A MITEL
PRODUCT
GUIDE

Mitel Virtual Care Collaboration Service

Mitel Virtual Care Collaboration Service System Administration

Administrator Documentation
09/2024

A31003-V9910-M103-06-76A9

Mitel

Contents

1 Overview..4

2 Accessing Virtual Care Collaboration Service Administration app..................5
2.1 Logging in with your Virtual Care Collaboration Service credentials..................5
2.2 Logging in with Single Sign On (SSO)..................6
2.3 Resetting your password..................6
2.4 Logging out..................7

3 Multi-tenancy support..................8
3.1 Root tenant management..................8
3.1.1 Creating a root tenant..................9
3.1.2 Viewing root tenants..................9
3.1.3 Searching for a root tenant..................9
3.1.4 Renaming a root tenant..................10
3.1.5 Configuring license settings for a root tenant..................10
3.1.6 Configuring chat settings for a root tenant..................10
3.1.7 Configuring SAML 2.0 authentication for a root tenant..................11
3.1.7.1 Configuring a SAML 2.0 identity provider..................12
3.1.7.2 Editing a SAML 2.0 identity provider..................12
3.1.7.3 Enabling or Disabling tenant-wide Single Sign On..................13
3.1.8 Deleting a root tenant..................14
3.2 Root tenant administrator management..................14
3.2.1 Creating a root tenant administrator..................14
3.2.2 Viewing root tenant administrators..................15
3.2.3 Editing a root tenant administrator..................15
3.2.4 Deleting a root tenant administrator..................16

4 Metrics..................17
4.1 Viewing metrics..................17

5 API key management..................19
5.1 Creating an API key..................19
5.2 Viewing API keys..................19
5.3 Searching for an API key..................20
5.4 Revoking an API key..................20
5.5 Deleting an API key..................21

6 Settings..................22
6.1 Changing the language settings..................22
6.2 Activating a license..................22
6.3 Reporting an issue..................23

1 Overview

Mitel Virtual Care Collaboration Service Administration app is a web-based interface that allows you to manage Mitel Virtual Care Collaboration Service. This guide describes how to make use of the Administration app as a system administrator.

A tenant in Virtual Care Collaboration Service can either map to a complete organization or a specific unit, department, or other entity within an organization. A tenant can have subordinate (child) tenants which in turn can have further child tenants under them, thus establishing a tenant hierarchy. The tenant hierarchy can have up to 4 levels.

As a system administrator, with the administration app you can easily:

- Create and manage root-level tenants or simply root tenants on Virtual Care Collaboration Service
- Create and manage administrators for root tenants
- View metrics for your Virtual Care Collaboration Service
- Create and manage API keys to integrate with third-party applications.

2 Accessing Virtual Care Collaboration Service Administration app

2.1 Logging in with your Virtual Care Collaboration Service credentials

You can log in to the Virtual Care Collaboration Service Administration app using your Virtual Care Collaboration Service account credentials.

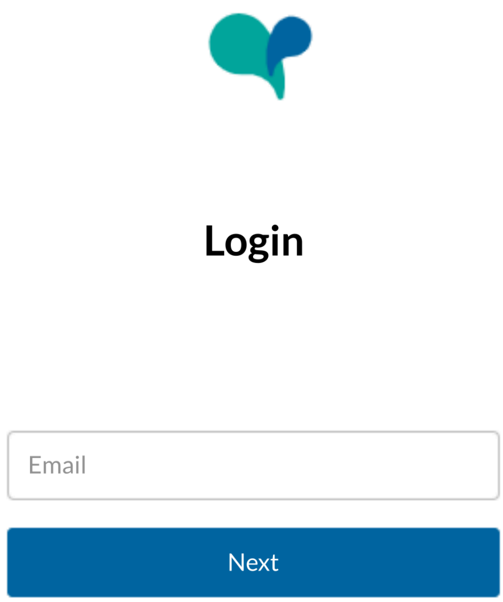
Step by Step

1) Open a web browser and enter the address (URL) of the Virtual Care Collaboration Service Administration app as provided by your organization.

The URL has the format: https://<Virtual Care Collaboration Service domain name>/admin

For example, if the system URL is https://vccs.example.com, the Admin app is available at https://vccs.example.com/admin.

2) Enter the email address associated with your account and click **Next**.



3) Enter the password associated with your account.

If you can't remember your password, click **Forgot my password**, enter the email address associated with your account, and then click **Request a reset link**. An email with a link to reset your password will be sent to you. For more information, see Resetting your password.

4) Click **Login**.

When logged in, your avatar appears in the bottom left corner of the screen.

2.2 Logging in with Single Sign On (SSO)

Single Sign On Authentication (SSO) allows you to log in to multiple applications using a single set of credentials. If SSO has been enabled for your organization, you can use your organizational account to log in to the Virtual Care Collaboration Service Administration app.

Step by Step

1) Open a web browser and enter the address (URL) of Virtual Care Collaboration Service Administration app as provided by your organization.
2) Enter the email address associated with your account and click **Next**.
3) You are redirected to the SSO provider's login page. On this page, enter your organizational credentials.

After successful authentication, you are redirected back to the Virtual Care Collaboration Service Administration app. Your avatar appears in the bottom left corner of the app.

2.3 Resetting your password

You can reset your password if you forget it.

Prerequisites

No SSO is enabled for your organization in Virtual Care Collaboration Service.

Step by Step

1) On the Virtual Care Collaboration Service login page, click **Forgot my password**.
2) Enter the email address associated with your account and click **Request a reset link**.
   An email with a link to reset your password will be sent to you.
3) Go to your email inbox and open the email with the subject **Reset password** from Virtual Care Collaboration Service.
4) Click the link in the email.
5) Enter your new password in the **New password** field.
6) Enter your new password again in the **Confirm password** field.
7) Click **Reset**.

NOTICE: The password must conform to the password policy defined for your Virtual Care Collaboration Service. If it does not, an error message appears showing the password policy requirements.

2.4 Logging out

To log out at any time:

Step by Step

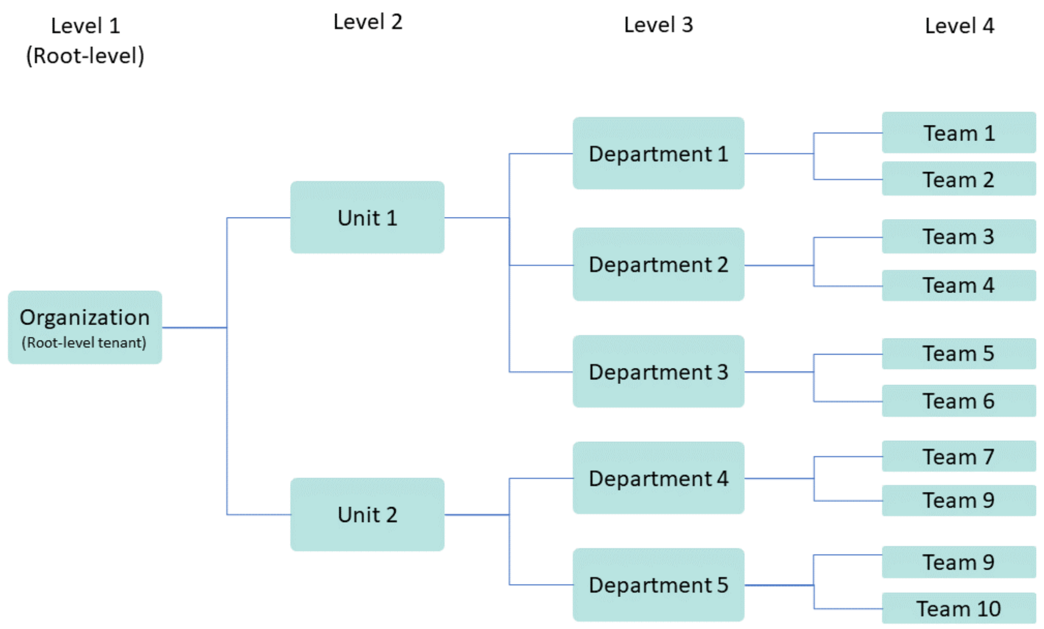
1) Click your avatar in the bottom left corner of the screen.

2) Select **Log out** from the drop-down list.

3 Multi-tenancy support

Virtual Care Collaboration Service supports multiple tenants. A tenant can either map to a complete organization (or a company) or a specific unit, department, or other entity within the organization. A tenant can have subordinate (child) tenants which in turn can have further child tenants under them, thus establishing a tenant hierarchy. The tenant hierarchy can have up to 4 levels starting with level 1.

The following figure depicts an example four-level tenant hierarchy.



A tenant without a parent is the root-level tenant or simply the root tenant. Only system administrators can create root tenants. System administrators can also create one or more administrators for the root tenants.

Root tenant administrators can manage (add, edit, remove) levels in the tenant hierarchy.

All tenant administrators can:

- create and manage subordinate tenants under their tenants at any level, up to level 4
- administer their own tenant and subordinate tenants (if any).

3.1 Root tenant management

As a system administrator, you can view, search for, create, edit or delete root tenants on Virtual Care Collaboration Service.

3.1.1 Creating a root tenant

You can create a root tenant on Virtual Care Collaboration Service.

Step by Step

1) From the left-hand navigation, select **Tenants**.
2) Click the + plus button under **Tenants**.
   The **Create new tenant** pop-up window appears.
3) Enter a name of the new root tenant.
4) Click **Create**.

The new root tenant is created and displayed under **Tenants**.

3.1.2 Viewing root tenants

You can view all root tenants created in Virtual Care Collaboration Service.

Step by Step

From the left-hand navigation, select **Tenants**.
A list of all root tenants is displayed under **Tenants**.

The following information is displayed for each root tenant:

- Tenant name
- Number of rooms
- Number of users

  The number of rooms includes the number of rooms in all subordinate tenants under this tenant. Similarly, the number of users includes the number of users in all subordinate tenants under this tenant.
- Number of subordinate tenants.

3.1.3 Searching for a root tenant

You can search for a root tenant by its name.

Step by Step

1) From the left-hand navigation, select **Tenants**.
   A list of all root tenants is displayed under **Tenants**.
2) Click **Search** and type the name of the root tenant you want to find.

   Search results appear dynamically as you type. They include matches that contain the search term, exactly as specified, but only when the search term is used at the beginning of a root tenant name.
3) To clear your search results or return to entire list of root tenants, delete the search term.

3.1.4 Renaming a root tenant

You can rename a root tenant at any time.

Step by Step

1) From the left-hand navigation, select **Tenants**.
   A list of all root tenants is displayed under **Tenants**.
2) Hover over the root tenant you want to rename and click .
   The **Edit tenant** pop-up window appears.
3) Enter the new tenant name and click **Save**.

3.1.5 Configuring license settings for a root tenant

You can configure a license for a root tenant at any time. You can specify the license type assigned to the root tenant and the maximum number of users allowed for a single license.

Prerequisites

You have activated the license for a root tenant.

Step by Step

1) From the left-hand navigation, select **Tenants**.
   A list of all root tenants is displayed under **Tenants**.
2) Hover over the root tenant you want to edit and click .
   The **Edit tenant** pop-up window appears.
3) Locate the **License** section.
4) Select one of the available types of license from the drop-down menu:
   - **Standard**
   - **Professional**
5) In the **Maximum number of users** field, enter the maximum number of users allowed for the selected license.

   The total number of available licenses for the selected license type is displayed.

   In case the license threshold is exceeded, the following alarm is triggered after 5 minutes: **License usage exceeded for 5 mins for tenant. Verify what license has been assigned to that tenant**. The license alarm is also raised at 4-hour and 7-day intervals.
6) Click **Save**.

3.1.6 Configuring chat settings for a root tenant

You can configure settings for chat sessions in a root tenant at any time. You can specify the file types that can be attached to chat messages, the maximum number of files allowed in a single chat message and the maximum file size (in MB) per file.

Chat settings you make will apply to the root tenant and any subordinate tenant(s).

Only system and root tenant administrators can configure chat settings.

Step by Step

1) From the left-hand navigation, select **Tenants**.
   A list of all root tenants is displayed under **Tenants**.
2) Hover over the root tenant you want to edit and click .
   The **Edit tenant** pop-up window appears.
3) Locate the **Chat** section.
4) In the **Accepted file types** field, enter one or more unique file type specifiers, separated by commas.

   These could be file extensions starting with a period ("."), like **.jpg,.png, .pdf**, or MIME type strings with no extensions, like **audio/*** (any audio file), **video/*** (any video file), **image/*** (any image file).
5) In the **Max files per message**, enter the maximum number of files allowed in a single chat message or select a number using the arrows.

   The max file size per message must be between 1 and 20.
6) In the **Maximum file size** field, enter the maximum file size (in MB) per file in a chat message or select a number using the arrows.

   The max file size must be between 1 and 100.
7) Click **Save**.

3.1.7 Configuring SAML 2.0 authentication for a root tenant

By default, users in a tenant are able to access Virtual Care Collaboration Service using the authentication method configured system-wide for all users in your organization. This can be either internal authentication using email and password or an SSO SAML authentication.

As a system administrator, you can configure and enable tenant-wide SSO SAML authentication for a root tenant. This will override the default authentication method configured system-wide and it will allow users in the root tenant and any subordinate tenant to access Virtual Care Collaboration Service using the corresponding authentication method. Users must have a valid user account in a SAML 2.0 Identify Provider (IdP) to log in successfully to Virtual Care Collaboration Service using SSO.

Root tenant administrators can always log in to the Administration app using their Virtual Care Collaboration Service credentials. This serves as a fallback option in case the SSO method fails. This means that if system- or tenant-wide SSO has been enabled for them, they can log in with either their Virtual Care Collaboration Service credentials or their organizational credentials.

3.1.7.1 Configuring a SAML 2.0 identity provider

Configuring a SAML 2.0 Identity Provider (IdP) is the first step in the process of configuring tenant-wide SSO SAML 2.0 authentication for a root tenant.

Step by Step

1) From the left-hand navigation, select **Tenants**.
2) Hover over the root tenant for which you want to configure a SAML 2.0 Identity Provider, and click .

   The **Edit tenant** pop-up window appears.
3) Locate the **Single Sign-on** section.
4) In the **IdP identifier** field, enter a name for the identity provider.
5) In the **IdP entry URL**, enter the remote login URL that you received from the identity provider.
6) Click **Configure** to start configuring an IdP certificate.
7) On the **Configure IdP certificate** pop-up window, enter the contents of the certificate that you received from the identity provider, then click **Save**.

   NOTICE: The IdP certificate settings are not saved until you click **Save** at the bottom of the **Edit tenant** pop-up.
8) By default, the **Tenant Single Sign-on** slider is set to OFF (gray), which means that SSO is not enabled on the root tenant. Once you have set all required settings for the identity provider (IdP Identifier, IdP Entry url, and certificate), you can enable tenant-wide SSO if you want, by switching the **Tenant Single Sign-on** slider to ON (blue).
9) Click **Save**.

3.1.7.2 Editing a SAML 2.0 identity provider

You can edit the settings of a SAML 2.0 identity provider configured for a root tenant.

Step by Step

1) From the left-hand navigation, select **Tenants**.
2) Hover over the root tenant for which you want to edit the SAML 2.0 Identity Provider, and click .

   The **Edit tenant** pop-up window appears.
3) Locate the **Single Sign-on** section.
4) If you want to replace the certificate configured for the identity provider with a new one, do the following:
   a) Click **Replace**.
   b) On the **Replace IdP certificate** pop-window, enter the contents of the certificate that you received from the identity provider, then click **Save**.

      NOTICE: IdP certificate changes are not saved until you click **Save** at the bottom of the **Edit tenant** pop-up.

5) If you want to delete the certificate configured for the identity provider, do the following:
   a) Click next to **Replace**.
   b) Click **OK** to confirm.
6) Edit the rest of the identity provider settings according to your needs.
7) Click **Save**.

NOTICE: Deleting any of the identity provider settings will automatically disable the tenant-wide SSO if it was previously enabled.

3.1.7.3 Enabling or Disabling tenant-wide Single Sign On

You can enable or disable tenant-wide SSO authentication for a root tenant.

When tenant-wide SSO authentication is disabled (default), users in the tenant and subordinate tenants are able to access Virtual Care Collaboration Service using the authentication method configured system-wide for all users in your organization.

When tenant-wide SSO authentication is enabled, users in the tenant and subordinate tenants are able to access Virtual Care Collaboration Service using the corresponding authentication method. The authentication method configured system-wide for all users in your organization is bypassed.

Root tenant administrators can always log in to the Administration app using their Virtual Care Collaboration Service credentials. This serves as a fallback option in case the SSO method fails.

You can enable or disable tenant-wide SSO for a root tenant when you configure a SAML 2.0 identity provider or afterward. For more information on how to enable SSO when you configure a SAML 2.0 identity provider, please see Configuring a SAML 2.0 identity provider on page 12.

Prerequisites

- You are an administrator of a root-level tenant.
- All required settings for a SAML 2.0 identity provider (IdP Identifier, IdP Entry url, and certificate) have been configured.

To enable or disable a tenant-wide SSO after a SAML 2.0 identity provider has been configured on the root tenant, do the following:

Step by Step

1) From the left-hand navigation, select **Tenants**.
2) Hover over the root tenant for which you want to configure a SAML 2.0 Identity Provider, and click .
   The **Edit tenant** pop-up window appears.
3) Locate the **Single Sign-on** section.

4) Switch the **Tenant Single Sign-on** slider to:
   - ON (blue) to enable tenant-wide SSO authentication

     or
   - OFF (gray) to disable tenant-wide SSO authentication.
5) Click **Save**.

3.1.8 Deleting a root tenant

You can delete a root tenant if the tenant has no subordinate tenants. Deleting a tenant will delete all resources (users or rooms) assigned to it.

Prerequisites

- The root tenant you want to delete has no subordinate tenants.

Step by Step

1) From the left-hand navigation, select **Tenants**.
   A list of all root tenants is displayed under **Tenants**.
2) Hover over the root tenant you want to delete and click .
3) Select **OK** to confirm.
4) If the root tenant has resources assigned to it, you will be promoted again to confirm the deletion. Select **OK** to confirm.

The root tenant is deleted from Virtual Care Collaboration Service. Any resources assigned to the root tenant are also deleted.

3.2 Root tenant administrator management

As a system administrator, you can view, create, edit or delete administrators for a root tenant.

3.2.1 Creating a root tenant administrator

You can create an administrator for a root tenant at any time.

Step by Step

1) From the left-hand navigation, select **Tenants**.
   A list of all root tenants is displayed under **Tenants**.
2) Select the root tenant for which you want to create an administrator.
   All administrators of the selected root tenant are displayed under **Administrators**.
3) Click at the top right.
   The **Create new user** pop-up window appears.

4) Enter the following required information for the new administrator:
   a) **First name**
   b) **Last name**
   c) **Email**
   d) **Password**
5) Select a **Language** from the drop-down menu.
6) Click **Create**.
   The new administrator is created and added to the list of administrators for the selected root tenant.

3.2.2 Viewing root tenant administrators

You can view all administrators of a root tenant in Virtual Care Collaboration Service.

Step by Step

1) From the left-hand navigation, select **Tenants**.
   A list of all root tenants is displayed under **Tenants**.
2) Select the root tenant for which you want to view its administrators.
   All administrators of the selected root tenant are displayed in a table under **Administrators**. They are sorted by their first name in ascending order.
   The table displays the following information for each administrator:

Field	Description
First name	The administrator's first name
Last name	The administrator's last name
Email	The administrator's email address
Language	The administrator's language in Virtual Care Collaboration Service

3.2.3 Editing a root tenant administrator

You can edit information about a root tenant administrator.

If you change an administrator's password, an email notification of the password change will be sent to the administrator. Provide the new password to the administrator so they can log in.

Step by Step

1) From the left-hand navigation, select **Tenants**.
   A list of all root tenants is displayed under **Tenants**.
2) Select the root tenant for which you want to edit an administrator.
   All administrators of the selected root tenant are displayed under **Administrators**.

3) Locate the administrator you want to edit and click ✎ to the right.
   The **Edit user** pop-up window appears.
4) Edit the administrator details and click **Save**.

3.2.4 Deleting a root tenant administrator

You can delete an administrator of a root tenant when they no longer require access to Virtual Care Collaboration Service or when they leave your organization.

NOTICE: You cannot delete the last administrator of a root tenant.

Step by Step

1) From the left-hand navigation, select **Tenants**.
   A list of all root tenants is displayed under **Tenants**.
2) Select the root tenant for which you want to delete an administrator.
   All administrators of the selected root tenant are displayed under **Administrators**.
3) Locate the administrator you want to delete and click 🗑 to the right.
4) Select **OK** to confirm.

4 Metrics

Metrics help you monitor performance and troubleshoot issues with Virtual Care Collaboration Service.

You can access metrics from the left-hand navigation menu of the Administration app by selecting **Metrics**.

The following metrics are available for display:

Metric	Description
Active Calls	Number of active calls
Practitioners Logged-in	Number of practitioners logged in to Virtual Care Collaboration Service
Patients in Waiting Room	Number of patients in waiting rooms
User license consumed[1]	Number of licenses consumed by logged-in practitioners Standard (blue line) Professional (red line)
User license consumed compared to configured limit	Number of licenses consumed compared to the total number of available licenses Standard (blue line) Professional (red line)

4.1 Viewing metrics

You can view the entire history for a metric in a specific date range.

Metrics are presented in the form of line graphs. Dots represent metric values recorded at different time points. Adjacent pairs of dots are connected by straight lines.

Step by Step

1) From the left-hand navigation, select **Metrics**.

A line graph depicts the selected metric' s value over time.

2) Hover over a dot on the line graph to view the exact value.

A tooltip is displayed that contains the date, time and metric value.

3) To change the metric shown in the graph:

a) Click the **Metric** drop-down list and select the metric of interest.

b) Click **Apply**.

The graph refreshes to show the values of the newly selected metric over time.

1 A license is shown in the metrics only when it is assigned, and the tenant has started using it.

4) To change the date range:

a) Enter a date in the **From** field or click the calendar icon on the right of the field and select a date from the date picker.

b) Enter a date in the **To** field or click the calendar icon on the right of the field and select a date from the date picker.

c) Click **Apply**.

The graph refreshes to show the metric's value in the new date range.

Next steps

If you want to export the line graph to a pdf file, first save the line graph as image or take a screenshot of it, then print the image file to a pdf printer to produce a pdf document.

5 API key management

Virtual Care Collaboration Service offers a REST API and several SDKs enabling other applications to integrate with it. Virtual Care Collaboration Service uses API keys to authenticate requests from other applications. The API keys are the equivalent of a username and password.

As a system administrator, you can create and manage API keys via the Administration app.

5.1 Creating an API key

You can create an API key at any time.

Step by Step

1) From the left-hand navigation, select ‹› **API keys**.
2) Click the + plus button at the top right.
   The **Create new API key** pop-up window opens.
3) Enter a **Name** for the application.
4) Enter the **TTL (time-to-live)** for the key, which defines the number of seconds the key is valid, or leave it empty for the default value.
   The default value is unlimited.
5) Click **Create**.
   The **API key created window** displays the newly created API key.
6) Click **Copy API key to clipboard** and store the key somewhere securely.

   NOTICE: Be sure to copy and paste the API key when it is displayed, as it will not be shown again.

7) Click ×.

The new API key is created and added to the list of keys with status **CREATED**.

5.2 Viewing API keys

You can view information about all the API keys that have been created in Virtual Care Collaboration Service.

Step by Step

1) From the left-hand navigation, select ‹› **API keys**.
   API keys are displayed in a table sorted by the application name in ascending order.
   The table displays the following information for each API key:

Field	Description
Application name	The name of the application

Field	Description
Expires on	The date and time until the API key is active
Status	The status of the API key
Issued	The email address of the admin who created the API key and the date time the key has been created
Revoked	The email address of the admin who revoked the API key and the date time the key has been revoked, if any

2) If you would like the list of API keys to be sorted differently:

- Click another column header to sort by the content of that column (by default in ascending order).
- Click the same column header again to change the sort order.

5.3 Searching for an API key

You can search for an API key using the application name, the API key status, expiration or issue date, or the email of the admin who created or revoked the API key.

Step by Step

1) From the left-hand navigation, select ‹› **API keys**.

2) Click 🔍 **Search** and type the information you want to find.

Search results appear dynamically as you type. They are sorted by the application name in ascending order.

3) To sort the search results differently:

- Click another column header to sort by the content of that column (by default in ascending order).
- Click the same column header again to change the sort order.

4) To clear your search results or return to the entire list of API keys, delete the search term.

5.4 Revoking an API key

Revoking an API key makes it unusable. When an API key is revoked, you need to update the application that uses that key to avoid breaking it.

Step by Step

1) From the left-hand navigation, select ‹› **API keys**.

A list with all the API keys is displayed.

2) Locate the key entry you want to revoke and click ⃠ to the right.

3) Click **OK** to confirm.
   The status of the API key changes to **REVOKED**.

> **NOTICE:** If there is more than one API key with the same application name, then all these keys will be revoked at once.

5.5 Deleting an API key

Deleting an API key removes it from the Virtual Care Collaboration Service system. This action is permanent and cannot be undone.

Prerequisites

The API key is in status REVOKED or more the one API key has been created for the same application.

Step by Step

1) From the left-hand navigation, select ‹› **API keys**.
   A list with all the API keys is displayed.
2) Locate the key entry you want to delete and click 🗑 to the right.
3) Click **OK** to confirm.

> **NOTICE:** If there is more than API key with the same application name, then all these keys will be deleted except for the latest valid key.
>
> If you select to delete the latest valid key for an application, then all API keys with the same application name will be deleted.

6 Settings

You can configure the settings of your Virtual Care Collaboration Service Administration app.

The **Settings** menu allows you to configure the Virtual Care Collaboration Service administration app or the whole Virtual Care Collaboration Service system.

You can open settings by clicking ⚙ on the left-hand navigation menu.

- Use the **General** tab to:
  - Change the language in which the program is displayed.
- Use the **Licences** tab to:
  - Activate a license for the system.

6.1 Changing the language settings

Virtual Care Collaboration Service Administration app currently supports the following languages:

- English
- German
- Spanish
- French
- Italian
- Dutch
- Catalan

You can change the language settings at any time.

Step by Step

1) From the left-hand navigation, select ⚙ **Settings**.
   The **General** tab is displayed by default.
2) Under the **Language** section, select your preferred language from the drop-down menu.
   The language will change automatically to the one selected.

6.2 Activating a license

You can activate a license for the system and then distribute the licenses to the root tenant(s) existing in the system.

Each license key is tied to a unique Locking id generated by the system. To obtain the license key, you need to provide the Locking id to the Virtual Care Collaboration Service support team.

Step by Step

1) From the left-hand navigation, select ⚙ **Settings**.

2) Select the **Licenses** tab.
3) In the **License key** field, enter the license key obtained from the Virtual Care Collaboration Service support team.
4) Click **Save**.

   The license has been activated for the selected root tenant.

   As the license expiration date approaches, you will receive an alarm with the following message: **System license is about to expire within the next 60 days. It's recommended to renew your license promptly to avoid service disruptions.** This alarm is also triggered 30 and 5 days before the license expires.

Next steps

You can configure the license settings. For more information, refer to Configuring license settings for a root tenant on page 10.

6.3 Reporting an issue

If you are experiencing an issue with Virtual Care Collaboration Service Administration app, you can report it from within the app. This will send logs from the app to the Virtual Care Collaboration Service support team so they can help troubleshoot.

Step by Step

1) Click your avatar in the bottom left corner of the screen.
2) Select **Report issue** from the drop-down menu.
3) On the pop-up dialogue, click **Submit**.