developer, or calling program to an API. API keys are often used for tracking and controlling how the interface is used, to prevent abuse of the API.

By default, the API keys are disabled in the management console. To enable the API keys, go to the *Settings (page 13)* section. A tenant admin can revoke API keys and edit the API keys settings, but to generate or delete API keys, you must have the role developer. A tenant admin assigns the role developer to a user. If you are a tenant admin, you can assign the role developer to yourself.

The API keys table shows the following information about the API keys: name, ID, owner, last update, creation date, expiry date, and status. Use the search field to search in the first three fields: **Key name**, **Key ID**, and **Owner**.

API key statuses

API keys can have the following statuses:

- Active: the API key is in use.
- Expired: the expiry date has been reached.
- Revoked: the API key has been revoked and can no longer be used.

As an admin, you can review the API key activities registered in the **Events** section in the management console. If suspicious activities are detected, such as, extensive use of a certain API key, you can revoke that API key. Open the detailed list by clicking the arrow to the far right in the table and copy the ID of the API key. You can then search for the ID in the **API keys** section to find the API key to revoke.

To revoke a single API key, click the button **...** to the far right and select **Revoke**. You can only revoke keys with the status *Active*. To revoke multiple keys, select the check boxes to the left of the keys to revoke and click **Revoke** in the top right corner. Revocation is irreversible, a revoked API key cannot be re-activated.

In addition to revocation there is the delete option. You can delete an API key from the hub, but not in the management console.

1.9 Web

You can create web integrations to add origins that are whitelisted to access the tenant. The web integration containing the whitelist is connected to an ID used in for example a mashup that is connecting to your tenant. When a request arrives, Qlik Sense Enterprise confirms that the request derives from a whitelisted domain and then approves the request, else not.

Click **...** to the far right to reach options for copying the ID, editing, or deleting the web integration.

Property	Description
Name	Name of the web integration.
ID	Unique ID assigned to the web integration when it is created.
Number of origins	Number of domains contained in the white-list.
Last updated	Displays when the web integration was last updated.
Date created	Displays when the web integration was created.

See also:

Managing web integrations (page 36)

1.10 Settings

On-demand data

On-demand apps are generated in the hub from navigation links that connect selection apps to template apps. The On-Demand App Service must be enabled to generate on-demand apps.

Property	Description
On-demand app generation	When the service is switched from enabled to disabled, any pending requests to generate on-demand apps are allowed to finish. But once the service has been disabled, no new requests to generate apps are accepted. This service is disabled by default.

Groups

Groups are used for access control of users, and can optionally be automatically created from *idp-groups*.

Property	Description
Enable auto-creation of groups	When enabled, groups are inherited from the identity provider so that access can be granted to the same groups of users that exist in the IdP. This simplifies access administration compared to granting access to one user at a time. It is required that you use single sign-on and have administrative access to your IdP to configure groups. Note that new IdP groups will show up in Qlik Sense Enterprise as users log in (or log in again) to the Qlik Sense Enterprise tenant. IdP groups are not imported all at the same time. Instead, IdP groups are discovered at login time. Further, only groups associated with users in Qlik Sense Enterprise will be available as described earlier.

Dynamic license assignment

With dynamic license assignment, you can automate assignment of access to users. For details, see: *Assigning access to users (page 16)*.

Property	Description
Enable dynamic assignment of professional access	When enabled, users who log in are automatically assigned professional access, if available.
Enable dynamic assignment of analyzer access	When enabled, and no professional access is available, users who log in are automatically assigned analyzer access, if available.

API keys

Property	Description
Enable API keys	This switch enables or disables all the API keys in the tenant. Only the tenant admin can enable the API keys.
Change maximum token expiration	By changing the token expiration value, all new tokens will have the new expiration value. Already existing APIs will not be affected by the change, they will have the same expiration value as before.
Change maximum of API keys per user	This setting only affects new API keys. If a new API key makes the total number exceed the maximum number, creation is denied.

2 Licensing Qlik Sense Enterprise on Kubernetes

When you buy a new license for cloud editions of Qlik Sense, the license key is set automatically during on-boarding. If needed, you can change the license key manually at a later moment.

The user who enters the tenant for the first time becomes tenant admin. The tenant admin can assign the role tenant admin to other users. It is required to have at least one tenant admin. To prevent accidental removal of the last tenant admin, you cannot remove the role tenant admin from yourself.

It is possible to lose the ability to repair or modify the identity provider configuration in cloud editions of Qlik Sense if the account owner has been removed as a tenant admin. If the identity provider (IdP) in use in a tenant is no longer functional and needs to be modified, it is necessary for the original tenant account owner to access the management console through the recovery URL. This will fail if this user is no longer an administrator. For more information, see Repairing or modifying your IdP when the account owner is removed as tenant admin.

Qlik Sense Enterprise on Kubernetes is licensed using a signed key. You apply your license for a Qlik Sense Enterprise on Kubernetes installation in the management console.

For an overview of the License section of the management console, see: *Management console (page 6)*.

2.1 Applying the Qlik Sense Enterprise on Kubernetes license

Do the following:

1. In the management console, navigate to the **Licenses** section.
2. In the **Overview** tab, enter the signed key in the **License key** input box.
3. Select **Submit** to apply the license.

3 Assigning access to users

Tenant admins can assign and remove access for users in the management console, on the **Assigned users** tab in the **Licenses** page.

3.1 Add access type to a user

Access types can be added to users.

Do the following:

1. Click **Add assignment**.
2. Select a user from the **Search for a user** field.
3. Select the **Access type**.
4. Click **Add**.
5. Add more users if needed and when finished click **Close**.

3.2 Remove assignment

Licenses can be removed for users.

Do the following:

1. Select the user from the list.

   You can select multiple users at the same time.

2. Click **Remove assignment**.
3. Click **Delete** to confirm the license removal.

3.3 Assign professional access to a user with analyzer access

You can assign professional access to users with analyzer access.

Do the following:

1. Select the user from the list.

   You can select multiple users at the same time.

2. Click **Assign professional access**.
3. Click **Confirm** to confirm the assignment.

3.4 Dynamic license assignment

To simplify assignment of access to users, you can enable dynamic assignment. Choose between four options:

- Dynamic assignment enabled for both professional and analyzer access:

  Professional access is assigned, if available, otherwise analyzer access. If neither of those are available, analyzer capacity is assigned, if available.

- Dynamic assignment enabled only for professional access:

  Professional access is assigned, if available, otherwise analyzer capacity is assigned, if available.

- Dynamic assignment enabled only for analyzer access:

  Analyzer access is assigned, if available, otherwise analyzer capacity is assigned, if available.

- Dynamic assignment disabled for both professional and analyzer access:

  Analyzer capacity access is assigned, if available.

You can upgrade from analyzer access to professional access, but not downgrade from professional to analyzer.

If you change to a new license key, all your assignments are removed, because they are associated with the license, not the tenant. However, if you start using the old license key again, the assignments will be present.

Enabling dynamic license assignment

With dynamic license assignment, you can automate assignment of access to users. You manage dynamic assignment in the **Dynamic license assignment** in the **Settings** page.

Property	Description
Enable dynamic assignment of professional access	When enabled, users who log in are automatically assigned professional access, if available.
Enable dynamic assignment of analyzer access	When enabled, and no professional access is available, users who log in are automatically assigned analyzer access, if available.

4 Administer tenant admins

Tenant admins are administered from the management console on the **Users** page.

The users page displays all the users that have logged into the tenant. If a user has a certain role (tenant admin), it is displayed in the roles field.

Use the search to find users. Use the buttons for assigning and removing tenant admins. For each user in the table, you also have a button to the far right where you can assign and remove the tenant admin role. If you have the invite users license, you also have options for resending or deleting user invitations.

4.1 Assign tenant admin

A tenant admin can assign the tenant admin role to other users.

Do the following:

1. Select name from list.
2. Click the **Assign tenant admin** button.
3. Confirm the role assignment.

4.2 Remove tenant admin

A tenant admin can remove the tenant admin role from other users.

Tenant admins cannot remove the tenant admin role from themselves.

Do the following:

1. Select name from list.
2. Click the **Remove tenant admin** button.
3. Confirm the role removal.

5 Managing reload schedules

With scheduling, you can view and delete reload schedules for apps in your system. From the hub users can edit existing and create new reload schedules.

5.1 Reloading app data in the management console

Apps in the cloud hub do not automatically update when their data sources are updated. Reloading an app updates it with the latest data from the app data sources. From the cloud hub, you can manually reload your apps or schedule reloads for your apps.

In addition to this, tenant admins can view and delete reload schedules from the management console. This is done on the **Schedules** tab.

Viewing a reload schedule

You can view existing reload schedules from the management console. Select the reload schedule from the list and then click **View**.

Deleting a reload schedule

Do the following:

1. Select the reload task you want to remove and then click **Delete**.

   You can remove several items at a time.

2. Confirm that you want to delete the reload task.

5.2 Reloading app data in the cloud hub

Apps in the cloud hub do not automatically update when their data sources are updated. Reloading an app updates it with the latest data from the app data sources. You can manually reload your apps or schedule reloads for your apps.

You cannot reload data in the cloud hub for apps published to the cloud hub from a Qlik Sense Enterprise deployment. Apps published from Qlik Sense Enterprise can be reloaded using the QMC in Qlik Sense Enterprise.

You can only reload apps you own.

You can view the status of current and past reloads for an app from **Reload history** in **Details**.

Scheduling reloading app data

You can create a schedule for data reloading in your app. Qlik Sense adds a reload to the reload queue at the frequency, date, and time you schedule. You can schedule a single reload of the data or schedule a repeating reload of app data.

When you schedule a single reload, you can pick a specific date and time for the reload. When you schedule a repeating reload, you can pick the interval and time of the reload. Repeating reloads can be set at the following intervals:

- Hourly
- Daily
- Weekly
- Monthly
- Yearly

You can remove a scheduled reload from an app by setting the schedule to **Inactive** and saving.

The dates and times in the schedule reload dialog use your current time zone. Qlik Sense determines your current time zone based on your browser settings.

Do the following:

1. Click on the app and select **Schedule reload**.
2. Set the schedule to active and create your schedule.

   If you cannot see the AM option when setting the reload time, use the scroll bar.
3. Click **Save**.

Manually reloading app data

You can reload an app manually, adding a reload task to the reload queue.

Do the following:

- Click on the app and select **Reload**.

Viewing reload history for your app

Reload history contains the reload history for the selected app. You can view the status, start and end times, and duration of past and current reloads. For failed reloads, you can also view error logs.

To view the reload history for an app, click on the app, select **Details**, and click **Reload history**.

6 Working in shared spaces

A shared space is a section of the cloud hub used to develop apps collaboratively and control access to apps. You can find your shared spaces using the spaces drop-down in **Explore.**

Any user with a professional license can create a space. Apps within a space can have sheets, stories, and bookmarks added to them by multiple users. Shared spaces are restricted to the members. Apps in the space can only be viewed by space members.

Permissions are assigned to members when they are added to a shared space. Permissions define what members can do in the shared space. There are four permissions in shared spaces:

- **Owner**: You are the first administrator that can manage the space and its members as well as create content in the space.
- **Is admin**: You can manage the space and its members as well as create content in the space.
- **Can edit**: You can add and edit content in apps. You cannot manage the space and its membership.
- **Can view**: You can view apps in the space, but cannot create content or manage the space.

Member permissions can be changed, giving them a different role in the space or removing them from the space.

You can create new apps directly in a shared space. You can also move apps from your personal space to your shared space so other members can work on them.

6.1 Creating shared spaces

A space's owner is the user who created the space. The owner of a space cannot be changed in the cloud hub. Space owners can be changed in the Management Console.

Space names must be unique within a cloud hub.

Do the following:

1. Click the spaces drop-down and select **Add a space**.
2. Enter a name for the space and a description for the space.
3. Click **Create**.

6.2 Adding members to shared spaces

Members can be added to the space by the owner or members with **Is admin** permission. If your tenant administrator has enabled groups, you can also add groups of users to your space.

If a member has individual permission and group permission in a space, the highest permission level is applied.

Do the following:

1. In the space, click **Manage members**.
2. Search for members by name and select the members you want to add to the space.
3. Select a permission for the members and click **Add**.
4. Click **Done**.

6.3 Editing the names and descriptions of shared spaces

You can change the name and description of the space.

Do the following:

1. In the space, click the **Edit spaces** icon.
2. Change the name and description and click **Save**.

6.4 Deleting shared spaces

You can delete a space. Deleting a space will also delete all apps in the space. Only the owner or a user with **Is admin** permission can delete a space.

1. In the space, click the **Edit spaces** icon.
2. Click **Delete**.
3. Click **Delete**.

6.5 Developing and sharing apps with shared spaces

There are different ways of developing apps collaboratively and sharing them with other members of your cloud hub. Here is a sample workflow for using shared spaces:

Create an app

Create an app in your personal space. Add data sources, create a data model, and create scheduled reloads for the app.

The creator of an app is the only user who can manage the data in an app, so the data model must be complete before the app can be collaboratively developed with other users.

Create a shared space

Add a shared space to your cloud hub for collaborative development of your app.

Move your app to the space

Once the app is ready for collaboration, move your app to your shared space.

Using apps in shared spaces (page 23)

Add users to the space
: Add collaborators to your space and assign them **Can edit** permission. Collaborators must have a professional license.

Develop apps in the space collaboratively
: All **Can edit** users can add sheets, stories, and bookmarks to the app. Their content is private until they chose to make it public in the app.
Granting access to sheets, bookmarks, and stories

Update your app
: You may receive feedback from your app audience. An app in a space can be updated at any time with changes to the data model or content in the app.

Retire an app from the shared space
: When the app is no longer required, you can delete it from the cloud hub.

Retire the space
: When the space is no longer required, you can delete it from the cloud hub.

6.6 Using apps in shared spaces

Apps can be created, developed, and shared with other members of the cloud hub in a shared space.

Apps can be created and developed in a similar way to how apps are created and shared in a personal space. Depending on your space permissions and your license, you can create and develop apps in the space. If you have **Can view** permission, you can only view the apps in the space.

For a detailed view of what you can do with apps based on your permission and license, see *Managing permissions in shared spaces (page 25)*.

Creating apps in a shared space

Users can create or upload apps in a shared space by clicking **Create** and selecting **Create app** or **Upload app**. You cannot duplicate apps to a space, but you can move apps to a space.

Tags you add to an app are shared with other members of the cloud hub, but only if they have access to your app.

Data connections are owned by the user who created the connection. Only the owner of the data connection, or the owner of the shared space it resides in, can delete the connection. The data connection can only be edited by the owner.

Users with **Can edit** permission can read, write, and load data connections and load scripts in **Data manager** or **Data load editor**. They can also create data connections to external sources and load data from those connections.

You can create on-demand selection apps in a shared space. Selection apps and template apps must be in the same space. For more information, see Creating an on-demand selection app.

Adding content to apps in shared spaces

Users with **Can edit** or **Is admin** permissions can add sheets, stories, and bookmarks to apps in the shared space. Sheets, stories, and bookmarks added to the app are private. Only the creator of the private content can see it in the app. When they are ready to be shared, the creator makes them public.

Only the space owner can edit data in the app, but other shared space members can create, edit, and delete:

- Master items
- Variables
- Media library content

Snapshots taken for stories are not shared with other users.

Shared space members with **Owner**, **Can edit**, or **Is admin** permissions can modify the following app properties:

- Selected theme
- Enable right-to-left reading order
- Setting a bookmark as app default
- Sheet title styling

Reloading apps in a shared space

Users with **Owner**, **Is admin**, and **Can edit** permissions can manually reload apps and create scheduled reloads in the space.

Moving apps between spaces

You can move apps between shared spaces as well as between a shared space and a personal space.

If you create an app in a shared space, the data connections related to it will stay in that space, even if the app moves. For example, you create an app called *QuarterlyAnalysis* in the Data Team shared space. If you move *QuarterlyAnalysis* to a different shared space, the data connections will remain in the Data Team shared space. If the data needs to be edited or reloaded, it must be done by a user with **Can edit** rights in the Data Team shared space. The same would apply if you created an app in a personal space and moved it to a shared or space.

Do the following:

1. Click on the app and select **Edit**.
2. Select the new space from **Space**.

3. To open the new space, select **Go to space**.
4. Click **Save**.

Duplicating apps in a shared space

You can duplicate apps in a shared space.

> *If an app uses section access for data, you cannot duplicate the app.*

Do the following:

- Click on the app and select **Duplicate**.

Exporting apps from shared spaces

You can export an app from a shared space as a .qvf file. Exported apps do not include any private sheets in the app.

> *If an app uses section access for data, you cannot export the app.*

Do the following:

- Click on the app and select **Export with data** or **Export without data**.

Sharing apps from shared spaces

You can add members to a space and give them **Can view** permission so they can view the apps in a space. You cannot share individual apps from a space. If you do not want to share a space with viewers, you can move the app to a space you have created for app viewers. You can also move the app to your personal space and share it with specific cloud hub members.

6.7 Managing permissions in shared spaces

Shared space permissions control access to apps in the space. They define a member's role in the shared space. Permissions are assigned to members when they are added to a space.

Any cloud hub member with a professional license can create a space. When you create a space, you are assigned the **Owner** permission. Owners can then add new members to the space and assign them permissions. Space permissions are managed in **Manage members**. In **Manage members**, you can search for cloud hub members, assign them permissions, and add them to your shared space.

Member permissions can be changed to give them a new role in a space. A user with **Can view** permission might be changed to an app developer by changing their permission to **Can edit**. Member permissions can be changed by space owners and members with **Is admin** permissions.

Members can be removed from a space in **Manage members** by clicking the delete icon beside the member.

*You can check your permissions in a shared space by clicking **Manage members**. If you do not see **Manage members**, you have **Can view** or **Can edit** permission for the space.*

Space permissions and app ownership

Your permission determines what actions you can take with apps in a space. Whether or not you are the owner of the app you are working with determines additional permissions.

The app owner is the user who has created the app. The app owner is the only user who can:

- View or edit data in **Data model viewer**, **Data load editor**, or **Data manager**.
- Manually reload or schedule a reload for the app.
- Edit app attributes (change name, description, and tags).
- Edit app properties (select theme, enable right-to-left reading order, set a bookmark as app default, and sheet title styling).

Space permissions override app ownership. If an app is moved to a space that the app owner does not have permission to access, then the app owner cannot access the app. If the app owner's permission in a space is changed to **Can view**, they will lose the ability to add data to the app and reload the app. When moving an app between spaces, ensure the app owner has **Can edit**, **Is admin**, or **Owner** permissions in the destination space, if you want the app owner to still manage reloading the app and the data model.

Permissions in a shared space

Permissions can be assigned by **Owner** and **Is admin** users. What shared space permissions enable you to do depends on if you have a professional or an analyzer license assigned to you by your tenant administrator. If your tenant administrator has enabled groups, you can also add groups of users to your space.

If a member has different individual permission and group permission in a space, the highest permission level is applied.

Permissions for members with professional licenses

The following tables outline what members with the professional license can do in a space:

Space actions by permission in a shared space

Action	Owner	Is admin	Can edit	Can view
Rename the space	Yes	Yes	No	No
Create new apps in the space	Yes	Yes	Yes	No

Action	Owner	Is admin	Can edit	Can view
Move apps to another space	Yes	Yes	Yes	No
Move apps to the space	Yes	Yes	Yes	No
Duplicate apps in the space	Yes	Yes	Yes	No
Export apps in the space	Yes	Yes	Yes	No
Add members to the space	Yes	Yes	No	No
Change member permissions for the space (**Is admin**, **Can edit**, **Can view**)	Yes	Yes	No	No
Remove members from the space	Yes	Yes	No	No
Delete the space	Yes	Yes	No	No

App actions by permission in a shared space

Action	Owner	Is admin	Can edit	Can view
Open an app	Yes	Yes	Yes	Yes
Delete an app	Yes	Yes	Yes	No
Open **Data model viewer**	Yes	Yes	Yes	No
 *The user must be the app owner.*				
Open and edit the data model in **Data load editor** or **Data manager**	Yes	No	No	No
 *The user must be the app owner.*				
Add data files to a space in **Data load editor** and **Data manager**	Yes	No	No	No
 *The user must be the app owner.*				
Edit app attributes (change name, description, and tags)	Yes	Yes	Yes	No
Edit app properties (select theme, enable right-to-left reading order, set a bookmark as app default, and sheet title styling)	Yes	Yes	Yes	No
Reload the app	Yes	Yes	Yes	No
Create, edit, and delete master items and variables	Yes	Yes	Yes	No
 *The user must be the app owner.*				

Action	Owner	Is admin	Can edit	Can view
Create, edit, and delete media library content	Yes	Yes	Yes	No
 *The user must be the app owner.*				
Add private sheets to the app	Yes	Yes	Yes	No
Add private bookmarks and stories to the app	Yes	Yes	Yes	Yes
Make private sheets, bookmarks, and stories public in the app	Yes	Yes	Yes	No
Make public sheets, bookmarks, and stories private in the app	Yes	Yes	Yes	No
Take snapshots in the app	Yes	Yes	Yes	Yes
Make snapshots public	Yes	Yes	Yes	No
View on-demand app navigation links	Yes	Yes	Yes	Yes
Create or update app navigation on-demand links	Yes	Yes	Yes	No
Open on-demand selection apps	Yes	Yes	Yes	Yes
Generate on-demand apps	Yes	Yes	Yes	Yes

Permissions for members with analyzer licenses

The following tables outline what members with an analyzer license can do in a space:

Space actions by permission in a shared space

Action	Owner	Is admin	Can edit	Can view
Change app owners	Yes	Yes		
Export apps in the space	Yes	Yes	Yes	No

App actions by permission in a shared space

Action	Owner	Is admin	Can edit	Can view
Open an app	Yes	Yes	Yes	Yes
Delete an app	Yes	Yes	Yes	No
Edit app attributes (change name, description, and tags)	Yes	Yes	Yes	No
 *The user must be the app owner.*				
Edit app properties (select theme, enable right-to-left reading order, set a bookmark as app default, and sheet title styling)	Yes	Yes	Yes	No

Action	Owner	Is admin	Can edit	Can view
The user must be the app owner.				
Add private bookmarks and stories to the app	Yes	Yes	Yes	Yes
Take snapshots in the app	Yes	Yes	Yes	Yes
View on-demand app navigation links	Yes	Yes	Yes	Yes
Open on-demand selection apps	Yes	Yes	Yes	Yes
Generate on-demand apps	Yes	Yes	Yes	Yes

6.8 Managing spaces in the management console

The spaces section has two tabs:

- **Overview** shows the current number of shared and managed spaces, and the creation date of the latest space.
- **Spaces** shows a table with space name, space type, space owner, description of the space, and the space creation date. You also have buttons for deleting a space, changing the owner, editing the space, and creating a new space.

The following are the space types:

- Personal spaces: In personal spaces, only the owner can edit apps, that is, you cannot co-develop in personal spaces. You can share apps outside your space, but only for viewing.
- Shared spaces: Shared spaces allow for easy co-development of apps within a closed group of users. What actions you can perform with an app in a space is determined by permissions and your license. With a professional license you can create a shared space in the hub. You can then add new members to your shared space and assign them permissions.
- Managed spaces: Managed spaces enable governed access to apps. Managed spaces are restricted to members. Permissions are assigned to members when they are added to a managed space. Permissions define what members can access in a space. Apps that you develop in a personal or shared space can be published to a managed space. Only space owners and target app consumers can open apps in a managed space. Other users can open apps if they have viewing permissions. Managed spaces can only be created by tenant administrators.

Changing the owner of a space

Do the following:

1. Select the spaces for which you want to change owner.
2. Click **Change owner**.
   A dialog is displayed.

3. Search for a user who will be the new owner.
4. Click **Apply**.

7 Events

In the events section, you can follow up on events in your system and get information about the event type and the user who initiated the event.

Property	Description
Date	Date and time in UTC format.
Source	Source of the event information. See examples.
Event type	Type of event. See examples.
User	User initiating the event. If the user name cannot be displayed, the user ID is displayed instead. Click the arrow to the far right to display additional information from the source or event.

In the table, sort by using the arrows in the properties header and filter by using the funnel. There are buttons for refreshing and resetting after filtering.

Examples of sources:

- `com.qlik/licenses`
- `com.qlik/engine`
- `com.qlik/edge-auth`

Examples of events:

- `app.created`
- `user-session.begin`
- `assignment.added`
- `assignment.revoked`

8 Managing themes

To manage themes in the management console, navigate to the **Themes** page. For an overview of this section of the management console, see: *Management console (page 6)*.

8.1 Adding a new theme

Do the following:

1. Click **Add** in upper the right-hand corner.
2. In the pop-up, click **Browse** to select a theme file, or drop a file in the designated area.

   You cannot upload a theme with the same QEXT filename as an existing one.
3. Optionally, add tags.
4. Click **Publish**.

Supported file formats and size

Themes only support HTML files, CSS, JSON, and images (PNG, JPEG, GIF, and SVG), along with QEXT metadata files and font files.

Maximum size of a file within a theme folder is 250 MB.

8.2 Editing a theme

You can edit one theme at a time.

Do the following:

1. To the left in the table, select the check box for the theme you want to edit.
2. In the upper the right-hand corner, click **Edit**.
   The editing panel is displayed with options for replacing the existing theme and adding or removing tags.
3. Make your edits and save.

8.3 Deleting a theme

Do the following:

1. To the left in the table, select the check boxes for the themes you want to delete.
2. In the upper the right-hand corner, click **Delete**.

Deletion of themes can affect all resources. All users within a tenant are affected by a deletion.

9 Managing extensions

Extensions only are available in Qlik Sense Enterprise on Kubernetes and not in Qlik Sense Enterprise on Cloud Services.

To manage extensions in the management console, navigate to the **Extensions** page. For an overview of this section of the management console, see: *Management console (page 6)*.

9.1 Adding a new extension

Do the following:

1. Click **Add** in upper the right-hand corner.
2. In the pop-up, click **Browse** to select an extension file, or drop a file in the designated area.

   You cannot upload an extension with the same QEXT filename as an existing one.
3. Optionally, add tags.
4. Click **Publish**.

Supported file formats and size

Extensions support all files by default, but some MIME types of files are disallowed.

Maximum size of a file within an extension folder is 250 MB.

9.2 Editing an extension

You can edit one extension at a time.

Do the following:

1. To the left in the table, select the check box for the extension you want to edit.
2. In the upper the right-hand corner, click **Edit**.
   The editing panel is displayed with options for replacing the existing extension and adding or removing tags.
3. Make your edits and save.

9.3 Deleting an extension

Do the following:

1. To the left in the table, select the check boxes for the extensions you want to delete.
2. In the upper the right-hand corner, click **Delete**.

Deletion of extensions can affect all resources. All users within a tenant are affected by a deletion.

9 Generating API keys

You can generate API keys from the hub. Before you start, make sure that the following two requirements are fulfilled:

- The setting **Enable API keys** is turned on in the management console.
- The tenant admin has assigned the role developer to you.

9.4 Generating an API key from the hub

Do the following:

1. Log onto your tenant, for example, *https://<tenantname>.com*.
2. Click your profile in the top right corner and select **Settings**.
3. Select **API** keys.
4. Click **Generate new API keys**.
5. Enter an API key description and select when the API key should expire.
6. Click **Generate**.
   An API key is generated.
7. Copy the API key and store it in a safe place.

After creation, you can edit the name of the API key. You can also delete it.

10 Managing web integrations

Web integrations are administered by tenant admins from the management console on the **Integrations** page.

10.1 Creating a new web integration

Do the following:

1. Click **Create new** in upper the right-hand corner.
2. In the dialog, give the web integration a name.
3. Type the address of the origin in the following format: *https://domain.com*. Then click **Add** to add the origin to the whitelist.

   You can add several origins.
4. Click **Create**.

10.2 Editing a web integration

Do the following:

1. Select the web integration you want to edit and then click **Edit**.
2. In the dialog, change the web integration options as wanted.
3. Click **Save**.

10.3 Deleting a web integration

Do the following:

1. Select the web integration you want to remove and then click **Delete**.

   You can remove several items at a time.
2. Confirm that you want to delete the web integration.

10.4 Copying a web integration ID for use in mashups

Do the following:

1. Select the web integration you want to copy the ID for, click **...** and then select **Copy ID**.

   The ID is copied to the clipboard.

11 Managing on-demand app generation

On-demand apps are generated in the hub from navigation links that connect selection apps to template apps. The On-Demand App Service must be enabled in the management console to generate on-demand apps.

On-demand app generation is controlled by the On-Demand App Service. Tenant admins can enable the On-Demand App Service in the management console, on the **Settings** tab. The service is disabled by default and must be enabled before selection and template apps can be linked and on-demand apps generated.

When the service is switched from enabled to disabled, any pending requests to generate on-demand apps are allowed to finish. But once the service has been disabled, no new requests to generate apps will be accepted nor will developers be able to create or edit new On-demand app navigation links. These capabilities are restored once the service is re-enabled.

11.1 Enabling and disabling on-demand app generation

To enable or disable on-demand app generation, in the management console navigate to the **Settings** page. In the **On-demand app generation (ODAG)** tab, manage the following setting:

Property	Description
On-demand app generation	When the service is switched from enabled to disabled, any pending requests to generate on-demand apps are allowed to finish. But once the service has been disabled, no new requests to generate apps are accepted. This service is disabled by default.

12 Auto-creation of groups

Groups are used for access control of users, and can optionally be automatically created from *idp-groups*.

To enable or disable auto-creation of groups, in the management console navigate to the **Settings** page.

In the **Groups** tab, manage the following setting:

Groups are used for access control of users, and can optionally be automatically created from *idp-groups*.

Property	Description
Enable auto-creation of groups	When enabled, groups are inherited from the identity provider so that access can be granted to the same groups of users that exist in the IdP. This simplifies access administration compared to granting access to one user at a time. It is required that you use single sign-on and have administrative access to your IdP to configure groups. Note that new IdP groups will show up in Qlik Sense Enterprise as users log in (or log in again) to the Qlik Sense Enterprise tenant. IdP groups are not imported all at the same time. Instead, IdP groups are discovered at login time. Further, only groups associated with users in Qlik Sense Enterprise will be available as described earlier.

13 Viewing logs in Qlik Sense Enterprise on Kubernetes

All services in Qlik Sense Enterprise on Kubernetes emit log data that can be used for debugging issues and activity. Logs can be read on demand or they can be collated and pushed to a log aggregation product for further analysis and use.

13.1 Viewing service logs

To inspect the recent logs of a service, for example to debug an issue, the Kubernetes CLI (or other Kubernetes management tools) can be used to quickly view log data.

The following assumes you have the **kubectl** tool installed and connected to your Kubernetes cluster.

Run the following to get a list of all the services running, this will also list if any services are reporting themselves as having issues.

```
Kubectl get pods
```

Identify the service you want to inspect the logs for from the list and run the following adjusting as needed.

```
Kubectl log qliksense-engine-xxxxxxx
```

This will render the recent log entries to the console in JSON format.

If a pod is not running, for example it is in a pending state, then it may not issue any log entries. You can use the following command to see what issue Kubernetes is reporting with that pods configuration:

```
kubectl describe pod qliksense-engine-XXXXX
```

There are two common reasons for a pod to not start:

- Wrong storage configuration - this will report issues about the availability of its volume claims.
- Insufficient resources - depending on the Kubernetes provider there can be insufficient resources or a limitation on how many pods can run on a node. In this instance it will report errors about pods being “unschedulable”

13.2 Collating and forwarding logs

The logs produced can be forwarded to be gathered, stored, searched and viewed all the system logs on mass in log aggregation tools.

Below is an example of using 3rd party tools including:

- Gathering your system logs in **fluentd**
- Storing your log files in **Elasticsearch**

Elasticsearch requires a significant amount of resources and is therefore not recommended to be executed on your local machine unless your Kubernetes cluster has a lot of available memory and CPU.

- Consuming your log files in **Kibana**

13.3 Installing Elasticsearch

Elasticsearch is a search engine that provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents.

In this example we install a minimum setup of **Elasticsearch**, that does not include any persistence.

1. Create a file named **elasticsearch.yaml** to configure your installation preferences, and add the following:

```
image:
  tag: "6.1.4"

client:
  replicas: 1
  resources:
    limits:
      cpu: "0.5"
      memory: "1024Mi"  ## not setting a limit here can take down the cluster using all
available memory
    # requests:   # use defaults
    #   cpu: "25m"
    #   memory: "512Mi"

master:
  persistence:
    enabled: false
  replicas: 2
  # heapSize: "512m"    ## use default, should be less than request, MUST be less than limit
  resources:
    limits:
      cpu: "0.5"
      memory: "1024Mi"  ## set a limit
    # requests:   # use defaults
    #   cpu: "25m"
    #   memory: "512Mi"

data:
  persistence:
    enabled: false
  replicas: 1
  heapSize: "512m"
  resources:
    limits:
      cpu: "0.5"
```

```
    memory: "1024Mi"
  requests:
    cpu: "25m"
    memory: "512Mi"
```

2. Run the following command to install **Elasticsearch**:
   ```
   helm upgrade --install elasticsearch incubator/elasticsearch -f ./elasticsearch.yaml
   ```

13.4 Installing fluentd

Fluentd is an open source data collector for unified logging layer. It allows you to unify data collection and consumption for a better use and understanding of data. Follow these steps to install **fluentd**.

1. Create a file named **fluentd.yaml** to configure your installation preferences, and add the following:
   ```
   elasticsearch:
     host: elasticsearch-elasticsearch-client
   ```
2. Run the following command to install **fluentd**:
   ```
   helm upgrade --install fluentd incubator/fluentd-elasticsearch -f fluentd.yaml
   ```

13.5 Installing Kibana

Kibana lets you visualize your **Elasticsearch** data and navigate the Elastic Stack. You can use it to view and search your logs. Follow these steps to install **Kibana**.

1. Create a file named **kibana.yaml** to configure your installation preferences, and add the following:
   ```
   env:
     ELASTICSEARCH_URL: http://elasticsearch-elasticsearch-client:9200
   ```
2. Run the following command to install **Kibana**:
   ```
   helm upgrade --install kibana stable/kibana -f kibana.yaml
   ```

13.6 Accessing Kibana

Run the following command to access **Kibana**:

```
export POD_NAME=$(kubectl get pods --namespace default -l "app=kibana,release=kibana" -o jsonpath="
{.items[0].metadata.name}")
echo "Visit http://127.0.0.1:5601 to access Kibana"
kubectl port-forward $POD_NAME 5601
```

In **Kibana** you can run the following query to test your setup:

```
kubernetes.container_name:engine
```

14 Monitoring metrics in Qlik Sense Enterprise on Kubernetes

All Qlik Sense Enterprise on Kubernetes services expose metrics that can be used to monitor activities, health and performance data.

The data can be surfaced and collated using open source components. The example below shows how to use Prometheus and Grafana to scrape and analyze metrics in real time.

14.1 Viewing metrics with Prometheus

Prometheus is a system monitoring and alerting toolkit that can be used for scraping and storing metrics. It collects metrics from configured targets at given intervals, evaluates rule expressions, displays the results, and can trigger alerts if some condition is observed to be true.

Prometheus finds the metrics by looking for Kubernetes annotations that have been added to the services.

```
prometheus.io/port=8080
prometheus.io/scrape=true
```

Installing the Prometheus chart

Run the following command to install the **stable/prometheus** chart.

Adjust the configuration of your cluster settings, such as RBAC.

```
helm upgrade --install prometheus stable/prometheus --
set=rbac.create=true,alertmanager.enabled=false,pushgateway.enabled=false
```

Viewing the metrics

View the metrics with the following command:

```
export POD_NAME=$(kubectl get pods --namespace default -l
"app=prometheus,release=prometheus,component=server" -o jsonpath="{.items[0].metadata.name}")
echo "Visit http://127.0.0.1:9090 to access prometheus"
kubectl port-forward $POD_NAME 9090
```

14.2 Viewing metrics with Grafana

Grafana is another tool for monitoring and analyzing metrics.

Installing Grafana

Run the following command to install Grafana:

```
helm upgrade --install grafana stable/grafana -f grafana.yaml
```

The example YAML file referenced in the command above provides the following abilities:

- Configure Grafana to look at Prometheus metrics.
- Preload a GO Services dashboard for exposing Golang metrics.
- Preload a Kubernetes dashboard with general metrics.
- Preload a Kubernetes container details dashboard with more specific POD metrics.

See the Online help for full code example.

Viewing the metrics

Run the following command to retrieve your admin user password:

```
kubectl get secret --namespace default grafana -o jsonpath="{.data.admin-password}" | base64 --decode
; echo
```

In the same shell, run the following command to retrieve the Grafana URL:

```
export POD_NAME=$(kubectl get pods --namespace default -l "app=grafana,release=grafana" -o jsonpath="
{.items[0].metadata.name}")
echo "Visit http://127.0.0.1:3000 to access grafana"
export GRAFANA_PASSWORD=$(kubectl get secret --namespace default grafana -o jsonpath="{.data.admin-
password}" | base64 --decode ; echo)
echo "Login as admin:$GRAFANA_PASSWORD"
kubectl port-forward $POD_NAME 3000
```