A MITEL
PRODUCT
GUIDE

Unify

OpenScape Endpoint Management V1

Administrator Documentation

06/2024

A31003-S2310-M100-02-76A9

Notices

Trademarks

Contents

1 Introduction

This document describes how to make use of the OpenScape Endpoint Management (OSEM) solution, as an administrator.

OpenScape Endpoint Management provides a solution for administrating clients, users and groups as well as use deployment templates for easier handling of clients. With OpenScape Endpoint Management, you can also easily upload software files to clients, maintain storage providers, run specific jobs on clients and configure certificates.

1.1 Target audience

This manual is intended both for administrators who install and configure the OpenScape Endpoint Management server and for users who carry out configuration and deployment tasks on the OpenScape Endpoint Management client.

Users must have prior experience of LAN administration and an in-depth knowledge of IP Device configuration.

1.2 Conventions Used

The following conventions are used in this manual:

Convention	Example
`courier`	Input and output Example: enter `LOCAL` as the file name
Italics	Variable Example: *Name* can be up to eight characters long
Bold	Indicates user interface elements Example: Click **OK** Select **Exit** from the **File menu**
Bold	Special emphasis Example: You are **not** permitted to delete this name
`<courier>`	Key combinations Example: `<CTRL>+<ALT>+<ESC>`
>	Menu sequence Example: **File > End**
NOTICE:	Additional information

Convention	Example
IMPORTANT:	Warning on critical aspects of a process

1.3 Constraint Notes

Some of the settings configurable via OpenScape Endpoint Management are available only for particular end devices or firmware versions. In such cases, an appropriate note is given.

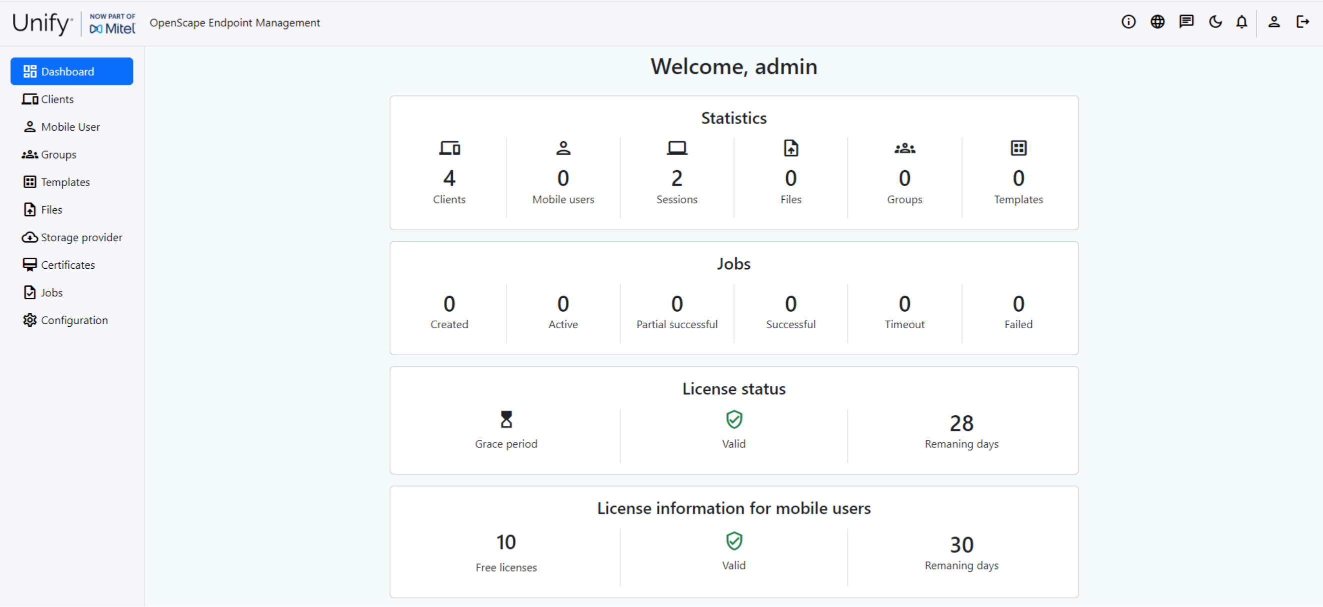
2 Getting started

This section describes how to access and log in to OpenScape Endpoint Management administration app and walks you through the main interface.

2.1 Main interface

The OpenScape Endpoint Management welcome screen allows you to view statistics of the registered clients and users, active sessions, uploaded files, number of groups, running or finished jobs, license information as well as various configuration options.

The welcome screen allows you to navigate to a specific tab by selecting the desired one from the left menu. You can access additional options, such as system information, in-app chat, language options, app theme customization, the notifications panel and your profile details from the top right of the app.



Welcome, admin

Statistics

4	0	2	0	0	0
Clients	Mobile users	Sessions	Files	Groups	Templates

Jobs

0	0	0	0	0	0
Created	Active	Partial successful	Successful	Timeout	Failed

License status

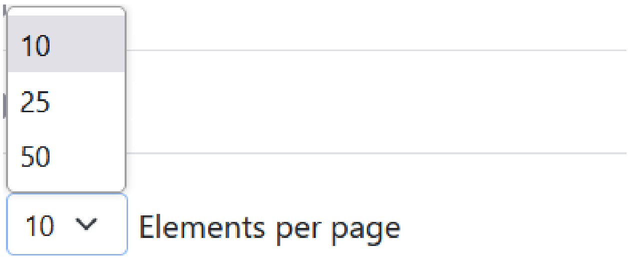
		28
Grace period	Valid	Remaining days

License information for mobile users

10		30
Free licenses	Valid	Remaning days

When you select a tab from the left menu, you are navigated to the corresponding area of the app and you can view the list of elements available on that tab. For example, when you navigate to the **Clients** tab, you can view the list of clients available on your OpenScape Endpoint Management administration app.

The elements of a tab are organized in pages. By default, you can view 10 elements per page. However, you can change the number of elements displayed on a page by clicking the down arrow (⌄) next to **Elements per page** and selecting one of the available options: **10** (default), **25**, **50**.



To navigate to a different page, you can use the page navigation buttons on the bottom left of the app:

- Click |< to navigate to the first page.
- Click < to navigate to the previous page.
- Click > to navigate to the next page.
- Click >| to navigate to the last page.

To return to the welcome screen at any time, click on the **Unify** logo at the top left of the app.

Optionally, you can click « to minimize the left menu and hide the tab names. If you choose this option, you will see only the tab icons.

2.2 Signing in and out

This chapter describes how to sign in and out of the OpenScape Endpoint Management administration app.

2.2.1 Signing in

Follow the steps below to sign in to OpenScape Endpoint Management administration app:

Step by Step

1) Open a web browser and enter the address (URL) of the OpenScape Endpoint Management administration app.

The app opens prompting you to sign in.

You can click 🌐 at the top right of the login screen to select the language in which you wish to display the app.

The following languages are available:

- English (default)
- German

2) Enter your username and password.

3) Alternatively, if you want to stay signed in to your account, enable the option **Keep me logged in**.

4) Click **Login**.

You are navigated to the welcome screen.

2.2.2 Signing out

To sign out at any time click ↦ at the top right of the app.

2.3 Viewing app information

You can view the information of the OSEM's current version by clicking ⓘ at the top right of the app.

The following information is displayed:

- The current version of the app.
- The features of the current release by accessing **What's new** section.
- The **EULA** (End User License Terms for OpenScape Endpoint Management). When accessing it, you are navigated to a new browser tab with details about license terms and conditions for end users
- The **TPSI** (Third Party Software Information for OpenScape Endpoint Management). When accessing it, you are navigated to a new browser tab with details about third party software information.
- You can also download **Open -Source** licenses. By clicking on the Open-Source license, the license will be automatically downloaded.
- You can also view the **API documentation**. When accessing it, you are navigated to a new browser tab with details about the fields used in the OSEM app that can be used on API integration.

2.4 Changing the language settings

OpenScape Endpoint Management currently supports the following languages: English (default) and German.

You can set the preferred language for your OpenScape Endpoint Management administration app in one of the following ways:

- Before signing in to the app, from the login screen.

  For more information, see Signing in on page 10.
- After signing in to the app, from the top right of the app.
  - Click 🌐 and select the language you want to use.

The language will change to the one you have selected.

2.5 Chatting with a virtual agent

OpenScape Endpoint Management administration app integrates a chat that enabled seamless communication with a virtual agent. You can use it to get hints about specific features of the app.

Once you sign in to the app, you can open the integrated chat by clicking 💬 on the top bar. The chat opens in a pop-up window and you can type a text message in the input field to start interacting with the virtual agent. The virtual agent provides an answer based on your query.

You can clear the chat window by clicking ≡ next to the input field. Previous queries and answers are no longed displayed.

To hide the chat, click again the 💬 icon.

2.6 Selecting a theme

You can select one of the predefined themes and change the appearance of the app. Changing the theme does not affect any custom configurations you have made in the app.

OpenScape Endpoint Management currently supports the following themes: light mode (default) and dark mode.

You can change the theme from the top bar of the app:

- Click ☾ to apply the dark theme.
- Click ☀ to apply the light theme.

2.7 Viewing notifications

OpenScape Endpoint Management enables administrators to view notifications about different app events (e.g. a failed login).

To view notifications, click 🔔 at the top right of the app.

A pop-up window opens and you can view a list of app notifications (if any).

When new notifications are available on your app, a red dot appears at the top right of the notification icon.

You can clear notifications that you don't want to see anymore in one of the following ways:

- Click ⊖ on the right side of a notification

  or
- Click **Clear all** on the top right of the **Notifications** pop-up window.

2.8 Managing your account

You can view or edit details of your account, access your account settings, manage sessions and register new users.

2.8.1 Editing account details

You can view and edit the details of your account at any time.

Step by Step

1) Click 👤 at the top right of the app.
2) Select **Account**

   You are directed to the **Account** area of the app and you can view your account's details.
3) Click the option to **Update user details** to set the language and edit the email address associated to your account. For more information regarding language settings, see Changing the language settings on page 11.

   A window opens allowing you to update your email address or language.
4) When you finished editing, enter your password then click **Update**.

You can also see the total number of failed logins and the date of the last failed authentication attempt in the **Failed logins** section.

2.8.2 Updating password

You can change the password of your account at any time.

By default, when an account for OpenScape Endpoint Management is created, the password is automatically set to **change_me**.

For security reasons, on the first login into the app, you are forced to change the default password.

Step by Step

1) Click 👤 at the top right of the app.
2) Select **Account**

   You are navigated to the **Account** area of the app and you can view your account's details.

3) Click on the option to **Update Password** to change your password.

A new window opens allowing you to update your password.

Provide the following information:

- Enter your current password in the **Old password** field.
- Enter the new password you want to set in the **New password** field.

> **NOTICE:** For security reasons, the password must meet the following requirements:
>
> – Length between 14 and 20 characters
> – At least one uppercase letter, one lowercase letter, one digit and one special character
> – No more than 3 identical characters in a row (e.g.: aaaa)
> – No more than 3 sequential characters in a row (e.g.: 1234)
> – Must not include the user name or its reverse (ex: user or resu)

- Re-enter the new password in the **Confirm new password** field.

If you want to see the passwords in clear text, switch the **Show passwords** slider to ON (green).

4) To apply the changes, click **Update**.

2.8.3 Managing sessions

You can view and manage your account's sessions.

The following details are available for each session:

- The browser and operating system used for the connection.
- The starting date and time of the session.
- The expiration date and time of the session.

Step by Step

1) Click 👤 at the top right of the app.
2) Select **Account**

You are directed to the **Account** area of the app and you can view your account's details.

3) Click the option **Manage open sessions** to view your active sessions.
A pop-up window opens and you can view all open sessions.

The currently active session is displayed in green.

Next steps

You can end sessions on your account in one of the following ways:

- Click ↦ to end any remote session, except for the currently active one.
- Click **Close all** to end all sessions.

2.8.4 Activating Multi Factor Authentication

You can activate multi factor authentication to enhance your account's security.

In order to configure the multi factor authentication, you must have installed an authenticator app (e.g. Microsoft Authenticator app) on your mobile phone.

Step by Step

1) Click 👤 at the top right of the app.

   You are navigated to the **Account** area of the app and you can view your account's details.
2) Click on the option **Activate Multi Factor Authentication** section.
   A pop-up window with a QR code opens.
3) Scan the QR code using your authenticator app. on your phone.
4) A 6-digits code is generated inside the authenticator app.
5) Provide the 6-digits authentication code in the **Authentication code** field.
6) Click on **Submit**.

   If you have problems scanning the QR code, do a manual setup by selecting **Click to copy data for setup** and follow the instructions.

NOTICE: Some Two-Factor authentication (2FA) apps (for example Microsoft Authenticator) do not support the

SHA - 256 algorithm. You can change to the SHA - 1 algorithm via **Configuration - > Security - >**

Time - based one - time password hash algorithm.
For more information, please refer to Configuring security settings on page 136.

2.8.5 Registering a new account

As an administrator, you can register a new account, provide contact information and assign specific roles.

Step by Step

1) Click 👤 at the top right of the app.
2) Select **Registered accounts**

   You are navigated to the **Accounts management** area.
3) Click **+ New** on the top right.

4) Enter the details of the new account:

- In the **User name** field, enter the user name you are assigning to the new account to log in to the app.
- In the **Password** field, enter the password you are assigning to the new account to log in to the app.
- In the **Confirm Password** field, enter the password again.
- From the **Language** drop-down list, select the language in which the app is displayed to the new account.
- In the **Email** field, enter the email address associated with the new account.
- From the **Pick role** list, select the role/s you want to assign to the new account.

5) Click **Create**.

The new account is created.

For security reasons, the new user is prompted to change their password on the first login. For more information, please refer to Updating password on page 13.

3 Concept and features

3.1 Supported clients

With OpenScape Endpoint Management, you can administer the following clients (IP devices):

- OpenScape Desk Phone CP710
- OpenScape Desk Phone CP700
- OpenScape Desk Phone CP700X
- OpenScape Desk Phone CP600
- OpenScape Desk Phone CP600E
- OpenScape Desk Phone CP410
- OpenScape Desk Phone CP400
- OpenScape Desk Phone CP210
- OpenScape Desk Phone CP205
- OpenScape Desk Phone CP200
- OpenScape Desk Phone CP110
- OpenScape Desk Phone CP100
- Desk Phone IP 55G
- Desk Phone IP 35G
- Desk Phone IP 35G Eco
- OpenStage 80
- OpenStage 60
- OpenStage 40
- OpenStage 20E
- OpenStage 20
- OpenStage 15

For each client, you can select one of the following software types:

- HFA
- SIP

3.2 Deployment scenarios

The following deployments are possible for OpenScape Endpoint Management:

- **Standalone deployment**

  Two options are available for this deployment type:

  - OpenScape Endpoint Management and the associated database are installed on the same Windows computer.
  - OpenScape Endpoint Management and the associated database are installed on the same Windows server.
- **Single node deployment**

  OpenScape Endpoint Management is installed on its own server while the database is installed on a separate server.

- **Multi-node deployment**

  In case of this deployment type, the OpenScape Endpoint Management servers may be used for load distribution.

  The OpenScape Endpoint Management nodes must be attainable over one IP address. Geographical separation is supported.

  This deployment model can also be used to achieve redundancy.
- **Integrated OSC 4000**

  In case of this deployment OpenScape Endpoint Management is part of the OpenScape 4000 installation.
- **SESAP Server**

  If OpenScape Endpoint Management is deployed on a SESAP server:

  – The mobility feature not supported.

    If the mobility feature is in use on the SESAP server, the installation of OpenScape Endpoint Management is not supported.

  – The number of subscribers supported is low (<1500).

    If the number of subscribers is greater than 1500 or if high load is expected on OpenScape Endpoint Management, a separate server should be used.

3.3 License information

You can view the license status and additional license information on the welcome screen.
The OpenScape Endpoint Management administration app supports CloudCLA and it must be licensed for full feature scope (support for mobile users).

After the first installation, the app automatically enters a grace period of 30 days.

To prevent losing access to OSEM, you must license the app.

When generating a License using the Central License Server you must set the **Governed by Cloud CLA** option to **YES**.

For more informatuon about the unique License Locking ID, please refer toConfiguring app licenses on page 133.
In the **License** section you can view the following details:

- whether the license is in a grace period
- the validity of the license
- the remaining days until expiration

In the **License information for mobile users** section you can see the amount of licenses allocated.

For software updates from one version to another, four different order positions using the same upgrade license are needed:

- Upgrade license from the old version to the new version
- Upgrade license from the old version to the new version within an existing SSP/SWA contract
- Upgrade license from the old version to the new version together with a new SWA contract

- Upgrade license from the old version to the new version together with a new SSP contract (also named as 'get current upgrade').
- Upgrading may be available for two older versions. Each version upgrade needs its own license.

4 Clients

As an administrator, you can view and manage the details of the available clients at any time from the **Clients** tab.

The **Clients** tab displays the following information:

- **E164**

  Represents the standardized phone number according to the ITU's international numbering plan with a maximum of 15 digits.

  Normally composed of three parts: CC, (Country Code), NDC (National Destination Code) and SN (Subscriber Number).

  Eg. 4989700732406.
- **Type**

  Supported workpoint device type.

  Eg. CP600, CP410, etc.
- **Device ID**

  Will be used as the unique device identifier.

  Eg. 00:1a:e8:75:fd:b1.
- **Software version**

  Represents the software version type used by the client.

  Eg. HFA V1 R7.4.0, SIP V1 R6.4.50.
- **Last contact**

  The last interaction with the device is presented under the form of date and hour.

  Eg. 20.09.2023 - 16:50:42.
- **Features**

  The features available for the client. When a feature icon is displayed with green, this is an indication that the feature is available for the client.

  – **Secure mode**:

    By default, the security mode is disabled 🔓. The security mode can be enabled by selecting **Enable secure mode** from the right configuration menu of the client ⋮ . Please see Enabling secure mode on page 28

  – **Mobility of the client**:

    Can have the following states:

    – enabled 👥

    – or disabled 👥.

    If the icon is active, in green color, the device is logged in. You can click on the active icon to display information regarding the device, namely the user and the login time.

  – **Access of the device**:

    The device can have direct access 🖧 or could require DCMP 🌐. If DCMP is globally deactivated, no devices can be reached via DCMP. For more information regarding DCMP configuration, please see *OpenScape*

Deployment Service, Administration & Installation Manual, chapter "DCMP tab".

- **Group of the device**:

  The group the device belongs to 👥
  For more information about the groups, please see Groups on page 115
- **Information** ⓘ

  Clicking on the information icon will display details regarding the part number of the workpoint (this number identifies the relevant hardware), specifies how many key modules are assigned to the IP client, the display type (shows the backlight type of display. Possible options: None, CCFL, LED) and the network speed.

You can also **refresh** the list of clients by clicking ↻ at the top right of the screen.

You can customize the view of the clients list by clicking ▥ at the top right of the **Clients** tab.

The following actions are possible:

- Switch the sliders to **ON** (green) or **OFF** (black) to show or hide columns.
- Click ▼ or ▲ to change the order of the columns.

  When finished, click **Ok** to save your changes.

4.1 Registering a new client

You can easily register a new client (a virtual Plug&Play client) on the OpenScape Endpoint Management administration app.

Follow the steps below to create and configure a new client.

Step by Step

1) Navigate to **Clients** tab

2) Click on **+New**.

3) The **Create Plug&Play client** window is displayed.

4) Enter the information regarding the new client.

- Select the **Hardware type** from the drop-down list.
- In the **Device ID** field, enter the client's ID.
- In the **E164 field**, enter the client's E164 number.
- Select the **Secure Mode** from the drop-down list. For further information regarding Secure Mode please see Enabling secure mode on page 28.
- Select the **Template** from the drop-down list. For more information about the templates, please see chapter Templates on page 35.

5) Click **Register**.
A confirmation message is displayed.

4.2 Scanning for devices

You can easily scan for clients in your OpenScape Endpoint Management administration app, by specifying the IP address range and the port number you want to scan by.

Step by Step

1) Select **Clients** from the left menu.

2) Click on **+ Scan**,
The **Scan for devices** window is displayed.

3) Add the information regarding the new scan. To avoid heavy network load, the IP address range should be selected so that where possible only one workpoint is scanned. If the IP range specified contains other clients, malfunctions can sometimes occur at the devices.

- In the IP address field, enter the IP address you want to scan.
- From the drop-down list select the Subnet mask.

4) Click **+Scan**.
A confirmation message is displayed and the scan for clients is started.

NOTICE: In the **Active scans** field you can check the status of the current scans.

4.3 Filtering the clients list

If the clients list is long, you can filter it to quickly find the one you are looking for.

Step by Step

1) Navigate to **Clients** tab

2) Click **Filter** in the top right of the screen and enter one or more filter terms:

- You can use the first field to search for **E164, MAC address or software version**.
- Select the **Software type** from the drop-down list.
- Select the **Client** type from the drop-down list.
- Select the **Groups** from the drop-down list.

3) Click **Apply** to view the searched results.

4) To clear your search results and return to the entire user list, click on **Reset**.

4.4 Sorting the clients list

You can sort the clients list in an ascending or descending order.

Columns that can be sorted contain the sort indicator (▲ ▼) in the column header.

The active sort order is indicated by:

- A dark arrow pointing up (▲), when the column is sorted in an ascending order.
- A dark arrow pointing down (▼), when the column is sorted in a descending order.

You can change the sort order by clicking on the desired arrow.

4.5 Configuring client settings

You can configure a client at any time by clicking ⋮ on the right of the client.

The following configuration options are available:

1) Open WBM
2) Refresh data
3) Configure
4) Deploy files
5) Copying client settings
6) Generating a template
7) Reset
8) Enable secure mode
9) Disable secure mode
10) Delete

4.5.1 Opening a WBM connection

You can open a WBM connection for a client by following the steps:

Step by Step

1) Click ⋮ on the right of the client.
2) Click on **Open WBM**.

The WBM (Web-Based Management) opens for the specific workpoint in a new browser window with the respective IP address.

> **NOTICE:** The button is only active if the client has configured an IP address.

4.5.2 Refreshing client data settings

You can update the client settings using the database.

You can refresh the information associated with a specific client by clicking ⋮ on the right of the client, then selecting **Refresh**.

Select one of the following options:

- Click **Cancel** to close the notification.

  When you select this option, your client data settings will not be refreshed.

- Click **Confirm** to refresh your client data settings.

  Upon successfully refreshing data, the following message is displayed: **Operation completed successfully**.

4.5.3 Configuring client parameters

You can view and manage the configuration of your client by using the **Configurations for client** section.

Step by Step

1) Select **Clients** from the left menu
2) Configure a client in one of the following ways:
   - Click on the icon ⋮ and select **Configure**
   - Tick the check box next to a client, then click **Configuration** at the top right of the app.
3) Select **Configure**.

You are navigated to the **Configuration for client** area.

This is a central menu for displaying and administering clients parameters.

The **Configuration for client** section displays the following information:

- **Properties:** In the header you can view the **Properties** of the device.
- **Search function:** You can also use the **Search** area to find a specific configuration parameter of the client.
- You can click on the ⋮ on the top right corner to **Refresh data** or **Discard changes**.
- **Submit:** After you completed the setup of the client, you can submit the changes by clicking the **Submit** button.
- You can minimize the **Configuration for client** window by using the minimization icon (_) on the top right corner of the window.

Next steps

For further information regarding the configurations for client, please see Configurations for clients, users and templates on page 39.

4.5.4 Deploying client files

In this section you can deploy files of the clients.

Step by Step

1) Select **Clients** from the left menu
2) Deploy a file in one of the following ways::
   - Click on the icon ⋮ and select **Deploy files**.
   - Tick the check box next to a client, then press **Deploy files** at the top right of the app.

3) Select the **Deploy files** option.

   The list of existing files is displayed (if any).
   The file to be deployed must include the following information:

   - **Filename**: the name of the file. This usually contains the type of the client, software version and type (e.g. CP_400_HFA_V1_R7_4_0.img)
   - **Storage:** whether the file exists at the storage location
   - **Type:** if the type of file is a software, ringtone, screensaver, LDAP template, logo, dongle, music on hold, picture.
   - **Size**: the size of the file
   - **Supported clients**: the type of the supported clients (e.g. CP400, CP600, etc).
   - **Software version**: this contains the software type (HFA or SIP) and the software version (e.g. HFA V1 R7.4.0)

4) Click **Filter** in the top right of the screen and enter one or more filer options:

   - Enter a name or storage of the client.
   - From the **Software type** drop-down list, select the type of storage you want to filter by: SIP Software or HFA Software.
   - From the **File type** drop-down list, select the type of file you want to filter by: software, ringtone, screensaver, LDAP template, logo, dongle, music on hold, picture.

5) Click **Apply**.
6) Select the file you want to deploy by clicking on the check box on the left.
7) Click on **Deploy** to deploy the file.
   Select one of the available options:

   - **Schedule** - by default the schedule is set to **Now**. You can schedule the deployment of the file by checking the **Scheduled box**.
   - **Cancel** - by default, this option is selected. If you select **Cancel**, then the notification will close.
   - **Confirm** - you hover over the **Confirm**, the button will turn green, when clicking on the button the deployment of file operation is executed and is then confirmed by the message **Operation completed successfully**.

4.5.5 Copying client settings

In case of hardware changes or factory reset of a client, you can easily copy the configuration of a client.

Follow the steps below to copy the configuration of a client.

Step by Step

1) Navigate to the **Clients** tab
2) Click on the icon ⋮ and select **Copy client**.
   The **Copy client** window opens.

3) Enter client information.
   - Select the **Reason for copy** from the drop-down list. The following options are available:
     - **Hardware change** with the following options:
       - E164 number, which is grayed out and it cannot be edited
       - SW type (SIP, HFA or GW)
       - Hardware type
       - Secure Mode
     - **Factory reset** with the following options:
       - Device ID
       - Secure Mode

4) Click **Submit**.
   A confirmation message is displayed.

4.5.6 Generating a template

You can easily generate a template for a client from the client's list.

Step by Step

1) Navigate to the **Clients** tab

2) Click on the icon ⋮ and select **Generate template**.
   The **Generate template** window opens.

3) Enter the template's details:

- From the **Type** drop-down list select the desired type for your template.

  The following options are available:

  – Onboarding template
  – Default template
- In the **Name** field, enter a custom name for your template.
- In the **Ranking** field, enter the rank you want to assign to your template.

  By default, ranking 1 is used.
- From the **Clients** drop-down list, select the device/s you want to make the template applicable for.

  For more information about the types of clients supported by OpenScape Endpoint Management, see Supported clients on page 17.

  If no client is selected, then all clients from the list will be considered for the template.
- From the **Software** drop-down menu, select the software type/s you want to make the template applicable for.

  The following options are available:

  – SIP
  – HFA

  If no software type is selected, then all software types from the list will be considered for the template.
- From the **Software update** drop-down list, select whether you want to enable software updates for the selected template.

  The following options are available: **Disabled**, **Ignored**, **Always**, **Only newer versions**.

4) Click **Submit**.
A new template is created.

4.5.7 Resetting client configuration settings

You can reset a client's configuration to the default values.

Step by Step

1) Click ⋮ on the right of the client.

2) Select the **Reset** option.
Select one of the available options:

- Click **Reset configuration to factory default values**.
- Click **Keep certificates after factory reset**. This option is only available if the **Reset configuration to factory default values** option has been checked. When clicking on the button the reset operation is executed and after is confirmed by the message **Operation completed successfully**.
- Click **Cancel** to quit the action and close the pop-up message.
- Click **Confirm** to perform the reset action. Upon successful completion, the following message is displayed **Operation completed successfully**.

You can also **schedule** the reset. By default the schedule is set to **Now**.

4.5.8 Setting the Secure Mode of a Client

4.5.8.1 Enabling secure mode

You can configure the secure mode of a client on a client that has the secure mode status disabled.

Step by Step

1) Click ⋮ on the right of the desired client.
2) Click **Enable secure mode**.
3) Select one of the available options:
    - **No PIN** - the security mode is enabled without a PIN .
    - **Default PIN** - a PIN is created automatically to allow encrypted transfer of server credentials to the device. If this option is selected, then the system creates a new default PIN. The PIN is used by IP Devices with Insecure security status.
    - **Individual PIN** - an individual PIN must be entered at the device to decrypt the server credentials.

      In individual secure mode, TAN (Target’s Authentication Number) failure can occur.
4) Optionally, schedule the enabling of secure mode by selecting the desired date and time. For this, do the following actions in the pop-up window displayed:.
    - Schedule the secure mode of the client by checking the Scheduled box. By default, the **schedule reset** is set to **Now**.
    - Cancel the operation. If you select **Cancel**, then the pop-up message will close.
    - Click **Confirm** to confirm the operation. The confirmation message **Operation completed successfully** is displayed.
5) After the secure mode has been enabled, the icon of the secure mode will be active (green) and the information regarding the client's secure mode will be displayed on clicking on the icon.

4.5.8.2 Disabling secure mode

You can disable secure mode of a client that has secure mode enabled.

Step by Step

1) Click ⋮ on the right of the desired client.
2) Select **Disable secure mode**.

3) Optionally, schedule the disabling of secure mode by selecting the desired date and time. For this, do the following actions in the pop-up window displayed:.
   - Schedule the secure mode of the client by checking the Scheduled box. By default, the **schedule reset** is set to **Now**.
   - Cancel the operation. If you select **Cancel**, then the pop-up message will close.
   - Click **Confirm** to confirm the operation. Upon successful completion, the following message is displayed **Operation completed successfully**.
4) After the secure mode has been disabled, the icon of the secure mode will be inactive (gray).

4.5.9 Delete

You can detele a client at any time.

Step by Step

1) Click ⋮ on the right of the desired client.
2) Delete a client in one of the following ways:
   - Click on the icon ⋮ and select **Delete**
   - Tick the check box next to a client, then press **Delete** at the top right of the app.
3) A pop-up window will be displayed and you are presented with the following options:
   - Click on the **Confirm** button to delete the client. Upon successful completion, the following message is displayed **Operation completed successfully**.

     NOTICE: Once a client is deleted, it will no longer appears in the Clients list.

   - Click **Cancel**, to quit the action and close the pop-up window.

5 Mobile users

As an administrator, you can view the list of all available mobile users, add new mobile users and configure their account details from the tab.

You can refresh the list of mobile users at any time by clicking ⟳ at the top right of the screen.
You can also logout specific mobile users, filter the mobile users list or delete mobile users that are not needed anymore.

You can customize the view of the mobile users list by clicking ▥ at the top right of the **Mobile Users** tab.

The following actions are possible:

- Switch the sliders to **ON** (green) or **OFF** (black) to show or hide columns.
- Click ▾ or ▴ to change the order of the columns.

  When finished, click **OK** to save your changes.

The tab displays the following information:

- **E164**

  Represents the standardized phone number according to the ITU’s international numbering plan with a maximum of 15 digits.
- **Base device**

  Device selection of the programmed key.
- **Last login**

  The last user login is presented under the form of date and hour.

  Eg. 20.09.2023 - 16:50:42.
- **Last logout**

  The last user logout is presented under the form of date and hour.

  Eg. 20.09.2023 - 19:01:56.
- **Status**

  Indicates whether the user is logged in or logged off.
  You can view the login status of the mobile users. The following statuses are available:

  1) 👤, when the user is logged off.
  2) 👤, when the user is logged in.
- **Profile size**

  Represents the profile size used for the user.

5.1 Registering a new user

You can register a new user at any time.

Step by Step

1) Select 👤 **Mobile users** from the left menu.

2) Click on **+New**,
The **Register new user** window appears

3) Add the information regarding the new user:

- In the **E164** field, enter the user's number.
- In the **Password** field, enter the password associated with user's account.
- In the **Confirm password** field, enter again the password.

4) Click **Register**.

5) If the E164 number you have entered for the new user is already associated with another user's account, the registration will fail and the following message will be displayed: **E164 user already exists.**
A confirmation message is displayed and the new user is added to the users list.

5.2 Filtering the users list

If the users list is too long, you can filter it to quickly find the one you are looking for.

Step by Step

1) Select **Mobile users** from the left menu.
A list of existing users is displayed (if any).

2) Click **Filter**, in the top right of the screen and enter one or more filter terms. You have the option to search based on the E164 number, the status of the user or both. The E164 number can be partially or fully introduced.

- Enter an E164 number in the input field
- From the Status drop-down list, select the user status you want to filter by.

3) Click **Apply**.
The users that match the filtering you have applied are displayed (if any).

4) To clear your search results and return to the users list, click on **Reset**.

5.3 Sorting the users list

You can sort the users list in an ascending or descending order.

Columns that can be sorted contain the sort indicator (▲ ▼) in the column header.

The active sort order is indicated by:

- A dark arrow pointing up (▲), when the column is sorted in an ascending order.
- A dark arrow pointing down (▼), when the column is sorted in a descending order.

You can change the sort order by clicking on the desired arrow.

5.4 Configuring a user account

You can easily configure a user's account.

Step by Step

1) Select **Mobile users** from the left menu
2) There are 2 ways to configure a user:
   - Click on the icon ⋮ and select **Configure**
   - Tick the check box next to a client, then press **Configuration** at the top right of the screen.

In the Users configuration tab you can manage the following settings:

1) Logging in or Logging out a user on page 32
2) Configurations for clients, users and templates on page 39
3) Deleting a user on page 33

5.4.1 Logging in or Logging out a user

You can easily login or logout users in your OpenScape Endpoint Management administration app.

Based on user's connection status, follow the steps:

Step by Step

1) Select **Mobile User** from the left menu.

   If the users list is too long, you can filter it to quickly find the one you are looking for.
2) Scroll through the list of users to locate the desired user.
3) Click ⋮ at the right of the user, then select one of the following:
   - **Logout user** - if the user is logged in. You can logout a user in one of the following ways:
   - Switch the Scheduled slider to **ON** (green) to select the date and time when you want to logout the user.
   - Switch the Scheduled slider to **OFF** (gray) to logout the user immediately.
   - Press **Confirm**.

   - **Login user** - if the user is logged out. If you select this option, the Login user screen appears and you can select the user/s you want to login. You can login a user in one of the following ways:
   - Switch the Scheduled slider to **ON** (green) to select the date and time when you want to login the user.
   - Switch the Scheduled slider to **OFF** (gray) to login the user immediately.
   - Press **Confirm**.

5.4.2 Configuring user parameters

You can view and manage the configuration of the users by using the **Configuration for user** tab.

Step by Step

1) Select **Mobile users** from the left menu
2) There are 2 ways to configure a user:
   - Click on the icon ⋮ and select **Configure**
   - Tick the check box next to a user, then press **Configuration** at the top right of the screen.

You are navigated to the **Configuration for user** area.

The **Configuration for user** section displays the following information:

Properties: In the header you can view the **Properties** of the user highlighted in green color.

Search function: You can also use the **Search** area to find a specific configuration parameter of the user.

You can click on the ⋮ on the top right corner to **Refresh data** or **Discard changes**.

Submit: After you completed the setup of the client, you can Submit the changes by clicking the **Submit** button.

You can minimize the **Configuration for user** window by using the minimization icon _on the top right corner of the window.

For further information regarding the configurations for users, please see Configurations for clients, users and templates on page 39.

5.4.3 Deleting a user

You can easily delete a user that is not needed anymore.

Step by Step

1) Select **Mobile users** from the left menu.
   A list of existing users is displayed (if any).
2) Scroll through the list of users to locate the users that you want to delete.

> **NOTICE:** If the list is too long, you can filter it to quickly find the user/s you are looking for.
>
> For more information, see Filtering the users list on page 31.

3) Tick the check box next to one or more users, then click **Delete** at the top right of the screen.

   Alternatively, you can delete one user at a time by clicking ⋮ at the right of the user, then selecting **Delete** from the drop-down menu.

4) Click **Confirm** to proceed with the deletion.

Deleted users are no longer available in the users list.

Next steps

If you want to make available again a deleted user, you must add it again. For more information, see Registering a new account on page 15.

6 Templates

You can easily view or edit existing templates, create new ones, configure template settings or delete templates that are not needed anymore from the **Templates** tab.

You can refresh the list of templates at any time by clicking ↻ at the top right of the screen.

You can customize the view of the templates list by clicking ▥ at the top right of the **Templates** tab.

The following actions are possible:

- Switch the sliders to **ON** (green) or **OFF** (black) to show or hide columns.
- Click ▾ or ▴ to change the order of the columns.

  When finished, click **Ok** to save you changes.

The **Templates** tab displays the following information about templates:

- **Name** - the name of the template.
- **Type** - the template type.
- **Ranking** - the ranking of the template.
- **Supported clients** - the clients that the template is available for.
- **Supported software** - the software type that the template is available for.
- **Software update** - whether software updates are enabled for the template.
- **Content** - the content of the template.

The following template types are available:

- **Default**
- **Onboarding**

6.1 Creating a template

You can easily create a new template to transfer a list of pre-defined attributes to clients faster.

Step by Step

1) Select ⊞ **Templates** from the left menu.
A list of existing templates is displayed (if any).

2) Click **+ New** in the top right corner of the screen.
The **Add Template** window appears.

3) Enter the details of the new template:

- From the **Type** drop-down list select the desired type for your template.

  The following options are available:

  – Onboarding template
  – Default template
- In the **Name** field, enter a custom name for your template.
- In the **Ranking** field, enter the rank you want to assign to your template.

  By default, ranking 1 is used.
- From the **Clients** drop-down list, select the device/s you want to make the template applicable for.

  For more information about the types of clients supported by OpenScape Endpoint Management, see Supported clients on page 17.

  If no client is selected, then all clients from the list will be considered for the template.
- From the **Software** drop-down menu, select the software type/s you want to make the template applicable for.

  The following options are available:

  – SIP
  – HFA

  If no software type is selected, then all software types from the list will be considered for the template.
- From the **Software update** drop-down list, select whether you want to enable software updates for the selected template.

  The following options are available: **Disabled**, **Ignored**, **Always**, **Only newer versions**.

4) Click **Submit**.
A new template is created.

5) Click **X** at the top of the **Add Template** window to return to **Templates**.

NOTICE: When you create a template, you only define template's general information. By default, no configuration settings are defined upon template's creation. After a template is created, you need to configure it to be able to use it for transferring information to client.

6.2 Viewing the content of a template

You can view the content of a template that has been configured previously.

Locate the template you want to edit and click ⋮ to the right, then select one of the following options:

- ✎: to edit the template. For more information regarding editing a template, please see section Creating a template on page 35
- ⚙: to assign configuration of a template.

- 🗎: to assign files to be included in a template.
- Based on template's configuration, an secure mode option can be:
  - Enabled (green), if the template has been configured for the specific option.
  - Disabled (gray), if the template has not been configured for a specific option.

6.3 Editing a template

You can edit the following information of an existing template:

- General information, that has been defined at template's creation.
- The configuration settings of the template.

Step by Step

1) Select ▦ **Templates** from the left menu.
A list of existing templates is displayed.

2) Locate the template you want to edit and click ⋮ to the right, then select one of the following options:

- Click **Edit** to edit template's general information.

  When selecting this option, the **Edit** window opens allowing you to change the template's settings you have defined upon the template creation.
- Click **Assign Configuration** to edit the configuration of a template.

  When selecting this option, a new window opens allowing you to edit template's configuration. For more information about a template's configuration, see chapter Configurations for clients, users and templates on page 39.
- Click **Assign Files** to assign a file to a template.

  When selecting this option, a new window opens allowing you to assign a file to a template. For more information about a template's file, see chapter Uploading a file on page 119.

3) Adjust template's details according to your needs, then click **Submit**.

6.4 Deleting one or more templates

You can easily delete one or more templates that are not needed anymore.

Step by Step

1) Select **Templates** from the left menu.
A list of existing templates is displayed.

2) Scroll through the list of templates to locate one or more templates that you want to delete.

If you want to select multiple templates at once, click the down arrow next to **Name** and select the desired option from the drop-down list:

- **All** - to mark all existing templates for deletion.
- **Current page** - to mark for deletion only the templates displayed on the current page.

NOTICE:

To undo the selection, click **None** in the drop-down list.

3) Tick the check box next to one or more templates, then click **Delete** at the top right of the screen.

Alternatively, you can delete a template at a time by clicking ⋮ at the right of the template, then selecting **Delete** from the drop-down menu.

4) Click **Confirm** to proceed with the deletion.

Deleted templates are no longer available in the list of templates.

Next steps

If you want to make available again a template you have deleted previously, you must create it again. For more information, see Creating a template on page 35.

7 Configurations for clients, users and templates

You can view and manage the configuration of your clients, users or templates via the respective **Configuration** menu.

Step by Step

1) Select **Clients**, **Mobile users** or **Templates** from the left menu.
2) Scroll through the list of clients, users or templates to locate the one you want to configure, then click ⋮ on the right and select **Configure**.

> **NOTICE:** You can filter the list of clients or users to quickly find the one you are looking for.
>
> For more information, see Filtering the clients list on page 22 or Filtering the users list on page 31.

3) Alternatively, for users and clients you can open the configuration area by ticking the check box next to the desired user/client and then pressing **Configuration** at the top right of the screen.

You are navigated to the configuration area of the client, user of template you have selected. Here you can view and administer configuration settings specific to the element you have selected.

The configuration area for clients, users and templates includes:

- The properties of the device, client or template in the header of the configuration area.
- A search box that allows you to quickly find specific configuration options.
- Two additional options available when clicking ⋮ at the top right of the configuration area: **Refresh data** and **Discard changes**.
- The **Submit** button, which allows you to save the configuration changes.

> **NOTICE:** The configuration steps for clients, users and templates are similar. However, several options are different or not available at all when accessing them from the **Clients**, **Mobile users** or **Templates** tabs. In such cases, appropriate information is provided in the following chapters.

7.1 General

This chapter provides instructions for the configuration options available in the **General** menu.

7.1.1 General information

The **General information** section is only available for clients.

To navigate to this area, expand the **General** menu, then select **General information**.

This section is **read-only** and it displays the following information:

- **Device type** - the type of the client.
- **Gigabit Ethernet enabled** - this option indicates whether the device has a gigabit LAN interface.

  This can be set to: **True** (default) or **False**.
- **Software type** - the type of software in use.
- **Software version** - the software version in use.
- **Contact-me URI** - this field is for display purposes and contains the complete URL used by the client to set up a connection to the OpenScape Endpoint Management.
- **MAC address** - the media access control address (MAC address) of the client.
- **Part number** - the part number of the workpoint that identifies the relevant hardware.
- **Backlight type** - the backlight type of display.
- **Key modules** - the number of Self Labeling Keys Modules connected.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.1.2 Connection information

You can view the **Connection information** configuration.

To navigate to this area, expand the **General** menu, then select **Connection information**.

Connection information

- **Connection address**
- **Client Contact-me URI**
- **Connection Default Port**
- **Connection Secure Port**
- **Cloud Connection PIN**
- **Cloud Connection Code**

This configuration is view-only.

7.1.3 Bluetooth

You can edit and manage the **Bluetooth** configuration for a client.

To navigate to this area, expand the **General** menu, then select **Bluetooth**.

If you have selected to configure the bluetooth settings of a **Client**, the following settings are available:

- **Bluetooth allowed**

  This can be set to **True** or **False** (default).
- **Bluetooth Beacon Mode**

  This can be set to **Disabled**, **Eddystone** or **iBeacon**.
- **iBeacon UUID**

- **iBeacon Major** - by default set to "0"
- **iBeacon Minor** - by default set to "0"
- **Eddystone Beacon Intervalle** - by default set to "1000"

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.1.4 Date & Time

The **Date & Time** configuration is available for users, clients, and templates.

To navigate to this area, expand the **General** menu, then select **Date & Time**.

Date & Time configuration for a user

If you have selected to configure the date and time settings of a **user**, the following settings are available:

- **Date format** - the format for date entry.

  The following date formats are available:

  - **dd mm yyyy** (example: 02 10 2023)
  - **yyyy mm dd** (example: 2023 10 02)
  - **mm dd yyyy** (example: 10 02 2023)
  - **dd/mm/yy** (example: 02/10/23)
- **Time format** - the format for the time entry.

  The following time formats are available:

  - 24 Hour
  - 12 Hour

Date & Time configuration for a client

If you have selected to configure the date and time settings of a **client**, the following settings are available:

- **SNTP server address**

  Abbreviation for "Simple Network Time Protocol". The protocol is used between time servers and telephones in a network in order to synchronize the time on the telephones.

  The date and time information comes from the IP address of the SNTP server.
- **SNTP backup server address**

  The date and time information comes from the backup IP address of the SNTP server.
- **SNTP timezone offset (minutes)**

  Time offset from UTC (Coordinated Universal Time) in minutes.

  The default value is 60 (phone residing in Munich)

- **Daylight saving enabled**

  You can activate the Daylight Saving function.

  This can be set to: **True** (default) or **False**.

  > **NOTICE:** If Automatic Daylight Saving Time changeover is set to **False** or no SNTP server is in use, you must manually switch between daylight saving and winter time. You must therefore change the status of the Daylight Saving twice a year. Pay particular attention to this when using this parameter in template data.

- **Daylight saving (minutes)** - the difference in minutes to normal or winter time.

  Default value is 60.
- **Automatic daylight saving enabled**

  This can be set to: **True** (default) or **False**.

  > **NOTICE:** If activated, the daylight saving time is toggled automatically according to the rule of the selected daylight saving zone.

- **Daylight saving zone**

  This can be set to one of the following options:

  – Not set
  – Australia 2007 (ACT, South Australia, Tasmania, Victoria)
  – Australien 2007 (New South Wales)
  – Australien (Western Australia)
  – Australien 2008+ (ACT, New South Wales, South Australia, Tasmania, Victoria)
  – Brasilia
  – Canada
  – Canada (Newfoundland)
  – Europe (Portugal, United Kingdom)
  – Europe (REST)
  – Europe (Finland)
  – Mexico
  – New Zealand
  – New Zealand (Chatham)
  – Chile (Santiago)
  – Gaza Strip
  – Greenland (Godthab)
  – Iran (Tehran)
  – Israel (Jerusalem)

Date & Time configuration for a template

If you have selected to configure the date and time settings of a **template**, the following settings are available:

- **SNTP server address**

  Abbreviation for "Simple Network Time Protocol". The protocol is used between time servers and telephones in a network in order to synchronize the time on the telephones.

  The date and time information comes from the IP address of the SNTP server.
- **SNTP backup server address**

  The date and time information comes from the backup IP address of the SNTP server.
- **SNTP timezone offset (minutes)**

  Time offset from UTC (Coordinated Universal Time) in minutes.

  The default value is 60 (phone residing in Munich).
- **Time source**
- **Date format**
- **Time format**
- **Daylight saving enabled**
- **Daylight saving (minutes)**
- **Automatic daylight saving enabled**
- **Daylight saving zone**
- **SNTP secret**

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.1.5 Mobility

The **Mobility** configuration is available for users, clients, and templates.

To navigate to this area, expand the **General** menu, then select **Mobility**.

Mobility configuration for a user

If you have selected to configure the mobility settings of a **Mobile user**, the following setting is available:

- **Hide mobility icon**

  This can be set to **True** or **False** (default).

Mobility configuration for a client

If you have selected to configure the mobility settings of a **client**, the following settings are available:

- **Mobility enabled**

  This can be set to **True** or **False** (default).

  If is set to **True**, the device is available for Mobile User log on.
- **Mobility logon attempts**

  This can be set to: **1**, **2**, **5**, **10**, or **Unlimited**.
- **Cancel mobility password**

  Enter the password to disable the mobility function on the workpoint.

- **Mobility mode**

  This can be set to **Basic** or **Data privacy**.
- **Mobility state**

  This field is read-only and the default value is 0.

Mobility configuration for a template

If you have selected to configure the mobility settings of a **template**, the following settings are available:

- **Mobility enabled**

  This can be set to **True** or **False**.

  If is set to **True**, the device is available for Mobile User log on.
- **International mobility ID**

  This can be set to **True** or **False**.

  If is set to **True**, the device automatically adds the local country code to the extension, in addition to the trunk number and local area code when a mobile user logs on.
- **Mobile password on logoff**

  This can be set to **True** or **False**.

  If set to **True**, the password need to be provided on mobile logoff.
- **Hide mobility icon**

  This can be set to **True** or **False**.
- **Mobility logon attempts**

  This can be set to: **1**, **2**, **5**, **10**, or **Unlimited**.
- **Cancel mobility password**

  Enter the password to disable the mobility function on the workpoint.
- **Mobility mode**

  This can be set to **Basic** or **Data privacy**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.1.6 Files

You can edit and manage the **Files** configuration for a client.

To navigate to this area, expand the **General** menu, then select **Files**.

In the **Files** section you will see the number of installed files.

To edit a file, click on the icon 🗑

After configuring all necessary options, click **Submit** in the top right of the configuration window.

A pop-up window will be displayed to save the configuration of the client:

- Switch the Scheduled slider to **ON** (green) to select the date and time when you want to save the configuration

- Switch the Scheduled slider to **OFF** (gray) for the configuration to take place immediately.

Click **Confirm**.

7.2 Integrations

This chapter provides instructions for the configuration options available in the **Integrations** menu.

7.2.1 OpenScape UC

The **OpenScape UC** configuration is available for clients, users and templates.

To navigate to this area, expand the **Integrations** menu, then select **OpenScape UC**.

The same configuration settings need be applied for clients, users and templates, as described below:

- **OpenScape UC server address**

  Enter the IP address of the OpenScape UC application server.
- **OpenScape UC login username**

  Enter the username for logging into the OpenScape UC application.
- **OpenScape UC login password**

  Click the ✎ icon to enter a password for logging into the OpenScape UC application.

  A pop-up window opens prompting you to:

  – Enter the a password you want to set in the **New password** field.
  – Re-enter the new password in the **Confirm new password** field.

  Click **OK** to set the password.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.2.2 OpenScape Business UC

The **OpenScape Business UC** configuration is available for clients, users and templates.

To navigate to this area, expand the **Integrations** menu, then select **OpenScape UC**.

The same configuration settings need be applied for clients, users and templates, as described below:

- **OSBiz UC protocol**

  Enter the protocol used for OpenScape Business UC.
- **OSBiz UC server address**

  Enter the IP address of the OpenScape Business UC application server.

- **OSBiz UC server port**

  Enter the port used for communication with the OpenScape Business UC server.
- **OSBiz UC user config enabled**

  This can be set to: **True** or **False**.

  If set to **True**, the config option is enabled for OpenScape Business UC users.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.2.3 Microsoft Exchange

The **Microsoft Exchange** configuration is available for clients, users and templates.

To navigate to this area, expand the **Integrations** menu, then select **Microsoft Exchange**.

The same configuration settings need be applied for clients, users and templates, as described below:

- **Microsoft® Exchange server address**

  Enter the IP address or the host name of the Microsoft Exchange Server.
- **Microsoft® Exchange login username**

  Provide the Microsoft Exchange username credential.

  The username cannot contain more than 64 characters.
- **Microsoft® Exchange login password**

  Provide the Microsoft Exchange password credential.

  The password cannot contain more than 32 characters.
- **Microsoft® Exchange contact folder name**

  Provide the folder where the User Contact data resides.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.2.4 E/A Cockpit

The **E/A Cockpit** configuration is available for users and templates.

To navigate to this area, expand the **Integrations** menu, then select **E/A Cockpit**.

The same configuration settings need be applied for users and templates, as described below:

- **E/A Cockpit server address:**

  Enter the IP or FQDN address of the E/A Cockpit server.

  The address can be contain `https://` or not, or it ca be provided as: `IP address:port`.

  The default port for https is 8443.
- **E/A Cockpit allow server push:**

  This can be set to: **True** (default) or **False**.

  If set to **True**, push requests from the E/A Cockpit Application server are allowed.
- **E/A Cockpit mobility logoff action:**

  This setting handles the action taken by the CP phone during SIP Mobile logoff.

  This can be set to one of the following values:

  – **None** - mo action is taken.
  – **Unavailable**- an assistant will be set to OFF_DESK, an executive will be set to TO_ASSISTANT_XXX (xxx depends on a different executive related setting)
  – **To Voicemail** - available if a voicemail number is configured in the E/A cockpit profile.
  – **To Mobile**- available if a mobile number is configured in the E/A cockpit profile.
  – **To Number** - available if a to-number is configured.

> **NOTICE:** When a SIP mobile user which has E/A cockpit configured, logs off and has the mobility logoff action set to anything except **None**, the E/A cockpit application on the phone will set the state to **Unavailable**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.2.5 Standard CSTA

The **Standard CSTA** configuration is available for users and templates.

To navigate to this area, expand the **Integrations** menu, then select **Standard CSTA**.

The same configuration settings need be applied for users and templates, as described below:

- **CSTA server address**

  Enter the IP address or host name of the CSTA application server.
- **CSTA server port:**

  Enter the port used for establishing the connection to the CSTA server.

  The default port is **5060**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.3 Telephony

This chapter provides instructions for the configuration options available in the **Telephony** menu.

7.3.1 General

You can view and manage the telephony general settings of a client.

To navigate to this area, expand the **Telephony** menu, then select **General**.

In this section you have the following options:

- **Name update source** the following options are available:
  - No source (default)
  - LDAP only
  - Signalling only
  - LDAP and Signalling
- **Emergency Number**
- **Not used timeout**: set by default to 2 minutes

  After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.3.2 SIP Settings

The **SIP Settings** configuration is available for users, clients and templates.

> **NOTICE:** For clients, this option is available only if the client's software type is **SIP**.

To navigate to this area, expand the **Telephony** menu, then select **SIP Settings**.

SIP Settings configuration for a client or a template

If you have selected to configure the SIP Settings of a **client** or a **template**, the following setting is available:

- **E164 number** - unique number for client identification.
- **SIP name** - the client's name that is used as a synonym for the phone number during registration.

  By default, the SIP name is the same as the E164 number.
- **SIP credentials username** - the username of the SIP client.
- **SIP credentials password** -

  Click the ✎ icon to enter a password for logging into the SIP server.

  A pop-up window opens prompting you to:

  - Enter the a password you want to set in the **New password** field.
  - Re-enter the new password in the **Confirm new password** field.

  Click **OK** to set the password.

- **SIP credentials realm** - the SIP range in which the client is operated.

  SIP realm is used to identify the telephone at SIP server.
- **Transport protocol** - the protocol for SIP signaling.

  This can be set to: **UDP**, **TCP**, or **TLS**.
- **Connection type** - the connection type of the phone with the main SIP server.

  This can be set to:

  – **Persistent** - is always acting as connection client, and no listening port gets opened to allow incoming connection attempts.

  – **Listening** - opens a listening port on the configured local SIP protocol.
- **Keepalive method** - the keepalive method used between comms and the switch.

  This can be set to:

  – **Sequence** - is always acting as connection client, no listening port gets opened to allow incoming connection attempts.

  – **CRLF** - opens a listening port on the configured local SIP protocol.
- **Connectivity check interval** - the value of the connectivity check interval, in seconds.
- **Registration timer** - the time period for re-registration at the SIP server.

  Re-registration ensures that the SIP telephone remains logged on to the SIP server. It can also detect server connectivity problems.
- **Registration refresh minimum timer** - the time interval that triggers a SIP registration session to be refreshed before the maximum expiration time, provided by the SIP server.

  The value indicates the earliest point (before the session expiration), when the device sends a session refresh message to prevent the session from expiring.

  This can be set to a value in the range of 0 (default) to 3600 seconds.
- **Registration backoff timer** - the time in seconds allowed between re-registration attempts, after a registration failure.
- **Subscription timer** - the time interval that triggers a SIP subscription session to be refreshed before the maximum expiration time provided by the SIP server.

  The value indicates the earliest point (before the session expiration), when the device can consider sending a session refresh message prevent a session from expiring.

  The default value of the time interval is 3600.
- **Subscription failure retry timer** - the time in seconds allowed between retry attempts, after subscription failure.
- **Call transaction response timer** - the time in milliseconds that a device will wait for a requested SIP message before the server is considered unavailable.
- **Non call transaction response timer** - the time in milliseconds allowed for non-invite (nonCall) based transaction.

- **Ringing state termination timer** - the time in seconds to terminate an incoming call transaction in ringing state (including alerting and being busy).

  When this timer is set to non-zero value, the ringing state and phone alerting (ringing, visual alert) is stopped by phone after the set period. When set to 0, the timer is off.
- **Session timer enabled**

  This can be set to: **True** or **False**.
- **Session timer** - the timer used to monitor the duration of an SIP session.
- **Server type**

  This can be set to: **OpenScape Voice**, **Broadsoft**, **HiQ8000**, **Genesys**, **Google Voice**, **RingCentral**.
- **Server address** - the IP address of the server, on which the program is running (example: 172.29.179.73).
- **Server port** - the port used by the server-side program for receiving data from the client.
- **Registrar address** - the IP address or host name of the SIP registrar.
- **Registrar port** - the port number of the SIP registrar.
- **Gateway enabled**

  This can be set to: **True** or **False**.
- **Gateway address** - the IP address or host name of the gateway.
- **Gateway port** - the port number of the gateway.
- **Local phone port** - the local phone port number of the client.
- **TLS renegotiation**

  This can be set to one of the following options:

  - **Secure (RFC 5746)** - access is allowed to TLS Servers that don’t support secure TLS renegotiation (through RFC 5746).
  - **Insecure allowed** - access to servers without secure TLS Renegotiation.
- **Failover type** - determines the phone failover to the next SRV priority IP on 500/503 server responses so that users can continue to use their mobile phones on temporary issues. This functionality is available only to CP200 / CP400 / CP600 V1R2 devices and higher.

  This can be set to: **Timeout only** (default) or **Timeout and error**.
- **Event check-sync handling** - the enumeration value of "Event check-sync".

  This can be set to one of the following values:

  - **Disabled** - the phone will reject handling of check-sync events.
  - **Challenge** (default): If digest authentication parameters are set, the phone will challenge the server for authentication.
  - **No challenge** - the phone will never challenge the server for authentication.
- **Keep resolved DNS records** - when enabled, previously resolved DNS records are kept in case of any DNS issues.

  This can be set to: **True** or **False**.
- **Prefer From header for display name**

  This can be set to: **True** or **False**.
- **DNS-SRV fallback on re-registration**

  This can be set to: **True** or **False**.

- **Indicate 100rel support**

  This can be set to: **True** or **False**.
- **All supported codecs in SDP response**

  This can be set to: **True** or **False**.
- **Early 183 response**

  This can be set to: **True** or **False**.

SIP Settings configuration for a user

If you have selected to configure the SIP Settings of a **user**, the following setting is available:

- **E164 number** - unique number for client identification.
- **SIP name** - the client's name that is used as a synonym for the phone number during registration.

  By default, the SIP name is the same as the E164 number.
- **SIP credentials username** - the username of the SIP client.
- **SIP credentials password** -

  Click the ✎ icon to enter a password for logging into the SIP server.

  A pop-up window opens prompting you to:

  – Enter the a password you want to set in the **New password** field.
  – Re-enter the new password in the **Confirm new password** field.

  Click **OK** to set the password.
- **SIP credentials realm** - the SIP range in which the client is operated.

  SIP realm is used to identify the telephone at SIP server.
- **Transport protocol** - the protocol for SIP signaling.

  This can be set to: **UDP**, **TCP**, or **TLS**.
- **Connection type** - the connection type of the phone with the main SIP server.

  This can be set to:

  – **Persistent** - is always acting as connection client, and no listening port gets opened to allow incoming connection attempts.
  – **Listening** - opens a listening port on the configured local SIP protocol.
- **Keepalive method** - the keepalive method used between comms and the switch.

  This can be set to:

  – **Sequence** - is always acting as connection client, no listening port gets opened to allow incoming connection attempts.
  – **CRLF** - opens a listening port on the configured local SIP protocol.
- **Connectivity check interval** - the value of the connectivity check interval, in seconds.
- **Registration timer** - the time period for re-registration at the SIP server.

  Re-registration ensures that the SIP telephone remains logged on to the SIP server. It can also detect server connectivity problems.

- **Registration refresh minimum timer** - the time interval that triggers a SIP registration session to be refreshed before the maximum expiration time, provided by the SIP server.

  The value indicates the earliest point (before the session expiration), when the device sends a session refresh message to prevent the session from expiring.

  This can be set to a value in the range of 0 (default) to 3600 seconds.
- **Subscription timer** - the time interval that triggers a SIP subscription session to be refreshed before the maximum expiration time provided by the SIP server.

  The value indicates the earliest point (before the session expiration), when the device can consider sending a session refresh message prevent a session from expiring.

  The default value of the time interval is 3600.
- **Subscription failure retry timer** - the time in seconds allowed between retry attempts, after subscription failure.
- **Ringing state termination timer** - the time in seconds to terminate an incoming call transaction in ringing state (including alerting and being busy).

  When this timer is set to non-zero value, the ringing state and phone alerting (ringing, visual alert) is stopped by phone after the set period. When set to 0, the timer is off.
- **Session timer enabled**

  This can be set to: **True** or **False**.
- **Session timer** - the timer used to monitor the duration of an SIP session.
- **Server type**

  This can be set to: **OpenScape Voice**, **Broadsoft**, **HiQ8000**, **Genesys**, **Google Voice**, **RingCentral**.
- **Server address** - the IP address of the server, on which the program is running (example: 172.29.179.73).
- **Server port** - the port used by the server-side program for receiving data from the client.
- **Registrar address** - the IP address or host name of the SIP registrar.
- **Registrar port** - the port number of the SIP registrar.
- **Local phone port** - the local phone port number of the client.
- **TLS renegotiation**

  This can be set to one of the following options:

  - **Secure (RFC 5746)** - access is allowed to TLS Servers that don’t support secure TLS renegotiation (through RFC 5746).
  - **Insecure allowed** - access to servers without secure TLS Renegotiation.
- **Failover type** - determines the phone failover to the next SRV priority IP on 500/503 server responses so that users can continue to use their mobile phones on temporary issues. This functionality is available only to CP200 / CP400 / CP600 V1R2 devices and higher.

  This can be set to: **Timeout only** (default) or **Timeout and error**.

- **Event check-sync handling** - the enumeration value of "Event check-sync".

  This can be set to one of the following values:

  - **Disabled** - the phone will reject handling of check-sync events.
  - **Challenge** (default): If digest authentication parameters are set, the phone will challenge the server for authentication.
  - **No challenge** - the phone will never challenge the server for authentication.
- **Keep resolved DNS records** - when enabled, previously resolved DNS records are kept in case of any DNS issues.

  This can be set to: **True** or **False**.
- **Prefer From header for display name**

  This can be set to: **True** or **False**.
- **DNS-SRV fallback on re-registration**

  This can be set to: **True** or **False**.
- **Indicate 100rel support**

  This can be set to: **True** or **False**.
- **All supported codecs in SDP response**

  This can be set to: **True** or **False**.
- **Early 183 response**

  This can be set to: **True** or **False**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.3.3 SIP backup settings

The **SIP backup settings** configuration is available for clients and templates.

> **NOTICE:** For clients, this option is available only if the client's software type is **SIP**.

To navigate to this area, expand the **Telephony** menu, then select **SIP backup settings**.

The same configuration settings need be applied for clients and templates, as described below:

- **Backup server address** - the IP address or host name of the backup server.
- **Backup server port** - the port number of the backup server.
- **Gateway for backup server**

  This can be set to: **True** or **False**.
- **Backup server registration timer** - backup time period for re-registration at the SIP server.
- **Register at backup server**

  This can be set to: **True** or **False**.
- **Backup server transport type** - the backup protocol for SIP signaling.

  This can be set to: **UDP**, **TCP**, or **TLS**.

- **Backup server connection type** - the connection type of the phone with the backup SIP server.

  This can be set to one of the following values:

  – **Persistent** - is always acting as connection client, no listening port gets opened to allow incoming connection attempts.
  – **Listening** - opens a listening port on the configured local SIP protocol.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.3.4 HFA Settings

The **HFA Settings** configuration is available for users, clients and templates.

> **NOTICE:** For clients, this option is available only if the client's software type is **HFA**.

To navigate to this area, expand the **Telephony** menu, then select **HFA Settings**.

SIP Settings configuration for a client

If you have selected to configure the HFA Settings of a **client** or a **template**, the following settings are available:

- **E164 number** - unique number used client identification.
- **System type**

  By default, the system type is set to unknown.
- **Signalling transport**

  This can be set to: **TCP** or **TLS**.
- **Server address** - the IP address of the server, on which the program is running (example: 172.29.179.73).
- **Server port** - the port used by the server-side program for receiving data from the client.
- **TLS renegotiation**

  This can be set to one of the following values:

  – **Secure (RFC 5746)** - access is allowed to TLS Servers that don’t support secure TLS renegotiation (through RFC 5746).
  – **Insecure allowed** - access to servers without secure TLS Renegotiation.
- **Gateway ID** - the unique identifier of the gateway.
- **Subscriber number** - the number associated with the subscriber.
- **Subscriber password**

  Click the ✎ icon to enter a password for logging into the SIP server.

  A pop-up window opens prompting you to:

  – Enter the a password you want to set in the **New password** field.
  – Re-enter the new password in the **Confirm new password** field.

  Click **OK** to set the password.

- **System H.225 port** - the H.225 port used on the system.
- **System Cornet TLS port** - the Cornet TLS port used on the system.
- **System H.225 TLS port** - the H.225 TLS port used on the system.

SIP Settings configuration for a user

If you have selected to configure the HFA Settings of a **user**, the following settings are available:

- **E164 number** - unique number used client identification.
- **Server address** - the IP address of the server, on which the program is running (example: 172.29.179.73).
- **Server port** - the port used by the server-side program for receiving data from the client.
- **TLS renegotiation**

  This can be set to one of the following values:

  - **Secure (RFC 5746)** - access is allowed to TLS Servers that don’t support secure TLS renegotiation (through RFC 5746).
  - **Insecure allowed** - access to servers without secure TLS Renegotiation.

SIP Settings configuration for a template

If you have selected to configure the HFA Settings of a **template**, the following settings are available:

- **E164 number** - unique number used client identification.
- **Signalling transport**

  This can be set to: **TCP** or **TLS**.
- **Server address** - the IP address of the server, on which the program is running (example: 172.29.179.73).
- **Server port** - the port used by the server-side program for receiving data from the client.
- **TLS renegotiation**

  This can be set to one of the following values:

  - **Secure (RFC 5746)** - access is allowed to TLS Servers that don’t support secure TLS renegotiation (through RFC 5746).
  - **Insecure allowed** - access to servers without secure TLS Renegotiation.
- **Gateway ID** - the unique identifier of the gateway.
- **Subscriber number** - the number associated with the subscriber.
- **Subscriber password**

  Click the ✎ icon to enter a password for logging into the SIP server.

  A pop-up window opens prompting you to:

  - Enter the a password you want to set in the **New password** field.
  - Re-enter the new password in the **Confirm new password** field.

  Click **OK** to set the password.
- **System H.225 port** - the H.225 port used on the system.
- **System Cornet TLS port** - the Cornet TLS port used on the system.
- **System H.225 TLS port** - the H.225 TLS port used on the system.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.3.5 HFA standby settings

The **HFA standby settings** configuration is available for clients and templates.

> **NOTICE:** For clients, this option is available only if the client's software type is **HFA**.

To navigate to this area, expand the **Telephony** menu, then select **HFA standby settings**.

HFA standby settings configuration for a client

If you have selected to configure the HFA standby settings of a **client**, the following setting is available:

- **Standby system type** - the type and version of the communication platform on which the client is operated.

  This field is read-only.
- **Signalling transport standby** - the signaling protocol for HFA.

  This can be set to: **TCP** or **TLS**.
- **Backup server address** - the IP address of the backup server, on which the program is running (example: 172.29.179.73).
- **Backup server port** - the backup port used by the server-side program for receiving data from the client.
- **Standby gateway ID** - the standby ID of the PBX, gateway or gatekeeper used for operating the client.
- **Standby subscriber number** - the standby phone number of the subscriber at the PBX (example: 12345)
- **Standby subscriber password** - the password of the standby client at the PBX.

  Click the ✎ icon to enter a password for logging into the SIP server.

  A pop-up window opens prompting you to:

  - Enter the a password you want to set in the **New password** field.
  - Re-enter the new password in the **Confirm new password** field.

  Click **OK** to set the password.
- **Standby H.225 port** - the Standby H.225 port used for the client.
- **Standby Cornet TLS port** - the Cornet TLS port used by the HFA gateway for secure communication with the client.

  The Cornet TLS port can be in the range of 0 to 65535. The default port is 4061.
- **Standby H.225 TLS port** - the port used for secure signalling with H.255.

  The Standby H.225 TLS port can be in the range of 0 to 65535. The default port is 1300.

HFA standby settings configuration for a template

If you have selected to configure the HFA standby settings of a **template**, the following setting is available:

- **Signalling transport standby** - the signaling protocol for HFA.

  This can be set to: **TCP** or **TLS**.
- **Backup server address** - the IP address of the backup server, on which the program is running (example: 172.29.179.73).
- **Backup server port** - the backup port used by the server-side program for receiving data from the client.
- **Standby gateway ID** - the standby ID of the PBX, gateway or gatekeeper used for operating the client.
- **Standby subscriber number** - the standby phone number of the subscriber at the PBX (example: 12345)
- **Standby subscriber password** - the password of the standby client at the PBX.

  Click the ✎ icon to enter a password for logging into the SIP server.

  A pop-up window opens prompting you to:

  – Enter the a password you want to set in the **New password** field.
  – Re-enter the new password in the **Confirm new password** field.

  Click **OK** to set the password.
- **Standby H.225 port** - the Standby H.225 port used for the client.
- **Standby Cornet TLS port** - the Cornet TLS port used by the HFA gateway for secure communication with the client.

  The Cornet TLS port can be in the range of 0 to 65535. The default port is 4061.
- **Standby H.225 TLS port** - the port used for secure signalling with H.255.

  The Standby H.225 TLS port can be in the range of 0 to 65535. The default port is 1300.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.3.6 HFA Redudancy settings

The **HFA Redudancy settings** configuration is available for clients and templates.

> **NOTICE:** For clients, this option is available only if the client's software type is **HFA**.

To navigate to this area, expand the **Telephony** menu, then select **HFA Redudancy settings**.

The same configuration settings need be applied for clients and templates, as described below:

- **Small remote site redundancy enabled**

  This can be set to: **True** or **False**.
- **Automatic switchback** - the option to activate automatic switchback to the main system.

  This can be set to: **True** or **False**.

- **Retry count main** - this counter specifies the number of attempts allowed before switching back to the main system.

  The value of this counter can be in the range of **1** (default) to **255** seconds.
- **Retry count standby** - this counter specifies the number of attempts allowed before switching back to the standby system.

  The value of this counter can be in the range of **1** to **255** . The default value is 3.
- **Timeout main** - the timeout interval for switchover to the main system.

  The value of this interval can be in the range of **1** to **255** seconds. The default value is 30.
- **Timeout standby** - the timeout interval for switchover to the standby system.

  The value of this interval can be in the range of **1** to **255** seconds. The default value is 30.
- **TC test enabled**

  This can be set to: **True** or **False**.
- **TC test retry** - the number of positive attempts allowed when switching back to the main system.

  This value can be in the range or **1** to **255** . The default value is 3.
- **TC test expiry** - the time interval for a renewed attempt to switch back to the main system.

  The value of this interval can be in the range of **1** to **255** . The default value is 3.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.3.7 Canonical dial settings

The **Canonical dial settings** configuration is available for clients, templates and mobile users.

To navigate to this area, expand the **Telephony** menu, then select **Canonical dial settings**.

- **Local country code**

  Digit or short digit string for dialing a particular prefix, for example.
- **National prefix digit**

  Format: digits. Example: 49 for Germany.
- **Local National Code**

  Format: digits. Example: **89** for Munich.
- **Minimum Local Number Length**

  Format: digits.

  Example: 01081
- **Maximum Local Number Length**

  Format: digits.

  Example: 01081

- **Local Enterprise Node**

  Format: digits.
- **PSTN Access Code**

  Format: digits.
- **Operator Code**

  Format: digits.
- **Emergency Numbers**

  Format: digits.
- **Initial Extension Digits**

  Format: digits.
- **Expect Dial Number**

  This can be set to: **True** or **False**.
- **Dial Internal Numbers**

  This can be set to: **Local Enterprise Form**, **Always Add Node** or **Use External Numbers**.
- **Dial External Numbers**

  This can be set to: **Local Public Form**, **National Public Form** or **International Form**.
- **External Access Code**

  This can be set to: **Not required** or **For External Numbers**.
- **Dial International Numbers**

  This can be set to: **Use National Code** or **Leave as +**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.3.8 Canonical dial lookup

The **Canonical Dial lookup** configuration is available for clients, templates and mobile users.

To navigate to this area, expand the **Telephony** menu, then select **Canonical Dial lookup**.

- **Local code**

  Format: alphanumeric.
- **International code**

  Format: alphanumeric.

You can configure multiple international and local codes. The list will expand dynamically once a value is entered in one of the fields above.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.3.9 Keyset settings

The **Canonical Dial lookup** configuration is available for clients, templates and mobile users.

To navigate to this area, expand the **Telephony** menu, then select **Canonical Dial lookup**.

> **NOTICE:** Only available in SIP workpoints.

- **Rollover Ring:**

  Type of alerting to be used in the case that, during an active call, an incoming call arrives on a different line.

  Possible options:

  - **No Ringing**
  - **Alert Ringing**
  - **Standard Rgingin**
  - **Alert Beep**
- **Rollover Visual Alert**

  Configure the visual alert for any incoming call rollover.

  Possible options:

  - **no indication**
  - **visual alert**
- **LED on registration**

  This can be set to: **True** or **False**.
- **Originating Line Preference**:

  Defines the preferred line to be used for outbound calls.

  Possible options:

  - **Idle Line**
  - **Primary Line**
  - **Last Line**
  - **None**
- **Terminating Line Preference**

  Defines the preferred line to be used for incoming calls.

  Possible options:

  - **Ringing Line**
  - **Ringing Line (Primary Line Preference)**
  - **Incoming Call**
  - **Incoming Call (Primary Line Preference)**
  - **None**

- **Line Action Mode**

  Defines what should happen to a line (call) when a connection is established over another line.

  Possible options:

  – **Hold** The original call is put on hold.
  – **Release** The connection to the original call is cleared down (the call is ended).
- **Reservation Timer (seconds)**

  Time in seconds indicating how long a line reservation can be maintained.

  Default: **60** s.
- **Line Key Forwarding Shown**

  This can be set to: **True** or **False**.
- **DSS Show Caller ID when alerting**

  This can be set to: **True** or **False**.
- **Call Pickup Detect Timer (sec)**

  Specifies how long group pickup is signaled by the key.

  Default: 3 Seconds.
- **Deflect Alerting Call Enabled**

  If this field is set to **True**, alert tones can be forwarded by pressing a key.

  This can be set to: **True** or **False**.
- **Allow Pickup To Be Refused**

  If this field is set to **True**, you can reject group pickup by pressing a key.

  This can be set to: **True** or **False**.
- **DSS Key Forwarding Shown**

  If this field is set to **True** and station forwarding is active for this line, the LED of the line key blinks.

  This can be set to: **True** or **False**.
- **DSS monitored**

  If this field is set to **True** you allow a DSS key to monitor the non-Keyset phone associated with the DSS key.

  This can be set to: **True** or **False**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.3.10 Diaplan settings

The **Dialplan** configuration is available for clients, templates and mobile users.

To navigate to this area, expand the **Telephony** menu, then select **Dialplan**.

NOTICE: Only available in SIP workpoints.

- **Dialplan Enabled**

  If this field is set to **True**, the dialplan is activated.

  This can be set to: **True** or **False**.
- **Dialplan ID**

  Name of the dial plan.

  Value range: alphanumeric characters.
- **Dialplan Error**

  Specifies the dial plan entry that is faulty in the event of an error.
- **Dialplan entry**

  You can add an entry by clicking **+**

  A window will be displayed with the following settings:

  - **Digit String** - Digit string for executing this action.
  - **Action** - Action executed for this digit string.

    Possible options:

    - **Action for digits**
    - **Send digits**
- **Minimum length** - Minimum digit string length for digit string interpretation. Default: 1.
- **Maximum length** - Maximum digit string length for digit string interpretation. Default: 1.
- **Timeout** - Delay before the action is performed. Default: 0.
- **Terminating character**

  Character that ends the digit string entered.

  Possible options:

  - **Not configured**
  - **#**
  - *
- **Special indication**

  Possible options:

  - **Not configured**
  - **Emergency call**
  - **Bypass**
- **Comment**

  Field for general information.
- **Sent termination character**

  This field is read-only and it displays whether the terminating character is included in the digit string. Default: False.

After configuring all necessary options, click **Confirm** in the dialplan entry configuration window.

Click **Submit** in the top right of the configuration window for the configuration of the dialplan to take place.

7.4 Audio

This chapter provides instructions for the configuration options available in the **Audio** menu.

7.4.1 General

The **General** configuration is available for clients, users and templates.

To navigate to this area, expand the **Audio** menu, then select **General**.

General audio settings configuration for a user

If you have selected to configure the General audio settings of a **user**, the following setting is available:

- **RTP base port** - the base port number for RTP transport.
- **Media negotiation mode** - this option indicates the Media Candidate Negotiation Mode.

  This can be set to one of the following options:

  - Single IP
  - ANAT - Alternative Network Adress Type (ANAT) provides a mechanism of IPv4/IPv6 media negotiation on a media stream basis.
  - ICE
- **Media IP mode** - this option indicates the media IP mode.

  This can be set to one of the following options: **IPv4**, **IPv6**, **IPv4 / IPv6** or **IPv6 / IPv4**.
- **Allow HD icon on display**

  This can be set to: **True** or **False**.
- **Display DTMF events**

  This can be set to: **True** or **False**.
- **Play DTMF events**

  This can be set to: **True** or **False**.

General audio settings configuration for a client

If you have selected to configure the General audio settings of a **SIP client**, the following setting is available:

- **RTP base port** - the base port number for RTP transport.
- **Media negotiation mode** - this option indicates the Media Candidate Negotiation Mode.

  This can be set to one of the following options:

  - **Single IP**
  - **ANAT** - Alternative Network Adress Type (ANAT) provides a mechanism of IPv4/IPv6 media negotiation on a media stream basis.
  - **ICE**
- **Media IP mode** - this option indicates the media IP mode.

  This can be set to one of the following options: **IPv4**, **IPv6**, **IPv4 / IPv6** or **IPv6 / IPv4**.

- **Allow HD icon on display**

  This can be set to: **True** or **False**.
- **Silence suppression enabled**

  This can be set to: **True** or **False**.
- **Display DTMF events**

  This can be set to: **True** or **False**.
- **Play DTMF events**

  This can be set to: **True** or **False**.
- **Loudspeaker enabled**

  This can be set to: **True** or **False**.
- **Microphone disabled**

  This can be set to: **True** or **False**.

If you have selected to configure the General audio settings of a **HFA client**, the following setting is available:

- **RTP base port** - the base port number for RTP transport.
- **Silence suppression enabled**

  This can be set to: **True** or **False**.

General audio settings configuration for a template

If you have selected to configure the General audio settings of a **template**, you must set the same setting as for a **SIP client**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.4.2 Codec settings

The **Codec settings** configuration is available for clients, users and templates.

To navigate to this area, expand the **Audio** menu, then select **General**.

Codec settings configuration for a user or a template

If you have selected to configure the codec settings of a **user** or a **template**, the following setting is available:

- You can enable or disable the following codecs: **G711**, **G722**, **G729**, **OPUS**.

  To enable or disable a codec, you need to switch the codec slider to:

  - ON (green), if you want to enable the codec.
  - OFF (gray), if you want to disable the codec.

  You can also order the list of codecs using the arrows:

  - Click ⌄ to move the codec selected to an upper position.
  - Click ⌃ to move the codec selected to a lower position.
- **Codecs packet size** - the size allowed for codec packets.

  This can be set to one of the following values: **10ms**, **20ms**, **Automatic**, **30ms**, **60ms** or **40ms**.

Codec settings configuration for a client

If you have selected to configure the codec settings of a **client**, the following setting is available:

- **Codecs** - this indicates if codecs enabled or disabled for the selected client.

  This can be set to:

  – ON (green), if you want to enable codecs.
  – OFF (gray), if you want to disable codecs.
- **Codecs packet size** - the size allowed for codec packets.

  This can be set to one of the following values: **10ms**, **20ms**, **Automatic**, **30ms**, **60ms** or **40ms**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.4.3 SRTP settings

The **SRTP settings** configuration is available for clients, users and templates.

To navigate to this area, expand the **Audio** menu, then select **SRTP settings**.

SRTP settings configuration for a user or a template

If you have selected to configure the SRTP settings of a **user** or a **template**, the following settings are available:

- You can enable or disable the following **SRTP Encryption methods**: **AES-128 SHA1-32**, **AES-128 SHA1-80** or **AES-256 SHA1-80**.

  To enable or disable a SRTP Encryption method, you need to switch the corresponding slider to:

  – ON (green), if you want to enable the method.
  – OFF (gray), if you want to disable the method.

  You can also order the list of methods using the arrows:

  – Click ⌄ to move the method selected to an upper position.

  – Click ⌃ to move the method selected to a lower position.
- **Secure calls enabled**

  This can be set to: **True** or **False**.
- **Secure call alert**

  This can be set to: **True** or **False**.
- **SRTP key negotiation mode** - the SRTP type(s) for secure calls.

  This setting identifies the type of SRTP that is allowed to be offered or accepted via SDP.

  The following values as possible: **MIKEY**, **SDES** (default), **DTLS**, **DTLS-SDES**.

- **SDP negotiation mode** - the SDP negotiation mode for secure calls.

  This setting identifies the SDP capability the configures whether fallback to RTP will be used and which BE-SRTP approach will be used.

  The following values as possible: **RTP and SRTP (2mline)** (default), **SRTP and RTP (2mline)**, **SRTP only**, **SRTP and RTP (1mline)**.
- **Secure calls alert audible indication**

  This can be set to: **True** or **False**.
- **SRTCP encryption enabled**

  This can be set to: **True** or **False**.
- **SRTP key negotiation method** - the SRTP type(s) for secure calls.

  Identifies the type of SRTP that is allowed to be offered or accepted via SDP.

  The following values as possible: **MIKEY** or **SRTP**.
- **Secure calls payload options**

  This can be set to: **RTP+ SRTP**, **SRTP only**, **SRTP + RTP**.
- **Crypto context update**

  This can be set to: **Full crypto context reset**, **Key update (RFC compliant)**.

SRTP settings configuration for a client

NOTICE: The SRTP settings are only available for SIP clients.

If you have selected to configure the SRTP settings of a **SIP client**, the following settings are available:

- **SRTP Encryption methods** - this indicates if SRTP encryption is enabled or disabled for the selected client.

  This can be set to:

  – ON (green), if you want to enable SRTP encryption.
  – OFF (gray), if you want to disable SRTP encryption.
- **Secure calls enabled**

  This can be set to: **True** or **False**.
- **Secure call alert**

  This can be set to: **True** or **False**.
- **SRTP key negotiation mode** - the SRTP type(s) for secure calls.

  This setting identifies the type of SRTP that is allowed to be offered or accepted via SDP.

  The following values as possible: **MIKEY**, **SDES** (default), **DTLS**, **DTLS-SDES**.
- **SDP negotiation mode** - the SDP negotiation mode for secure calls.

  This setting identifies the SDP capability the configures whether fallback to RTP will be used and which BE-SRTP approach will be used.

  The following values as possible: **RTP and SRTP (2mline)** (default), **SRTP and RTP (2mline)**, **SRTP only**, **SRTP and RTP (1mline)**.

- **Secure calls alert audible indication**

  This can be set to: **True** or **False**.
- **SRTCP encryption enabled**

  This can be set to: **True** or **False**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.4.4 OPUS settings

The **OPUS settings** configuration is available for clients (SIP or HFA) and templates.

To navigate to this area, expand the **Audio** menu, then select **OPUS settings**.

The same configuration settings need be applied for clients and templates, as described below:

- **OPUS Max bandwidth** - the bandwidth that OPUS encoder should operate on.

  This can be set to: **Wideband** (default) or **Narrowband**.
- **OPUS Bitrate type** - indicates the type of bitrate that OPUS encoder should work on.

  This can be set to: **VBR** (Variable Bitrate) or **CBR** (Constant Bitrate).
- **OPUS Max complexity** - the maximum computational complexity of codec.

  Lower values indicate bad quality. The complexity level of OPUS encoder can change to a lower value by SW on-the-fly according to CPU usage. It cannot exceed the value of max complexity item.

  This can be set to values in the range of 0 to 10 (default).
- **OPUS FEC** - this option includes redundant payload data for better quality in lossy networks, but increases computational complexity and bandwidth.

  This can be set to: **True** or **False** (default).
- **OPUS DTX** - this option determines whether to send empty payload frames during silence periods.

  This can be set to: **True** or **False** (default).
- **OPUS PLR** - the packet loss percentage of the network as an input to encoder.

  This can be set to values in the range of 0 (default) to 100.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.4.5 Alerting

The **Alerting** configuration is available for clients (SIP) and templates.

To navigate to this area, expand the **Audio** menu, then select **Alerting**.

- **Group Pickup Tone type**:

  Possible options:

  - Off
  - Beep
  - **Ring burst: phone plays ringer tone for a few seconds when any of the monitored phones starts ringing.**
  - Ring continuous: phone plays ringer tone whilst any of the monitored phones is ringing.
- **Group Pickup Tone Interval**

  A configurable repeat timer, the group pickup tone is repeated whilst there is a group pickup call available to the phone to pick up.You should be able to configure the interval between playing the Group pickup tone between 0 and 30 seconds, where 0 means the tone is played continuously.

  Default: 15 seconds
- **Group Pickup Visual Alert Type**:

  Defines the user action required to accept a pickup call.

  Possible Options:

  - **Prompt** An incoming pickup call is signaled by an alert on the phone GUI. As soon as the user goes off-hook or presses the speaker key, the pickup call is accepted. Alternatively, the user can press the corresponding function key, if configured.
  - **Notify** An incoming pickup call is signaled by an alert on the phone GUI. To accept the call, the user must confirm the alert or press the corresponding function key, if configured.
  - FPK only
- **BLF Alert Type**

  Optical alerting by key.

  Possible Values:

  - **Beep**
  - **Ring burst: phone plays ringer tone for a few seconds when any of the monitored phones starts ringing.**
  - **Ring continuous**: phone plays ringer tone whilst any of the monitored phones is ringing.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.4.6 ICE settings

The **ICE settings** configuration is available for clients (SIP) and templates.

To navigate to this area, expand the **Audio** menu, then select **ICE settings**.

The same configuration settings need be applied for SIP clients and templates, as described below:

- **Main ICE Server Type:** - the type of the main server providing ICE candidate addresses as an indexed list.

- **Backup ICE Server Type:** - the type of the backup server providing ICE candidate addresses as an indexed list.

  This value of the ICE Server Type for the main/backup server, can be set to one of the following values:

  - **None** - The main / backup server is not used.
  - **TURN** - The main /backup server is a TURN server that will return Relayed and Server reflexive candidates
  - **STUN**- The main /backup server is a STUN server that will only return Server reflexive candidates
- **Main ICE Server Address** - the address of the main server providing ICE candidate addresses as an indexed list.
- **Backup ICE Server Address** - the address of the backup server providing ICE candidate addresses as an indexed list.
- **Main ICE Server Port** - the IP port of the main server providing ICE candidate addresses as an indexed list.
- **Backup ICE Server Port** - the IP port of the backup server providing ICE candidate addresses as an indexed list.

  The default port is 3478.

  You should use the default port if the address is an IP address and not an FQDN address.
- **Main ICE Server Username** - the username for main ICE server.
- **Backup ICE Server Username** - the username for backup ICE server.
- **Main ICE Server Password** - the password used for main ICE server.
- **Backup ICE Server Password** - the password used for backup ICE server.

  The password fields for the main and backup ICE servers are read-only and can be edited by clicking the ✎ icon.

  A pop-up window opens prompting you to:

  - Enter the a password you want to set in the **New password** field.
  - Re-enter the new password in the **Confirm new password** field.

  Click **OK** to set the password.
- **Update SDP enabled**

  When enabled, the phone may send an updated SDP offer/answer as required by the ICE standard.

  This can be set to: **True** or **False**.
- **TURN IP mapping enabled**

  When enabled, the TURN server will provide an address mapping between IPv4 and IPv6 peer endpoints.Otherwise,only endpoints supporting the locally configured IP family may be addressed.

  This can be set to: **True** or **False**.
- **Check pairs maximum** - the maximum number of candidate pairs for connectivity checking.
- **Maximum check time (ms)** - the connectivity check duration. This option sets the amount of time in milliseconds allowed to perform the connectivity checks.

  The default value is 5000.

- **Gathering timeout (ms)** - the timeout value in milliseconds which controls the pacing of the ICE Gathering retransmissions sent on a candidate pair.

  The default value is 5000.
- **Gathering TA timer (ms)** - the value in milliseconds which controls the pacing of the candidates gathering.
- **Check TA timer (ms)** - the connectivity check interval. This option sets the Ta timer value in milliseconds which controls the pacing of the ICE Connectivity Checks sent on a candidate pairs.
- **Check TR timer (ms)** - the connectivity check interval. This option sets the Tr timer value in milliseconds which controls the pacing of the ICE Connectivity Checks sent on a candidate pairs.
- **Check RTO timer (ms)** - the connectivity check repeat interval. This option sets the RTO timer value in milliseconds which controls the pacing of the ICE Connectivity Check retransmissions sent on a candidate pair.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.5 Features

This chapter provides instructions for the features configuration options.

7.5.1 LDAP Configuration

The **General** configuration is available for clients, users and templates.

To navigate to this area, expand the **LDAP** menu, then select **General**.

The same configuration settings need be applied for clients, users and templates, as described below:

- **LDAP server address** - the IP address or host name of the LDAP server.
- **LDAP server default port** - the port number of the LDAP server.
- **LDAP server secure port** - the secure port number of the LDAP server.
- **LDAP server transport type** - the transport protocol used to transmit LDAP data.

  This can be set to: **UDP**, **TCP** or **TLS**.
- **LDAP server authentication type** - the authentication type of the LDAP server.

  This can be set to: **Anonymous** or **Simple**.
- **LDAP username** - the username credential for authenticated LDAP access.
- **LDAP password** - the password for authenticated LDAP access
- **LDAP avatar server address** - the server name (FQDN IP Address). This is valid for mobile users that logon to CP200/CP400/CP600 phones of V1R2 version and higher.
- **LDAP search trigger timeout** - search Trigger Timeout for LDAP simple search expressed in seconds.

  This can be set to one of the following values: 1, 2, 3 (default), 4, 5, 6, 7, 8, 9, 10, 60.

- **LDAP manual search only** - allow manual LDAP search on incoming and outgoing calls.

  This can be set to: **True** or **False**.
- **LDAP search firstname and lastname** - enable searching for firstname and lastname.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.5.2 LDAP Template

The **Template** configuration is available for clients, users and templates.

To navigate to this area, expand the **LDAP** menu, then select **Template**.

The same configuration settings need be applied for clients, users and templates, as described below:

- **Search Base** - his is the definition of the base point within the LDAP Directory for searches. This is relative to the initial node in the directory at the point of initial connection. For some LDAP servers, this could be an empty string.
- **Last Name field** - the last name contact field.
- **First Name** - the first name contact field.

> **NOTICE:** Available only for CP200/ CP400/ CP600 HFA phones of version V1R1 and higher.

- **Work 1 number field** - the business 1 contact field.
- **Work 2 number field** - the work 2 number field.
- **Mobile number field** - the mobile number of the contact.
- **Home number field** - this option sets the Private contact field.
- **Company name field** - this option sets the Company contact field.
- **Address 1 field** - this option sets the Address 1 contact field.
- **Address 2 field** - this option sets the Address 2 contact field.
- **Role field** - this option sets the Job function contact field.
- **Email field** - the email address associated with the contact.
- **Nickname field** - this indicates that Simple search should use nickname mode.

  The Attribute field does not relate to a contact field and so the field value is not shown by the phone.
- **Avatar field** - the full address of the web-server that holds avatar images.
- **Last name field** - the last name of the contact.
- **First name field** - the first name of the contact.
- **Work 1 number type** - the type of the Work 1 number.
- **Work 2 number type** - the type of the Work 2 number.
- **Mobile number type** - the type of the mobile number.
- **Home number type** - the type of the home number.
- **Company name type** - the type of Company name.
- **Address 1 type** - the type of Address 1.
- **Address 2 type** - the type of Address 2.
- **Role type** - the type of role.

- **Email type** - the type of email used.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.5.3 Action URLs

To navigate to this area, expand the **Features** menu, then select **Action URLs**.

The same configuration settings need be applied for SIP clients, users and templates, as described below:

- **Phone Started Method**
- **Primary Line Registered Method**
- **Primary Line Unregistered Method**
- **Phone Idle Method**
- **Phone Busy Method**
- **Incoming Call Primary Line Method**
- **Outgoing Call Primary Line Method**
- **Connected Call Primary Line Method**
- **Disconnected Call Primary Line Method**
- **Call Forwarding Primary Line Method**
- **DND Primary Line Method**

  The possible options for the configuration settings mentioned above are:

  – GET
  – POST
  – PUT

  For the configuration settings mentioned below, add the respective URL:

- **Phone Started URL**
- **Primary Line Registered URL**
- **Primary Line Unregistered URL**
- **Phone Idle URL**
- **Phone Busy URL**
- **Incoming Call Primary Line URL**
- **Outgoing Call Primary Line URL**
- **Connected Call Primary Line URL**
- **Disconnected Call Primary Line URL**
- **Call Forwarding Primary Line URL**
- **DND Primary Line URL**

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.5.4 Adressing

To navigate to this area, expand the **Features** menu, then select **Addressing**.

The same configuration settings need be applied for SIP clients, users and templates, as described below:

- **Message Waiting Server URI**

  URI of the message waiting server.
- **Conference URI**

  URI of the conference.
- **Group Pickup URI**:

  URI of the group pickup.
- **Directed Pickup URI**:

  IP address or host name of the server for providing the directed pickup feature.
- **BLF Pickup Code**:

  Feature code for BLF Pickup Code with Asterisk.
- **BLF Resource URI**:

  Default value is set to NULL.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.5.5 Call Recording

To navigate to this area, expand the **Features** menu, then select **Call Recording**.

The same configuration settings need be applied for SIP clients, users and templates, as described below:

The central voice recorder records the entire voice flow of two or more participants.

- **Call Recorder Address**:

  Address of the call recorder.

  The format is similar to an e-mail address: "username@hostname". Therefore, it can accept numbers, symbols and letters.
- **Call Recording Mode**

  Determines the behaviour of the call recording.

  Possible options:

  – **Manual**
  – **Auto Start**
  – **All Calls**
  – Disabled Available for SIP V1R8 (or later) phones.
  – **One call**
- **Call Recording Audible Indication**

  Select the tone for audible notification.

  Possible options:

  – True
  – False (by default)

- **Call Recording Continuous Audible Indication**

  Select the tone for audible notification.

  Possible options:

  – True
  – False (by default)

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.5.6 Feature Availability

To navigate to this area, expand the **Features** menu, then select **Feature Availability**.

The same configuration settings need be applied for SIP clients, users and templates, as described below:

- **Callback allowed for user**:

  This can be set to: **True** or **False**.
- **Web Based Management Allowed**

  A Web-based client interface for administering configurations and modifying user settings via remote access.

  This can be set to: **True** or **False**.
- **Refuse Call Allowed**

  This can be set to: **True** or **False**.
- **Built In Call Forwarding Allowed**

  This can be set to: **True** or **False**.
- **Do Not Disturb Allowed**

  This can be set to: **True** or **False**.
- **Call Pickup Allowed**

  This can be set to: **True** or **False**.
- **Call Recording Allowed**

  This can be set to: **True** or **False**.
- **Blind Transfer Allowed**

  This can be set to: **True** or **False**.
- **Repertory Dial Allowed**

  This can be set to: **True** or **False**.
- **BLF Allowed**

  This can be set to: **True** or **False**.
- **DSS Allowed**

  This can be set to: **True** or **False**.
- **Feature Toggle Allowed**

  This can be set to: **True** or **False**.
- **CTI Allowed**

  This can be set to: **True** or **False**.

- **Line Overview Allowed**

  This can be set to: **True** or **False**.
- **Third Call leg Allowed**

  This can be set to: **True** or **False**.
- **Group Pickup Allowed**

  This can be set to: **True** or **False**.
- **Phone Lock Allowed**

  This can be set to: **True** or **False**.
- **Exchange Allowed**

  This can be set to: **True** or **False**.
- **Circuit Allowed**

  This can be set to: **True** or **False**.
- **OpenScape UC Allowed**

  This can be set to: **True** or **False**.
- **Video Calls Allowed**

  This can be set to: **True** or **False**.
- **Agent Feature Allowed**

  This can be set to: **True** or **False**.
- **Limited FPK Set**

  This can be set to: **No Limitation** or **Set 1**.
- **Bluetooth Allowed**

  This can be set to: **True** or **False**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.5.7 Door opener

To navigate to this area, expand the **Features** menu, then select **Door opener**.

The same configuration settings need be applied for SIP clients, users and templates, as described below:

The following configuration can be set for up to 4 door openers.

- **Door Opener Type**

  Select a control method for the door opener from the drop down list. The available options are:

  - **Disabled** (default value)
  - **Call to open door**
  - **HTTP request to open door**
  - **HTTPS request to open door**
- **Door Opener Name**:

  Freely selectable name for the door opener (can be custom name or alphanumeric). The default name is DoorOpener.
- **Door Opener Method**

  This can be set to: **GET** or **POST**.

- **Door Opener Phone Number**

  The phone number for the door opener.
- **Door Opener Address**:

  IP address or DNS name of the door opener server e.g. 10.10.10.1 or mydoor.local.net.
- **Door Opener Port**:

  Target the port at the server.
- **Door Opener Username**

  Username for the door opener server.
- **Door Opener Password**

  Add a password for the door opener server.

  A pop-up window will be displayed where you need first to add and then to confirm a password.

  The passwords must match.

  Then press **OK** to confirm.
- **Door opener Path**
- **Door Opener URL Parameters**:

  Parameters inside the URL path, e.g. user=name&auth=123456.
- **Door Opener PIN**:

  The PIN to open the door, same PIN as the one configured at Door opener device.
- **Door Opener FPK Confirmation**:

  Checkbox for confirming the key to open the door.

  This can be set to: **True** or **False**.
- **Door Opener Video Camera**:

  If the video camera is available. The default is: None
- **Door Opener Automatic Door Video**:

  When someone rings at the door, the phone rings.

  If the call is from door opener with associated camera and the Automatic Door Video option is enabled, the user can see the camera stream before answering the call by pressing "Show video" SRK or related Camera FPK button. Otherwise, video image is shown automatically only after answering the call.

  If the call is from door opener with associated camera and the Automatic Door Video option is disabled, the user can see the camera stream either before of after answering the call by pressing "Show video" SRK or related Camera FPK button.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.5.8 Direct video

To navigate to this area, expand the **Features** menu, then select **Direct video**.

The same configuration settings need be applied for SIP clients, users and templates, as described below:

The following configuration can be set for up to 4 direct video cameras.

- **Direct Video Enabled**

  This can be set to: **True** or **False**.
- **Camera Name**:

  Freely selectable name for the door opener (can be custom name or alphanumeric). The default name is *Camera*.
- **Camera Protocol**:

  Protocol to transmit video, RTSP and HTTP.
- **Camera Address**:

  IP address or DNS name of the video server (e.g. 10.10.10.1 or mycamera.local.net).
- **Camera URL**:

  URL path of the camera, e.g. /videoapi/stream/
- **Camera Port**:

  Target the port at the server.
- **Camera Username**:

  Enter a username for the camera.
- **Camera Password**:

  Enter a password for the camera.

  A pop-up window will be displayed where you need first to add and then to confirm a password.

  The passwords must match.

  Then press **OK** to confirm.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.6 Network

This chapter provides instructions for the configuration options available in the **Network** menu.

7.6.1 General

The **General** configuration for networks is available for clients and templates.

To navigate to this area, expand the **Network** menu, then select **General**.

General network settings configuration for a client

If you have selected to configure the general network settings of a **client**, the following settings are available:

- **DNS Domain name** - the domain name of the DNS server.
- **DNS server 1** - the IP address or host name of the first DNS server.

- **DNS server 2** - the IP address or host name of the second DNS server.
- **HTTP proxy address** - the IP address or DNS name of the HTTP proxy to be used for sending HTTP requests from the OpenScape Endpoint Management to the clients.
- **HTTP proxy port** - the port of the HTTP proxy used to send HTTP requests from the OpenScape Endpoint Management to the clients.
- **IP packet Time-To-Live** - the lifespan of an IP data packet.

  Data packets transferred in IP networks can take different routes to reach their destination. Every time the data packet moves to a new network it passes a router which decrements the packet's TTL value by one. The packet is discarded when the value reaches 0. This ensures that packets that are unable to find their destination despite lengthy searches do not drift around the Internet ad infinitum. The higher the original TTL value of a data packet, therefore, the longer the packet can try to reach its destination.

  This can be set to: **64 bits** (default) or **128 bits**.
- **LLDP-Med enabled** - this option enables sending and receiving LLDP data.

  This can be set to: **True** (default) or **False**.
- **LLDP-Med Time-To-Live**

  This can be set to one of the following values: 40, 60, 80, 100, 120, 140, 180, 240, 320, 400.
- **VLAN Discovery method** - this settings determines how the VLAN ID is assigned to the end device. Can only be changed when QoS layer 2 has been activated.

  This can be set to one of the following values:

  – **Manual** - The VLAN ID is entered manually.

  – **DHCP** - The VLAN ID supplied by the DHCP server is used.

  – **LLDP-MED** - The VLAN ID supplied by LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discovery) is used. Available for OpenStage from V1R5 onwards.
- **VLAN ID** - the VLAN ID when using virtual LANs. Can only be changed if QoS layer 2 is active. The value is readonly if it has been dynamically assigned with DHCP.

  This can be set to a value in the range of 0 to 4095.
- **DHCPv4 enabled** - this option can be activated if a DHCP server is present.

  The workpoint then obtains the IP address data dynamically from the DHCP server.

  This can be set to: **True** (default) or **False**.
- **DHCP reuse enabled:** - this setting can be activated if a DHCP server is present. If the switch is activated, the DHCP lease will be reused.

  This can be set to: **True** or **False** (default).
- **IPv4 address**
- **IPv4 subnet mask** - the subnet mask for the IP address.
- **IPv4 default gateway** - the IP address or host name of the default gateway.

If you have selected to configure the general network settings of a **HFA client**, the following settings are available:

General network settings configuration for a template

If you have selected to configure the general network settings of a **template**, the following settings are available:

- **DNS Domain name** - the domain name of the DNS server.
- **DNS server 1** - the IP address or host name of the first DNS server.
- **DNS server 2** - the IP address or host name of the second DNS server.
- **HTTP proxy address** - the IP address or DNS name of the HTTP proxy to be used for sending HTTP requests from the OpenScape Endpoint Management to the clients.
- **HTTP proxy port** - the port of the HTTP proxy used to send HTTP requests from the OpenScape Endpoint Management to the clients.
- **IP packet Time-To-Live** - the lifespan of an IP data packet.

  Data packets transferred in IP networks can take different routes to reach their destination. Every time the data packet moves to a new network it passes a router which decrements the packet’s TTL value by one. The packet is discarded when the value reaches 0. This ensures that packets that are unable to find their destination despite lengthy searches do not drift around the Internet ad infinitum. The higher the original TTL value of a data packet, therefore, the longer the packet can try to reach its destination.

  This can be set to: **64 bits** (default) or **128 bits**.
- **Parse DHCP option 43** - the parse option for DHCP (43).

  This can be set to: **True** or **False**.
- **Parse DHCP option 66** - the parse option for DHCP (66).

  This can be set to: **True** or **False**.
- **LLDP-Med enabled** - this option enables sending and receiving LLDP data.

  This can be set to: **True** (default) or **False**.
- **LLDP-Med Time-To-Live**

  This can be set to one of the following values: 40, 60, 80, 100, 120, 140, 180, 240, 320, 400.
- **VLAN Discovery method** - this settings determines how the VLAN ID is assigned to the end device. Can only be changed when QoS layer 2 has been activated.

  This can be set to one of the following values:

  – **Manual** - The VLAN ID is entered manually.
  – **DHCP** - The VLAN ID supplied by the DHCP server is used.
  – **LLDP-MED** - The VLAN ID supplied by LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discovery) is used. Available for OpenStage from V1R5 onwards.
- **VLAN ID** - the VLAN ID when using virtual LANs. Can only be changed if QoS layer 2 is active. The value is readonly if it has been dynamically assigned with DHCP.

  This can be set to a value in the range of 0 to 4095.
- **DHCPv4 enabled** - this option can be activated if a DHCP server is present.

  The workpoint then obtains the IP address data dynamically from the DHCP server.

  This can be set to: **True** (default) or **False**.

- **DHCPv6 enabled**

  This can be set to: **True** (default) or **False**.
- **DHCP reuse enabled:** - this setting can be activated if a DHCP server is present. If the switch is activated, the DHCP lease will be reused.

  This can be set to: **True** or **False** (default).
- **IPv4 address**
- **IPv4 subnet mask** - the subnet mask for the IP address.
- **IPv4 default gateway** - the IP address or host name of the default gateway.
- **IPv6 address global**
- **IPv6 address prefix length**
- **IPv6 address global gateway**
- **IPv6 address link local**

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.6.2 802.1x

The **802.1x** configuration for networks is available for clients and templates.

To navigate to this area, expand the **Network** menu, then select **802.1x**.

If you have selected to configure the 802.1x, the following settings are available:

- **802.1x Authentication type**

  Possible values:

  – **Any Supported**
  – **None**
  – **EAP-TLS** - If selected, the telephone checks the validity of the server certificate sent by the access point.
  – **PEAP** - Provide support for IEEE 802.1x [802.1x] which is a standard for port-based network access control. 802.1x provides an authentication framework where a user (or device) is authenticated by a central authority (in RADIUS model) and where the user (or device) also authenticates the central authority. With this selection PEAP protocol does the extensible authentication.
- **MSCHAP Identity**:

  Device name for MSCHAP.
- **MSCHAP Password**:

  Set a password for MSCHAP. The value is write-only.
- **Confirm 802.1x installation**

  This can be set to: **True** or **False**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.6.3 Wi-Fi Settings

The **Wi-Fi Settings** configuration for networks is available for templates.

To navigate to this area, expand the **Network** menu, then select **Wi-Fi Settings**.

- **Wi-Fi Interface Enabled**

  This can be set to: **True** or **False**.
- **Wi-Fi Country Settings**

  Select the country from the list.
- **Wi-Fi Frequency Band**

  Select the frequency from the list.

  Possible values:

  - **5 GHz + 2.4 GHz**
  - **5 GHz**
  - **2.4 GHz**
- **Wi-Fi Allowed 5 GHz Channels**

  Possible values:

  - **All**
  - **Non DFS**
  - **UNII-1**
  - **UNII-3**
  - **UNII-1 + UNII-2**
  - **UNII-1 + UNII-2 + UNII-3**
  - **UNII-1 + UNII-2 Extended**
  - **Manual Selection**
- **Wi-Fi Manual Selected 5 GHz Channels**:

  Add manually the 5GHz Channel.
- **Wi-Fi Allowed 2.4 GHz Channels**:

  Possible values:

  - **All**
  - **Channel 1 + 6 +11**
  - **Manual Selection**
- **Wi-Fi Manual Selected 2.4 GHz Channels**

  Add manually the 2.4 GHz Channels.
- **Wi-Fi 802.11r Enabled**

  This can be set to: **True** or **False**.
- **Wi-Fi Roaming RSSI Threshold**

  Add the Wi-Fi Roaming RSSI Threshold.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.6.4 Wi-Fi Networks

The **Wi-Fi Network** configuration for networks is available for templates.

To navigate to this area, expand the **Network** menu, then select **Wi-Fi Network**.

You can configure Wi-Fi Network SSID by clicking **+**.

A window will be displayed with the following settings:

- **Wi-Fi Network SSID**

  The SSID is the network name used to identify the WLAN phone. The SSID is defined in the access point (WLAN router).
- **Wi-Fi Network Password**

  Insert the password to access the network.
- **Wi-Fi SSID hidden**

  If you set it to: **True** you choose to hide the name of the Wi-Fi Network.

  This can be set to: **True** or **False**.
- **Wi-Fi Encryption**

  This field enables you to select the type of key encryption algorithm from a drop-down box with the following choices:

  – **None** Data is not encrypted for transmission in the Wi-Fi.
  – **WEP** WEP Wi-Fi protected access mode.
  – **WPA/WPA2 Personal**
  – **WPA/WPA2 Enterprise**
  – **WPA2-Personal**
  – **WPA2-Enterprise**
  – **WPA2/WPA3-Personal**
  – **WPA3-Personal**
- **Wi-Fi IP Settings**

  – **DHCP** (Dynamic Host Configuration Protocol)

    Select this option to enable automatic management of IP addresses on the network.
  – **Manual**

    Select this option to enable manual management of IP addresses on the network.
- **IP Address**

  Enter the adress of IP.
- **IP Subnet Mask**

  Enter the IP mask Wi-Fi number.
- **IP Default Route**
- **Wi-Fi Authentication Mode**

  Select an Authentication protocol type.

  – **None**
  – **PEAPv0/EAP-MSCHAPv2**
  – **EAP-TLS**
  – **EAP-LEAP**
  – **FAST**
- **Wi-Fi EAP Identity**

  Enter EAP identity.
- **Wi-Fi EAP Password**

  Enter the EAP password number.

Click **Confirm** to save your selection.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.6.5 Routing

The **Routing** configuration for networks is available for clients and templates.

To navigate to this area, expand the **Network** menu, then select **Routing**.

Routing settings configuration for a client

If you have selected to configure the routing settings of a **client**, the following settings are available:

- **IPv4 Route 1 destination** - the IPv4 address or host name of the first static route.
- **IPv4 Route 1 subnet mask** - the subnet mask of the first static route.
- **IPv4 Route 1 gateway** - the IPv4 address or host name of the router/ gateway of the first static route.
- **IPv4 Route 2 destination** - the IPv4 address or host name of the second static route.
- **IPv4 Route 2 subnet mask** - the subnet mask of the second static route.
- **IPv4 Route 2 gateway** - the IPv4 address or host name of the router/ gateway of the second static route.

Routing settings configuration for a template

If you have selected to configure the routing settings of a **template**, the following settings are available:

- **IPv4 Route 1 destination** - the IPv4 address or host name of the first static route.
- **IPv4 Route 1 subnet mask** - the subnet mask of the first static route.
- **IPv4 Route 1 gateway** - the IPv4 address or host name of the router/ gateway of the first static route.
- **IPv4 Route 2 destination** - the IPv4 address or host name of the second static route.
- **IPv4 Route 2 subnet mask** - the subnet mask of the second static route.
- **IPv4 Route 2 gateway** - the IPv4 address or host name of the router/ gateway of the second static route.
- **IPv6 Route 1 destination** - the IPv6 address or host name of the first static route.
- **IPv6 Route 1 prefix length** - the prefix length of the first IPv6 static route.
- **IPv6 Route 1 gateway** - the IPv6 address or host name of the router/ gateway of the first static route.
- **IPv6 Route 2 destination** - the IPv6 address or host name of the second static route.
- **IPv6 Route 2 prefix length** - the prefix length of the second IPv6 static route.
- **IPv6 Route 2 gateway** - the IPv6 address or host name of the router/ gateway of the second static route.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.6.6 Interface settings

The **Interface settings** configuration for networks is available for clients and templates.

To navigate to this area, expand the **Network** menu, then select **Interface settings**.

Routing settings configuration for a client

If you have selected to configure the interface settings of a **client**, the following settings are available:

- **LAN port status** - the status of the LAN port.

  This field is read-only.
- **LAN port speed** - the average speed of the LAN port.
- **PC port status** - the status of the PC port.

  This field is read-only.
- **PC port speed** - the speed of the PC port.

  The following values for port speeds are possible:

  – Any
  – 10 Mbit half-duplex
  – 10 Mbit full-duplex
  – 100 Mbit half-duplex
  – 100 Mbit full-duplex
  – 1000 Mbit full-duplex
- **PC port mode** - the operating mode of the PC port.

  The following values are possible: **Disabled**, **Enabled**, **Mirror**.
- **PC port Auto-MDIX**

  This can be set to: **True** or **False**.

Interface settings configuration for a template

If you have selected to configure the interface settings of a **template**, the following settings are available:

- **LAN port speed** - the average speed of the LAN port.
- **PC port speed** - the speed of the PC port.

  The following values for port speeds are possible:

  – Any
  – 10 Mbit half-duplex
  – 10 Mbit full-duplex
  – 100 Mbit half-duplex
  – 100 Mbit full-duplex
  – 1000 Mbit full-duplex
- **PC port mode** - the operating mode of the PC port.

  The following values are possible: **Disabled**, **Enabled**, **Mirror**.
- **PC port Auto-MDIX**

  This can be set to: **True** or **False**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.6.7 Quality of Service

The **Quality of Service** configuration for networks is available for Clients templates.

To navigate to this area, expand the **Network** menu, then select **Quality of Service**.

- **Layer 2 Enabled**

  This can be set to: **True** or **False**.
- **Layer 2 Voice**

  Value range: **0** ... **7**
- **Layer 2 Signalling**

  Value range: **0** ... **7**
- **Layer 2 Default**

  Value range: **0** ... **7**
- **Layer 2 Video**

  Value range: **0** ... **7**
- **Layer 3 Enabled**

  This can be set to: **True** or **False**.
- **Layer 3 Voice**

  Possible values

  - BE (Default value)
  - AF11
  - AF12
  - AF13
  - AF21
  - AF22
  - AF23
  - AF31
  - AF32
  - AF33
  - AF41
  - AF42
  - AF43
  - EF
  - CS7
  - CS3
  - CS4
  - CS5
  - Value range: **0** ... **63**

- **Layer 3 Signalling**

  Possible values

  - BE (Default value)
  - AF11
  - AF12
  - AF13
  - AF21
  - AF22
  - AF23
  - AF31
  - AF32
  - AF33
  - AF41
  - AF42
  - AF43
  - EF
  - CS7
  - CS3
  - CS4
  - CS5
  - Value range: **0** ... **63**
- **Layer 3 Voice**

  Possible values

  - BE (Default value)
  - AF11
  - AF12
  - AF13
  - AF21
  - AF22
  - AF23
  - AF31
  - AF32
  - AF33
  - AF41
  - AF42
  - AF43
  - EF
  - CS7
  - CS3
  - CS4
  - CS5
  - Value range: **0** ... **63**

- **MLPP Immediate**

  Possible values

  - BE (Default value)
  - AF11
  - AF12
  - AF13
  - AF21
  - AF22
  - AF23
  - AF31
  - AF32
  - AF33
  - AF41
  - AF42
  - AF43
  - EF
  - CS7
  - CS3
  - CS4
  - CS5
  - Value range: **0** ... **63**
- **MLPP Flash**

  Possible values

  - BE (Default value)
  - AF11
  - AF12
  - AF13
  - AF21
  - AF22
  - AF23
  - AF31
  - AF32
  - AF33
  - AF41
  - AF42
  - AF43
  - EF
  - CS7
  - CS3
  - CS4
  - CS5
  - Value range: **0** ... **63**

- **MLPP Flash Override**

  Possible values

  - BE (Default value)
  - AF11
  - AF12
  - AF13
  - AF21
  - AF22
  - AF23
  - AF31
  - AF32
  - AF33
  - AF41
  - AF42
  - AF43
  - EF
  - CS7
  - CS3
  - CS4
  - CS5
  - Value range: **0** ... **63**

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.7 Mobile User

This chapter provides instructions for the configuration options available in the **Mobile User** menu.

7.7.1 General

The **General** user configuration is available for templates, clients and users.

To navigate to this area, expand the **User** menu, then select **General**.

General user settings configuration for a user or a client

If you have selected to configure the general user settings of a **SIP client** or a **user**, the following settings are available:

- **Language** - the domain name of the DNS server.
- **Country** - the IP address or host name of the first DNS server.
- **Enable display ID**

  This can be set to: **True** or **False** (default).

  If set to **True**, the call menu will be hidden after an adjustable timeout.
- **Display ID** - the ID of the user display.
- **Presence key forwarding types**

  This can be set to: **Only all calls** (default) or **All CF types**.

- **Show icon for all forwarding types**

  This can be set to: **True** or **False** (default).
- **MWI Led setting** - the Message Waiting Indicator (MWI).

  This can be set to: **MWI key only**, **MWI key and AlertBar LED**, **AlertBar LED** (default), **No LED**.
- **Missed call LED** - when this option is activated, the red LED indicating new missed calls will be extinguished as soon as the user enters the Conversations menu.

  This can be set to: **MWI key only**, **MWI key and AlertBar LED**, **AlertBar LED** (default), **No LED**.
- **IL alerts enabled** - by activating an inhibit notification popup / tone when level changes during call (connected or alerting) or when it connects without ringing.

  This can be set to: **True** (default) or **False**.

If you have selected to configure the general user settings of a **HFA client**, the following settings are available:

- **Language** - the domain name of the DNS server.
- **Country** - the IP address or host name of the first DNS server.

General user settings configuration for a template

If you have selected to configure the general user settings of a **template**, the following settings are available:

- **Language** - the domain name of the DNS server.
- **Country** - the IP address or host name of the first DNS server.
- **Enable display ID**

  This can be set to: **True** or **False** (default).

  If set to **True**, the call menu will be hidden after an adjustable timeout.
- **Display ID** - the ID of the user display.
- **Presence key forwarding types**

  This can be set to: **Only all calls** (default) or **All CF types**.
- **Show icon for all forwarding types**

  This can be set to: **True** or **False** (default).
- **MWI Led setting** - the Message Waiting Indicator (MWI).

  This can be set to: **MWI key only**, **MWI key and AlertBar LED**, **AlertBar LED** (default), **No LED**.
- **Missed call LED** - when this option is activated, the red LED indicating new missed calls will be extinguished as soon as the user enters the Conversations menu.

  This can be set to: **MWI key only**, **MWI key and AlertBar LED**, **AlertBar LED** (default), **No LED**.
- **Auto hide call menu**

  This can be set to: **True** or **False**.
- **Auto hide call menu time**

  This can be set to one of the following values: 0min, 5sec, 10sec, 20sec, 30sec, 60sec, 120sec.

- **IL alerts enabled** - by activating an inhibit notification pop-up / tone when level changes during call (connected or alerting) or when it connects without ringing.

  This can be set to: **True** (default) or **False**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.7.2 FPK

The **FPK** user configuration is available for templates, clients and users.

To navigate to this area, expand the **User** menu, then select **FPK**.

The same FPK settings need be applied for clients, user and templates, as described below:

Click ⊕. The **Add FPK** window opens and you can add the following settings:

- **Key** - select the key you want to assign to FPK.
- **Function** - select the function you want to assign to the key selected.

  Depending on the function you have selected, additional fields are displayed in the **Add FPK** window. Complete all fields accordingly, then click **Add**.

  The new key is added to the FPK list.

  To add another key, click ⊕ again and complete add fields accordingly.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.7.3 Display

The **FPK** user configuration is available for clients, users and templates.

To navigate to this area, expand the **User** menu, then select **FPK**.

Display settings configuration for a user or a template

If you have selected to configure the display settings of a **user** or a **template**, the following settings are available:

- **Inactivity screen type**

  This can be set to: **Menu Screen**, **Slideshow**, **Time screen**.
- **Inactivity Timeout**

  This can be set to one of the following values: 1, 5, 10, 20, 30, 60, 120.
- **Screensaver enabled**

  This can be set to: **True** (default) or **False**.
- **Screensaver image timeout** - the time interval in seconds for changing the images.

  This can be set to one of the following values: 5, 10, 20, 30, 60.

- **Pixelsaver timeout** - this option indicates when your screen times out.

  This can be set to one of the following values:

  – 1 min/ 5 min
  – 5 min/ 20 min
  – 30 min/ 2 hrs
  – 45 min/ 4 hrs
  – 60 min/ 8 hrs
- **Display Brightness**

  This can be set to one of the following values: -3, -2, -1, Default, +1, +2, +3.
- **Key module display text level** - the size of the displayed text.

  This can be set to one of the following values: **Normal** (default), **Medium**, **High**, **Max**.
- **Landing screen** - the landing screen from the drop-down list.

  This can be set to one of the following values: **Conversations**, **Favourites**, **Main Menu**.

Display settings configuration for a client

To configure the display settings of a HFA client, you must apply the same settings as described for a user or a template, except the **Landing screen** option which is not available for HFA clients.

To configure the display settings of a SIP client, you must apply the same settings as described for a user or a template, except the **Screensaver enabled** option which is not available for SIP clients.

7.7.4 Tones and Ringer

The **Tones and Ringer** user configuration is available for templates, clients and users.

To navigate to this area, expand the **User** menu, then select **Tones and Ringer**.

If you have selected to configure the Tones and Ringer settings of a **user**, a **SIP client** or a **template**, the following settings are available:

- **Ringer** - the Ringer File Name of the audio file containing the ringtone.
- **Pattern melody** - the pattern of the audio file containing the ringtone.
- **Pattern sequence**
- **Open listening**

  This can be set to: **Sandard Mode** or **US mode** (default option).
- **Headset socket**

  This can be set to: **Wired headset**, **Cordless**, **Conference unit**.
- **Key click volume** - the volume of key clicks.

  This can be set to: **Off**, **Low**, **Medium**, **High**.
- **Key click keys** - which keys shall have audible clicks.

  This can be set to: **Dialpad only**(default) or **All keys**.
- **Music on hold enabled** - music on hold for held and parked calls.

  This can be set to: **True** or **False**.

If you have selected to configure the Tones and Ringer settings of a **HFA client**, the following settings are available:

- **Ringer** - the Ringer File Name of the audio file containing the ringtone.
- **Headset socket**

  This can be set to: **Wired headset**, **Cordless**, **Conference unit**.
- **Key click volume** - the volume of key clicks.

  This can be set to: **Off**, **Low**, **Medium**, **High**.
- **Key click keys** - which keys shall have audible clicks.

  This can be set to: **Dialpad only**(default) or **All keys**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.7.5 Special Ringer

The **Special Ringer** user configuration is available for templates, clients and users.

To navigate to this area, expand the **User** menu, then select **Special Ringer**.

If you have selected to configure the Special Ringer settings of a **user**, a **SIP client** or a **template**, the following settings are available:

- **Ringer Internal Call** - the Ringer File Name of the audio file containing the ringtone.
- **Ringer External Call** - the pattern of the audio file containing the ringtone.
- **Ringer Callback Call** - the pattern of the audio file containing the ringtone.
- **Ringer Emergency Call** - the pattern of the audio file containing the ringtone.
- **Ringer Special Call 1, 2 or 3**
- **Special Ringer from 1 up to 5**

  You can manage the configuration or add special ringers by clicking **+** to add or ✏ to edit.

  A window will be displayed with the following settings:

  - Alert info
  - Ringer File - Select from the dropdown list the pattern of the audio file containing the ringtone.
  - Ringer Melody - Select from the dropdown list the number of the audio file containing the ringtone (Value range 1...8) or you can set the ringer to be muted.
  - Ringer Tone -Select from the dropdown list the tone of the audio file containing the ringtone (Value range 1...6).
  - Ringer Tone Duration - set the duration of the ringer tone. Default: 60 seconds.

Click **Confirm** to save your selection.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.7.6 Call logging

The **Call logging** user configuration is available for templates, clients (SIP) and users.

To navigate to this area, expand the **User** menu, then select **Call logging**.

If you have selected to configure the call logging settings of a **user**, a **SIP client** or a **template**, the following settings are available:

- **Call Log Enabled** - this option indicates whether Call logging is enabled.

  This can be set to: **True** (default) or **False**.
- **Delete missed calls automatically** - this option indicates whether calls log entries are deleted in case there is a call to an entry in Missed calls list.

  This can be set to: **Delete manually** (default) or **Delete when called**.
- **Call logging for answered elsewhere** - calls completed elsewhere will not be logged on phone.

  This can be set to one of the following options:

  – **Include in call log** (default) - outgoing calls that are made to entries in Missed calls tab of call log and that are connected will not be deleted from call log.

  – **Do not include in call log** - outgoing calls that are made to entries in Missed calls tab of call log and that are connected will be deleted from call log.

> **NOTICE:** The call logging settings are not available for HFA clients.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.7.7 CTI settings

The **CTI settings** user configuration is available for templates, clients (SIP) and users.

To navigate to this area, expand the **User** menu, then select **CTI settings**.

If you have selected to configure the CTI settings of a **user**, a **SIP client** or a **template**, the following settings are available:

- **Auto answer calls enabled** - The user can determine whether incoming calls are accepted automatically by the CTI application which is connected to the phone.

  This can be set to: **True** or **False** (default).
- **Auto reconnect calls enabled** - the user can determine whether a held call can be reconnected automatically by the CTI application.

  This can be set to: **True** or **False** (default).
- **Beep tone on auto answer** - the user can determine whether a signal will sound when a call that is accepted automatically by the CTI application connected to the phone.

  This can be set to: **True** or **False** (default).

- **Beep tone on auto reconnect** - the user can determine whether a signal will sound when a held call is reconnected by the CTI application.

  This can be set to: **True** or **False** (default).

> **NOTICE:** The CTI settings are not available for HFA clients.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.7.8 Call handling

The **Call handling** user configuration is available for templates, clients (SIP) and users.

To navigate to this area, expand the **User** menu, then select **Call handling**.

If you have selected to configure call handling of a **user**, a **SIP client** or a **template**, the following settings are available:

- **Call waiting enabled** - by activating visual and/or acoustic alerting for waiting calls

  This can be set to: **True** (default) or **False**.
- **Call waiting tone enabled** - by activating visual and/or acoustic alerting for waiting calls

  This can be set to: **True** (default) or **False**.
- **Do not disturb enabled** - activate the function for rejecting calls.

  This can be set to: **True** (default) or **False**.
- **Transfer calls enabled** - activate the function for transferring calls. If this option is activated, you can activate call transfer by replacing the handset even before the called party answers.

  This can be set to: **True** (default) or **False**.
- **Deflect calls enabled** - activate the function to deflect incoming calls.

  This can be set to: **True** (default) or **False**.
- **Default deflect destination** - the destination number for call forwarding.
- **Join calls enabled** - activate the function for joining calls.

  The user can join the first party with the party he consulted, clearing down his own connection to both parties in the process.

  This can be set to: **True** (default) or **False**.
- **Leave conference enabled** - activate the leave active conference.

  The user is disconnected from the conference call and the other call partners remain connected.

  This can be set to: **True** or **False** (default).
- **Held call reminder enabled** - the user specifies when he wants to receive an automatic reminder about a held call.

  Possible options:

  This can be set to: **True** (default) or **False**.

- **Held call reminder time** - the delay for the Hold Reminder in minutes.

  The minimum time value is 1, that is, the reminder is output after one minute. The maximum value is 15 minutes.
- **Hold and hangup** - activate the Hold and Hangup feature.

  This feature enables the user to temporarily hold and hang up a line without disconnecting your caller.

  This can be set to: **True** or **False** (default).
- **Conference calls enabled** - the user can allow system based conferences. Only available in optPoint workpoints.

  This can be set to: **True** (default) or **False**.
- **Busy when dialling enabled** - the user can determine whether incoming calls are refused while a call number is entered.

  This can be set to: **True** (default) or **False**.
- **Transfer during ringing enabled** - the user can determine whether a call is transferred as soon as the third participant’s phone rings, even if the transferring participant has not hung up.

  This can be set to: **True** (default) or **False**.
- **Initial digit timer** - the waiting time in seconds for a dialed digit after the dial tone starts.
- **Auto dial delay** - the delay time between the entry of the last call number digit and the start of the dialing process can be set by the user.

  It can be selected from 1 second to 9 seconds.
- **Implicit call association enabled** - activate the call association feature.

  This can be set to: **True** or **False** (default).

NOTICE: The CTI settings are not available for HFA clients.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.7.9 Call forwarding

The **Call forwarding** user configuration is available for templates, clients (SIP or HFA) and users.

To navigate to this area, expand the **User** menu, then select **Call forwarding**.

If you have selected to configure call forwarding of a **HFA client**, the following setting is available:

- **Visual alert time** - when visual alert is active, the toast message is shown on the forwarding phone screen according to the set time. The toast message appears for 5 seconds by default. However, you can configure the visual alert’s appearing time from this field.

  This can be set to a value in the range of 1 to 15 second.

If you have selected to configure call forwarding of a **SIP client**, a **user** or a **template** the following settings are available:

- **On busy activated** - the call forwarding activated on busy status.

  This can be set to: **True** or **False** (default).
- **On busy address** - the call number of the Call Forwarding destination.
- **No reply activated:**

  This can be set to: **True** or **False** (default).
- **No reply address** - the call number of the call Forwarding destination.
- **No reply delay (seconds)**

  As soon as this time span has expired without the call being accepted, the call is forwarded.
- **Unconditional activated** - by activating Unconditional Call Forwarding.

  This can be set to: **True** or **False** (default).
- **Unconditional address** - the call number of the Unconditional Call Forwarding destination.
- **Forwarding audible notification** - select an audible alert on the forwarding phone.

  This can be set to: **True** (default) or **False**.
- **Forwarding visual notification** - select a visual alert on the forwarding phone.

  This can be set to: **True** (default) or **False**.
- **Forwarding party display** - select which forwarding party will be displayed when multiple forwarding is active.

  This can be set to: **Display first** or **Display last**.
- **Forwarding favourite 1**, **Forwarding favourite 2**, **Forwarding favourite 3**, **Forwarding favourite 4**, **Forwarding favourite 5** - the order of the forwarding call favorite in case of unconditional, no reply or on busy.

7.7.10 Call forwarding Internal/ External

The **Call forwarding Internal/ External** user configuration is available for clients (SIP), templates and users.

To navigate to this area, expand the **User** menu, then select **Call forwarding Internal/ External**.

Call forwarding Internal/ External configuration for a user or a template

If you have selected to configure call forwarding Internal/ External for a **user** or a **template**, the following settings are available:

- **Internal/External menu allowed**

  This can be set to: **True** (default) or **False**.
- **On busy external activated** - call forwarding activated on busy status.

  This can be set to: **True** or **False** (default).
- **On busy external address** - the call number of the Call Forwarding destination.
- **On busy internal activated** - the call number of the Call Forwarding destination.

  This can be set to: **True** or **False** (default).

- **On busy internal address** - the call number of the Call Forwarding destination.
- **No reply external activated**

  This can be set to: **True** or **False** (default).
- **No reply external address** - the call number of the call Forwarding destination.
- **No reply internal activated**

  This can be set to: **True** or **False** (default).
- **No reply internal address** - the call number of the call Forwarding destination.
- **Unconditional external activated**

  This can be set to: **True** or **False** (default).
- **Unconditional external address** - call number of the call Forwarding destination.
- **Unconditional internal activated**

  This can be set to: **True** or **False** (default).
- **Unconditional internal address** - the call number of the call Forwarding destination.

Call forwarding Internal/ External configuration for a SIP client

NOTICE: This configuration is not available for HFA clients.

If you have selected to configure call forwarding Internal/ External for a **SIP client**, you must configure the same settings as described for templates and users.

In addition to these settings, several additional options are available for SIP clients:

- **cfu-unchangeable**
- **cfu-ext-unchangeable**
- **cfu-int-unchangeable**
- **cfb-unchangeable**
- **cfb-ext-unchangeable**
- **cfb-int-unchangeable**
- **cfnr-unchangeable**
- **cfnr-ext-unchangeable**
- **cfnr-int-unchangeable**

These options are read-only and are set to **False** by default.

7.7.11 Callback

The **Callback** configuration is available for clients (SIP), templates and users.

To navigate to this area, expand the **User** menu, then select **Callback**.

If you have selected to configure the Callback settings of a **user**, a **SIP client** or a **template**, the following settings are available:

- **Callback on busy code** - code for controlling the "Callback on busy" function on the server.
- **Callback on busy allowed for user** - activate the callback on busy feature for user.

  This can be set to: **True** (default) or **False**.
- **Callback on busy enabled** - the user can activate the transmission of a callback request to the system. With OpenStage V3 onwards, the callback request can be transmitted in every case; with other end devices, this is only possible in busy case.

  This can be set to: **True** (default) or **False**.
- **Callback on ring code** - the code for controlling the "Callback on ring" function on the server.

  This can be set to: **True** or **False** (default).
- **Callback on ring allowed for user** - activate the callback on ring feature for user.

  This can be set to: **True** or **False**.
- **Callback on ring enabled** - the user can activate the transmission of a callback request to the system in case a call is not replied.

  This can be set to: **True** or **False**.

  If the call is not accepted and the time span expires, the call is forwarded.
- **Cancel callback allowed for user**

  This can be set to: **True** or **False**.
- **Cancel callback code** - the code for cancelling the callback function on the server.

NOTICE: The Callback configuration is not available for HFA clients.

7.8 Security

This chapter provides instructions for the configuration options available in the **Security** menu.

7.8.1 General

The **General** security configuration is available for templates, clients (SIP and HFA) and users.

To navigate to this area, expand the **Security** menu, then select **General**.

General security settings configuration for a template

If you have selected to configure general security settings for a **template**, the following settings are available:

- **Software image verification enabled** - this option enables or disables the software image verification.

  This can be set to: **True** (default) or **False**.

- **FIPS mode enabled** - this option enables or disables the workpoint-booting in FIPS mode.

  This can be set to: **True** or **False** (default).
- **Server interface TLS version** - the standard protocol for performing computer authentication using certificates and encryption.

  This can be set to: **Only latest TLS versions** (default) or **All TLS versions**.
- **Local interface TLS version** - the standard protocol for performing computer authentication using certificates and encryption.

  This can be set to: **Only latest TLS versions** (default) or **All TLS versions**.
- **Web based management enabled** -a Web-based client interface for administering configurations and modifying user settings via remote access.

  This can be set to: **True** (default) or **False**.
- **HPT interface enabled** - this option enables or disables redirection to an external jHPT server and allowing configuration.

  This can be set to: **True** or **False** (default).
- **Factory reset claw enabled**

  This can be set to: **True** (default) or **False**.
- **Serial port** - this option shows password protection mode for the serial port.

  This can be set to: **Password required** (default), **No password**, **Unavailable**.
- **Disable local clock**

  This can be set to: **True** or **False** (default).
- **DoS protection enabled**

  This can be set to: **True** or **False** (default).

General security settings configuration for a client (SIP or HFA)

If you have selected to configure general security settings for a **SIP client**, the same settings as described for templates need to be configured, except the **Disable local clock** option, which is not available on SIP clients.

If you have selected to configure general security settings for a **HFA client**, the same settings as described for templates need to be configured, except the **FIPS mode enabled** option, which is not available on HFA clients.

General security settings configuration for a user

If you have selected to configure general security settings for a **user**, the following settings are available:

- **HPT interface enabled** - this option enables or disables redirection to an external jHPT server and allowing configuration.

  This can be set to: **True** or **False** (default).
- **DoS protection enabled**

  This can be set to: **True** or **False** (default).

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.8.2 Certificate Authorities

The **Certificate Authorities** configuration is available for templates, clients (SIP or HFA) and users.

To navigate to this area, expand the **Security** menu, then select **Certificate Authorities**.

If you have selected to configure Certificate Authorities settings for a **template**, you can add the following certificate authorities:

- **HTTPS server CA certificate 1**
- **HTTPS server CA certificate 2**
- **LDAP server CA certificate 1**
- **LDAP server CA certificate 2**
- **VoIP server CA certificate 1**
- **VoIP server CA certificate 2**
- **OCSR server 1 CA certificate 1**
- **OCSR server 1 CA certificate 2**
- **OCSR server 2 CA certificate 1**
- **OCSR server 2 CA certificate 2**
- **OCSR signature 1 CA certificate 1**
- **OCSR signature 1 CA certificate 2**
- **OCSR signature 2 CA certificate 1**
- **OCSR signature 2 CA certificate 2**
- **Radius server CA certificate 1**
- **Radius server CA certificate 2**
- **DMS server CA certificate 1**
- **DMS server CA certificate 2**
- **XSI server CA certificate 1**
- **XSI server CA certificate 2**
- **Exchange server CA certificate 1**
- **Exchange server CA certificate 2**
- **OpenScape UC server CA certificate 1**
- **OpenScape UC server CA certificate 2**

If you have selected to configure Certificate Authorities settings for a **user**, you can add the following certificate authorities:

- **Send URL server CA certificate 1**
- **Send URL server CA certificate 2**

If you have selected to configure Certificate Authorities settings for a **SIP client**, you can add the following certificate authorities:

- **HTTPS server CA certificate 1**
- **HTTPS server CA certificate 2**
- **LDAP server CA certificate 1**
- **LDAP server CA certificate 2**
- **VoIP server CA certificate 1**
- **VoIP server CA certificate 2**
- **Send URL server CA certificate 1**
- **Send URL server CA certificate 2**
- **OCSR server 1 CA certificate 1**
- **OCSR server 1 CA certificate 2**

- **OCSR server 2 CA certificate 1**
- **OCSR server 2 CA certificate 2**
- **OCSR signature 1 CA certificate 1**
- **OCSR signature 1 CA certificate 2**
- **OCSR signature 2 CA certificate 1**
- **OCSR signature 2 CA certificate 2**
- **Radius server CA certificate 1**
- **Radius server CA certificate 2**
- **DMS server CA certificate 1**
- **DMS server CA certificate 2**
- **XSI server CA certificate 1**
- **XSI server CA certificate 2**
- **Exchange server CA certificate 1**
- **Exchange server CA certificate 2**
- **E/A cockpit server CA certificate 1**
- **E/A cockpit server CA certificate 2**
- **OpenScape UC server CA certificate 1**
- **OpenScape UC server CA certificate 2**
- **ACS server CA certificate 1**
- **ACS server CA certificate 2**

In addition to the list above, you can add 20 **wlan-ca-cert** certificates and 2 **wlan-ca-cert-shared** certificates.

If you have selected to configure Certificate Authorities settings for a **HFA client**, you can add the same certificate authorities as described for templates.

To add a certificate authority:

1) Click ✎ at the right of the desired authority.

   The **Edit certificate authority** window opens prompting you to upload a certificate.
2) Click **Browse** and add the certificate you want to upload from your local computer.
3) Click **Update certificate**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.8.3 Certificates

The **Certificates** configuration is available for templates and clients (SIP or HFA).

To navigate to this area, expand the **Security** menu, then select **Certificates**.

If you have selected to configure Certificates settings for a **template**, you can add the following certificates:

- **HTTPS client certificate**
- **VoIP client certificate**
- **Web based management certificate**
- **802.1x client certificate**
- **PC application certificate**

- **DMS client certificate**
- **ACS client certificate**
- **Device specific client certificate**
- **LDAP client certificate**
- **WLAN client certificate shared**
- 20 **wlan-client-cert** certificates

If you have selected to configure Certificates settings for a **HFA client**, you can add the following certificates:

- **HTTPS client certificate**
- **VoIP client certificate**
- **Web based management certificate**
- **802.1x client certificate**

If you have selected to configure Certificates settings for a **SIP client**, you can add the same certificates as listed for templates, except the **PC application certificate** which is not available for this type of client.

To add a certificate:

1) Click ✎ at the right of the desired certificate.

   The **Edit certificate** window opens prompting you to upload a certificate.
2) Click **Browse** and add the certificate you want to upload from your local computer.
3) Click **Update certificate**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.8.4 Verification policies

The **Verification policies** configuration is available for templates and clients (SIP or HFA).

To navigate to this area, expand the **Security** menu, then select **Verification policies**.

If you have selected to configure verification policies for a **template**, the following policies are available:

- **SIP authentication policy**
- **HFA authentication policy**
- **802.1x authentication policy**
- **HTTPS authentication policy**
- **LDAP authentication policy**
- **Send URL authentication policy**
- **DMS authentication policy**
- **XSI authentication policy**
- **Exchange authentication policy**
- **E/A Cockpit authentication policy**
- **OpenScape UC authentication policy**
- **ACS authentication policy**
- **WLAN authentication policy**

If you have selected to configure verification policies for a **HFA client**, the following policies are available:

- **HFA authentication policy**
- **802.1x authentication policy**
- **HTTPS authentication policy**
- **LDAP authentication policy**
- **Send URL authentication policy**

If you have selected to configure verification policies for a **SIP client**, the following policies are available:

- **SIP authentication policy**
- **802.1x authentication policy**
- **HTTPS authentication policy**
- **LDAP authentication policy**
- **Send URL authentication policy**
- **DMS authentication policy**
- **XSI authentication policy**
- **ACS authentication policy**
- **WLAN authentication policy**

For each verification policy, you can set one of the following values.

- **No verification** - No authentication of server. Invalid certificates, which are received before by server or has been loaded by IP Phone, will be ignored. HTTPS connections to server are setup without authentications always.
- **Trusted** Certificates are checked for "expired", "not valid", "signed by trusted CA", and "revoked". Therefore one or two list of "trusted CAs" are required. The same list will be used for "trusted" and "full". As "trusted CAs" may be used RootCAs, temporary created CAs, or even the server certificate itself. Additional values, such as owner or issuer are not checked. HTTPS connections to server are setup even if some values of the certificate are incorrect.
- **Full** Certificates are checked for "expired", "not valid", "signed by trusted CA", "revoked", matching owner and so on. Therefore one or two list of "trusted CAs" are required. The same list will be used for "trusted" and "full". As "trusted CAs" may be used RootCAs, temporary created CAs, or even the server-certificate itself. HTTPS connections to server are setup only, if valid and correct certificates are available.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.8.5 SCEP settings

The **SCEP settings** configuration is available for templates and clients (SIP or HFA).

To navigate to this area, expand the **Security** menu, then select **SCEP settings**.

SCEP (Simple Certificate Enrollment Protocol) is a certificate deployment protocol that allows automatic provisioning and renewal of certificates.

If you have selected to configure the SCEP settings of a **client (SIP or HFA)** or a **template**, the following settings are available:

- **SCEP Server Address**

  IP address of SCEP server.
- **Server URL**

  URL of SCEP server.
- **SCEP Server Port**

  Port of SCEP server.
- **SCEP Server Secret**

  SCEP server secret.
- **SHA1 fingerprint**

  SHA1 fingerprint of SCEP.
- **Certificate Expiry Days**

  Number of days before certificate expiry. Possible values:

  - 0 days
  - 10 days
  - 20 days
  - 30 days
- **Certificate Country (IC)**

  Country of residence.
- **Certificate State (ST)**

  Province of residence.
- **Certificate City (L)**

  City of residence.
- **Certificate Organization (O)**

  Name of the organization.
- **Certificate Common Name (CN)**

  Common name.
- **Certificate Signature Algorithm**

  SHA256 or SHA512
- **Certificate Key Length**

  1024 bit or 2048 bit or 4096 bit
- **Certificate Type**

  Type of certificate (interface) that should be deployed.

  - None
  - DLS client
  - HTTPS client
  - SIP client
  - 802.1x client
  - DMS client
  - ACS client
  - LDAP client
  - Wlan range 1 to 20 client

- **Action**

  Type of action that should be performed:

  – **None**
  – **Enroll**
  – **Renew**
  – **Delete**
  – **Cancel pending**
  – **Assign existing certificate**
- **Certificate Status**

  Status of SCEP certificate.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.8.6 OCSP settings

The **OCSP settings** configuration is available for templates and clients (SIP or HFA).

To navigate to this area, expand the **Security** menu, then select **OCSP settings**.

If you have selected to configure the OCSP settings of a **client (SIP or HFA)** or a **template**, the following settings are available:

- **OCSP check enabled** - the Online Certificate Status Protocol can be enabled.

  This can be set to: **True** or **False** (default).
- **OCSP server address 1** - the server address that checks the status of the OCSP.
- **OCSP server address 2** - the second server address that checks the status of the OCSP.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.8.7 Password

The **Password** security configuration is available for templates, users and clients (SIP or HFA).

To navigate to this area, expand the **Security** menu, then select **Password**.

If you have selected to configure the password settings of a **client**, a **user** or a **template**, the following settings are available:

- **New user password**

- **New admin password**

  To add password for a user or an admin, click the ✎ icon.

  A pop-up window opens prompting you to:

  – Enter the a password you want to set in the **New password** field.
  – Re-enter the new password in the **Confirm new password** field.

  Click **OK** to set the password.
- **Password maximum tries** - the number of login attempts allowed before access is suspended.

  This can be set to one of the following values: 0, 2, 3, 4, 5.
- **Password expires after (days)** - the validity period of a password, in days.
- **Password expires warn before (days)** - the number of days after which the user is alerted about password expiration.
- **Password suspension time (mins)** - the number of minutes for password suspension.
- **Password change blocked for (hours)** - the number of hours for the password change to be blocked.
- **Password history valid for (days)** - the time interval during which a password may not be selected again as a new password by the phone, as it remains in the password history for this time.
- **Force password change**

  This can be set to: **True** (default) or **False**.
- **User password expiry date** - the time and date when the user's password expires.

  This field is read-only and by default is set to **Never**.
- **User password status**

  This can be set to one of the following values: **Active**, **Suspended** or **Disabled**.
- **User password minimum length** - the minimum number of characters required for user's password.
- **User password history** - the time interval in which a user password may not be selected again as a new password by the phone, as it remains in the password history for this time.
- **Admin password expiry date** - the time and date when the admin password expires.

  This field is read-only and by default is set to **Never**.
- **Admin password status**

  This can be set to one of the following values: **Active**, **Suspended** or **Disabled**.
- **Admin password minimum length** - the minimum number of characters required for admin password.
- **Admin password history** - the time interval in which an admin password may not be selected again as a new password by the phone, as it remains in the password history for this time.
- **Password minimum uppercase characters** - the minimum number of capital letters that a password must contain.
- **Password minimum lowercase characters** - the minimum number of lower case letters that a password must contain.

- **Password minimum digits** - the number of digits the password must contain.
- **Password minimum special characters** - the number of special characters (`-=[];'#\,./!"£$%^&*()_+{}:@~|<>?) the password must contain.
- **Password maximum characters in sequence** - the number of maximum sequence characters the password must contain.
- **Password minimum difference between passwords** - the number of minimum differences between passwords.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.9 Diagnostics

This chapter provides instructions for the configuration options available in the **Diagnostics** menu.

7.9.1 General

The **General** diagnostics configuration is available for clients and templates.

To navigate to this area, expand the **Diagnostics** menu, then select **General**.

If you have selected to configure the general diagnostics settings of a **client** or a **template**, the following settings are available:

- **Trace file size** - the maximum size allowed for a trace file.
- **Trace Timeout (min)** - the number of minutes after which a timeout for tracing is activated.
- **Clear trace file** - this option specifies whether the trace memory should be emptied before a new trace is executed.

  This can be set to: **True** or **False** (default).
- **Core files enabled** - this option specifies whether the core files are enabled.

  This can be set to: **True** (default) or **False**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.9.2 Trace level

The **Trace level** diagnostics configuration is available for clients and templates.

To navigate to this area, expand the **Diagnostics** menu, then select **Trace level**.

If you have selected to configure the trace levels settings of a **template**, the following settings are available:

- **Admin**

  This can be set to one of the following options: **Off**, **Fatal**, **Error**, **Warning**, **Trace**, **Debug**.
- **Call log**
- **Call view**

- **Phonebook**
- **Help**
- **Application Menu**
- **Certificate Management Service**
- **Communications Service**
- **Component Registrar**
- **CSTA Service**
- **Data Access Service**
- **Digit Analysis Service**
- **Digital Data Service**
- **Directory Service**
- **DLS Client Management Service**
- **Health Service**
- **Instrumentation Service**
- **Journal Service**
- **Media Control Service**
- **Media Processing Service**
- **Mobility Service**
- **OBEX Service**
- **Opera Client Management Service**
- **PotService**
- **Password Management Service**
- **Physical Interface Service**
- **Sidecar Service**
- **Team Service**
- **Tone Generation Service**
- **Transport Service**
- **Voice Engine**
- **Web Server Service**
- **SIP Signalling**
- **SIP Call Control**
- **SIP Messages**
- **Application Framework**
- **Desktop**
- **AGP Phonelet**
- **Service Framework**
- **Service Registry**
- **Bluetooth Service**
- **HFAServiceAgent**
- **VCARD Parser**
- **Voice Mail**
- **Backup Service**
- **Dot1x Service**
- **VoiceRecognitionPhonelet**
- **H.323 Messages**
- **H.235 Security**
- **trace-level-49**
- **Clock Service**
- **LDAP Service**
- **Security Log Service**

- **Media Recording Service**
- **HTTP Service**
- **Video Service**
- **M5T Stack**
- **Ansible Service**
- **UC Service**
- **Exchange Service**
- **Broadsoft Service**
- **WSI Service**
- **ConversationAPI**
- **GPALAudio Core**
- **GPALAudio Framework**
- **trace-level-65**
- **SWYX Service**

For each of the trace levels listed above, you can set one of the following values: **Off**, **Fatal**, **Error**, **Warning**, **Trace**, **Debug**.

If you have selected to configure the trace levels settings of a **client (SIP or HFA)**, only the following setting is available:

- **Admin**

  This can be set to one of the following options: **Off**, **Fatal**, **Error**, **Warning**, **Trace**, **Debug**.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.9.3 Remote trace

The **Remote trace** diagnostics configuration is available for clients and templates.

To navigate to this area, expand the **Diagnostics** menu, then select **Remote trace**.

If you have selected to configure the remote trace settings of a **template** or a **client (SIP or HFA)**, the following settings are available:

- **Remote trace enabled**

  This can be set to: **True** (default) or **False**.

  If the remote trace is set to **True**, the phones sends its trace data directly to the destination entered in the **Remote trace server address**.
- **Remote Trace Server Address** - the IP address or hostname of the server to which the trace data are sent.
- **Remote trace server port** - the port number at which the server receives the trace data.
- **Remote trace user notification enabled**

  This can be set to: **True** (default) or **False**.

  If set to **True**, the phone user will be notified when a trace is performed on the phone.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.9.4 SSH

The **SSH** diagnostics configuration is available for clients and templates.

To navigate to this area, expand the **Diagnostics** menu, then select **SSH**.

SSH configuration for a client (HFA or SIP)

If you have selected to configure the SSH settings of a **client (SIP or HFA)**, the following settings are available:

- **Enable SSH via WBM allowed**

  This can be set to: **True** (default) or **False**.
- **SSH access for admin user enabled**

  This can be set to: **True**or **False** (default).

  If set to **True**, the client can be accessed through SSH.
- **SSH session password** - the password of the SSH session.
- **SSH session connect timer** - the timer used to monitor the duration of an SSH session.

  This can be set to one of the following values: 1 min, 2 min, 3 min (default), 4 min, 5 min, 6 min, 7 min, 8 min, 9 min, 10 min.
- **SSH session lifetime** - the timer used to monitor the lifetime of an SSH session.

  This can be set to one of the following values: 5 min, 10 min, 20 min, 30 min, 60 min.
- **Remote SSH enabled**

  This can be set to: **True** or **False** (default).

  If set to **True**, you can enable a remote SSH.
- **Remote SSH server address** - the IP address or hostname of the server of the remote SSH session.
- **Remote SSH server port** - the number of the port at which the server receives the SSH session.
- **Remote SSH username** - the username of the remote SSH session.
- **Remote SSH HPT forwarding enabled**

  This can be set to: **True** or **False** (default).

  If set to **True**, you can forward a remote SSH.
- **Remote SSH WBM forwarding enabled**

  This can be set to: **True** or **False** (default).

  If set to **True**, you can forward a remote SSH via WBM.
- **Remote SSH known hosts** - the known hosts of the remote SSH session.
- **Remote SSH public key**

  This field is the read-only field and it contains the SSH remote public key.

SSH configuration for a template

If you have selected to configure the SSH settings of a **template**, the same settings as described for clients are available, except the **Remote SSH public key** option.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.9.5 Security logging

The **Security logging** diagnostics configuration is available for clients and templates.

To navigate to this area, expand the **Diagnostics** menu, then select **Security logging**.

Security logging configuration for a client (HFA or SIP)

If you have selected to configure the security logging settings of a **client (SIP or HFA)**, the following settings are available:

- **Archive at percentage level**

  This can be set to one of the following options: 10%, 20%, 30%, 35%, 40%, 45%, 50% (default), 55%, 60%, 65%, 70%, 80%, 90%.
- **Automatic archiving enabled**

  This can be set to: **True** or **False** (default).

  If set to **True**, you can enable automatic archiving.
- **Security log file maximum lines** - the number of the lines available in the security log. By default, this is set to 500.
- **Last archived** - the date and time it was last archived.

  This field is read-only.

Security logging configuration for a template

If you have selected to configure the security logging settings of a **template**, the following settings are available:

- **Archive at percentage level**

  This can be set to one of the following options: 10%, 20%, 30%, 35%, 40%, 45%, 50% (default), 55%, 60%, 65%, 70%, 80%, 90%.
- **Automatic archiving enabled**

  This can be set to: **True** or **False** (default).

  If set to **True**, you can enable automatic archiving.
- **Security log file maximum lines** - the number of the lines available in the security log. By default, this is set to 500.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.9.6 SNMP

The **SNMP** diagnostics configuration is available for clients (SIP or HFA) and templates.

To navigate to this area, expand the **Diagnostics** menu, then select **SNMP**.

If you have selected to configure the SNMP settings of a **template** or a **client (SIP or HFA)**, the following settings are available:

- **SNMP trap sending enabled**

  This can be set to: **True** (default) or **False**.

  If set to **True**, messages are sent to clients in the event of errors.
- **SNMP trap address** - the IP address of the SNMP Manager.

  This can be set to: **True** or **False**(default).
- **SNMP trap port** - the port number for the server that collects the data of the SNMP trap port.
- **SNMP trap password** - the password fields for the SNMP trap

  Click the ✎ icon to enter a password for the SNMP trap.

  A pop-up window opens prompting you to:

  – Enter the a password you want to set in the **New password** field.
  – Re-enter the new password in the **Confirm new password** field.

  Click **OK** to set the password.
- **SNMP queries enabled** - authorization to query data via SNMP.

  This can be set to: **True** or **False**(default).
- **SNMP queries password** - same as SNMP trap password.
- **Diagnostic trap sending enabled**

  This can be set to: **True** (default) or **False**.

  If set to **True**, diagnostic traps are sent.
- **Diagnostic trap to generic address enabled**

  This can be set to: **True** (default) or **False**.

  If set to **True**, diagnostic traps are sent to the trap server configured.
- **Diagnostic trap address** - the host name or IP address of the SNMP server that receives diagnostic traps.
- **Diagnostic trap port** - the port used by the SNMP server to receive diagnostic traps.
- **Diagnostic trap password** - same as SNMP trap password.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

7.9.7 QoS data collection

The **QoS data collection** diagnostics configuration is available for clients (SIP or HFA) and templates.

To navigate to this area, expand the **Diagnostics** menu, then select **QoS data collection**.

If you have selected to configure the QoS data collection settings of a **template** or a **client (SIP or HFA)**, the following settings are available:

- **QoS trap sending enabled**

  This can be set to: **True** (default) or **False**.

  If set to **True**, messages are sent to clients in the event of errors.
- **QoS trap to generic address enabled** - the IP address for the QoS trap.

  This can be set to: **True** or **False** (default).

- **QoS trap address** - the IP address for the QoS trap.
- **QoS trap port** - theport number for the server that collects the data of the QoS.
- **QoS trap password** - the password for the QoS trap.

  Click the ✎ icon to enter a password for the QoS trap.

  A pop-up window opens prompting you to:

  - Enter the a password you want to set in the **New password** field.
  - Re-enter the new password in the **Confirm new password** field.

  Click **OK** to set the password.
- **QoS report mode** - this option specifies when a report should be generated.

  This can be set to one of the following values:

  - **Off** - no report mode.
  - **Threshold exceeded (EOS)** - at the end of the connection that exceeded the threshold.
  - **Threshold exceeded (EOR)** - at the end of the reporting interval that exceeded the threshold.
  - **End of Session (EOS)** - at the end of the connection.
  - **End or Report Interval (EOR)** - at the end of the reporting interval.
- **QoS report interval (seconds)**- the time interval in which a QoS report is sent.
- **QoS session length (100 ms steps)** - a QoS report is sent if a session (e.g. a call) undershoots this minimum interval.
- **QoS observation interval (seconds)** - the time interval in which threshold violation is checked.

  This is a read-only field and the default value is 10 seconds.
- **QoS maximum jitter (ms)** - the maximum threshold in milliseconds for runtime fluctuations during data transmission.

  The default value is set to 20.
- **QoS average round trip delay (ms)** - the average response time in milliseconds for signal transmission. A report is issued if this is exceeded.

  The default value is set to 100.
- **Lost packets threshold compressing codecs** - the maximum number of total packets lost during uncompressed transmission. The number is specified in 1000-packet increments.

  The default value is set to 10.
- **Consecutive lost packets compressing codecs** - the maximum number of consecutive packets lost during uncompressed transmission.

  The default value is set to 2.
- **Consecutive good packets compressing codecs** - the minimum number of consecutive inbound packets lost during compressed transmission.

  The default value is set to 8.
- **Lost packets threshold non-compressing codecs** - the maximum number of consecutive packets lost during uncompressed transmission.

  The default value is set to 10.

- **Consecutive lost packets non-compressing codecs** - the maximum number of consecutive packets lost during uncompressed transmission.

  The default value is set to 2.
- **Consecutive good packets non-compressing codecs** - the minimum number of consecutive inbound packets lost during uncompressed transmission.

  The default value is set to 8.

After configuring all necessary options, click **Submit** in the top right of the configuration window.

8 Groups

As an administrator, you can view and manage the details of your groups account at any time from the **Groups** tab.

You can refresh the list of groups at any time by clicking ⟳ at the top right of the screen.

You can customize the view of the groups list by clicking ▥ at the top right of the **Groups** tab.

The following actions are possible:

- Switch the sliders to **ON** (green) or **OFF** (black) to show or hide columns.
- Click ▾ or ▴ to change the order of the columns.

  When finished, click **Ok** to save your changes

The **Groups** tab displays the following information:

- **Name**

  Represents the name of the group.
- **Description**

  The description of the group.
- **Members**

  Number of members in the group.
- **Templates**

  Templates of configuration used for the clients. Templates on page 35.
- **Active filters**

  Indicates the filters used to group members, these are highlighted in green color and contains IP addresses and Server addresses.

8.1 Creating a new group

As an administrator, you can create and manage groups at any time.

Step by Step

1) Click 👥 **Group** on the top left menu.
2) You are navigated to the **Groups** area and you can view and manage the groups.
3) Click on **+New**,
4) Add the information regarding the new group.

5) In the **Group details** section you can add the following details:
   - Add a name of the group.
   - Add a description of the newly added group.
   - From the **Templates** drop-down list, select the template for the group.

     For more information about the templates, see Templates on page 35.
   - In the **Filters** section you can dynamically search for clients to be added within the group by filtering by:
   - **E164 number** field, enter the number you want to assign to the group.
   - **IP address** add the Ip address of the client you want to add to the group.
   - **Client type** add the type of client that you want to include in the group.
   - **Server address** add the server address of the client you want to include in the group.

     Based on the search, the field **Clients that belong to the current filter** will provide the number of clients found.

6) Click **Submit** to register the new group.

A confirmation message will be displayed and the new group will be visible in the groups list.

8.2 Sorting the groups list

You can sort the groups list in an ascending or descending order.

The groups can be sorted using the **Name** column.

The active sort order is indicated by:

- A dark arrow pointing up (▲), when the column is sorted in an ascending order.
- A dark arrow pointing down (▼), when the column is sorted in a descending order.

You can change the sort order by clicking on the desired arrow.

8.3 Editing group details

As an administrator, you can edit group details at any time.

Step by Step

1) Click 👥 **Group** on the left menu.
2) Locate the group you want to edit and click ⋮ to the right,
3) Click **Edit** to edit the configuration of the group
   A window with the group details is displayed.

4) In the **Group details** section you can add the following details:

- Add a name of the group.
- Add a description of the newly added group.
- From the **Templates** drop-down list, select the template for the group.

  For more information about the templates, see Templates on page 35.
- In the **Filters** section you can dynamically search for clients to be added within the group by filtering by:
- **E164 number** field, enter the number you want to assign to the group.
- **IP address** add the IP address of the client you want to add to the group.
- **Client type** add the type of client that you want to include in the group.
- **Server address** add the server address of the client you want to include in the group.

  Based on the search, the field **Clients that belong to the current filter** will provide the number of clients found.

5) Click **Submit** to register the new group.

A confirmation message will be displayed and the new group will be visible in the groups list.

8.4 Deleting a group

You can easily delete a group.

Step by Step

1) Select **Groups** from the left menu.
A list of existing groups is displayed.

2) Scroll through the list of groups to locate one or more groups that you want to delete.

3) Tick the check box next to one or more groups, then click **Delete** at the top right of the screen.

Alternatively, you can delete a group at a time by clicking ⋮ at the right of the group, then selecting **Delete** from the drop-down menu.

4) Click **Confirm** to proceed with the deletion.

Deleted groups are no longer available in the list of groups.

9 Files

You can easily view a list of existing files, upload new ones or delete files that are not needed anymore from the **Files** tab. You can also filter and sort the files list to locate specific files easier.

You can refresh the list of files at any time by clicking ↻ at the top right of the screen.

You can customize the view of the files list by clicking ▥ at the top right of the **Files** tab.

The following actions are possible:

- Switch the sliders to **ON** (green) or **OFF** (black) to show or hide columns.
- Click ▾ or ▴ to change the order of the columns.

  When finished, click **Ok** to save you changes.

The **Files** tab displays the following information about files:

- **Filename** - the name of the file.
- **Storage** - the type of storage.
- **Type** - the file type.
- **Size** - the size of the file.
- **Supported clients** - the clients that the file is available for.
- **Software version** - the software version of the file.

The following file types are supported:

- **Software**: files that contain firmware for clients.
- **Ringtone**: files that can be set as ringtone for clients.
- **Screensaver**: image file for screensavers.
- **Logo**: image file for logos on clients.
- **LDAP template**: LDAP template files.
- **Dongle**: file containing Dongle Keys.
- **Music on hold**: audio files.
- **Picture**: picture files.

9.1 Filtering the files list

If the files list is long, you can filter it to quickly find the one you are looking for.

Step by Step

1) Select 🗎**Files** from the left menu.

   A list of existing files is displayed (if any).
2) Click **Filter** in the top right of the screen and enter one or more filer terms:
   - Enter a file name or storage type in the input field.
   - From the **Software type** drop-down list, select the software type you want to filter by.
   - From the **File type** drop-down list, select the file type you want to filter by.
3) Click **Apply**.

The files that match the filtering you have applied are displayed (if any).

Next steps

To cancel the current filer, click **Reset** above the **Filename** column.

9.2 Sorting the files list

You can sort the files list in an ascending or descending order.

Columns that can be sorted contain the sort indicator (▲ ▼) in the column header.

The active sort order is indicated by:

- A dark arrow pointing up (▲), when the column is sorted in an ascending order.
- A dark arrow pointing down (▼), when the column is sorted in a descending order.

You can change the sort order by clicking on the desired arrow.

9.3 Uploading a file

You can easily upload a new file to your OpenScape Endpoint Management app.

NOTICE: You can only upload a file at a time.

Step by Step

1) Select **Files** from the left menu.

   A list of existing files is displayed (if any).
2) Click **Upload** in the top right of the screen.
   The **Upload a file** window appears.
3) Click **Browse** and select the file you want to upload.

   You can only select one file at a time.

   The following details of the selected file are displayed: file name and file size.
4) Click **Submit**.

Upon successful upload, the new file is displayed in the files list.

9.4 Deleting a file

You can easily delete one or more files that are not needed anymore.

Step by Step

1) Select **Files** from the left menu.

   A list of existing files is displayed (if any).

2) Scroll through the list of files to locate one or more files that you want to delete.

> **NOTICE:** If the files list is too long, you can filter or sort it to quickly find the file/s you are looking for.
>
> For more information, see Filtering the files list on page 118 and Sorting the files list on page 119.

3) Tick the check box next to one or more files, then click **Delete** at the top right of the screen.

   Alternatively, you can delete a file at a time by clicking ⋮ at the right of the file, then selecting **Delete** from the drop-down menu.

4) Click **Confirm** to proceed with the deletion.

Deleted files are no longer available in the files list.

Next steps

If you want to make available again a file you have deleted previously, you must upload it again. For more information, see Uploading a file on page 119.

9.5 Downloading a file

You can easily download a file from your OpenScape Endpoint Management app.

> **NOTICE:** You can only download a file at a time.

Step by Step

1) Select **Files** from the left menu.

   A list of existing files is displayed (if any).

2) Scroll through the list of files to locate the file you want to download.

> **NOTICE:** If the files list is too long, you can filter or sort it to quickly find the file you are looking for.
>
> For more information, see Filtering the files list on page 118 and Sorting the files list on page 119.

3) Click ⋮ at the right of the file, then select **Download** from the drop-down menu.

The file is downloaded to the default download folder of your computer.

10 Storage provider

You can view or edit existing storage providers, add new ones or delete the ones that are not needed anymore from the **Storage provider** tab. You can also filter or scan the storage providers list to find specific providers easier.

You can refresh the list of storage providers at any time by clicking ↻ at the top right of the screen.

You can customize the view of the storage provider list by clicking ▥ at the top right of the **Storage provider** tab.

The following actions are possible:

- Switch the sliders to **ON** (green) or **OFF** (black) to show or hide columns.
- Click ▾ or ▴ to change the order of the columns.

  When finished, click **Ok** to save you changes

The **Storage provider** tab displays the following information about a provider:

- **Name** - the name of the storage provider.
- **Type** - the provider type.
- **Address** - the IP Address of the storage provider.
- **Files** - the file/s available for the storage provider.

The following types of storage providers are supported:

- **S3**
- **HTTPS**

10.1 Filtering the storage providers list

If the storage providers list is long, you can filter it to quickly find the one you are looking for.

Step by Step

1) Select ☁ **Storage provider** from the left menu.
   A list of existing storage providers is displayed (if any).
2) Click **Filter** in the top right of the screen and enter one or more filer terms:
   - Enter a provider name in the input field.
   - From the **Storage type** drop-down list, select the type of storage you want to filter by.
3) Click **Apply**.

The storage providers that match the filtering you have applied are displayed (if any).

Next steps

To cancel the current filer, click ⊗ above the **Name** column.

10.2 Scanning for a storage provider

You can easily scan for storage providers in your OpenScape Endpoint Management administration app, by specifying the subnet mask you want to scan by.

Step by Step

1) Select ☁ **Storage provider** from the left menu.
2) Click **+ Scan** at the top right of the screen.
   The **Scan** window is displayed.
3) From the **Subnet mask** drop-down list, select the subnet mask you want to scan by, then click **Scan**.

   The scan for storage providers is started.

   You can stop the scan at any time by clicking ⊗.

After the scan is completed, you can view the total numbers of objects scanned in the **Active scans** area.

10.3 Adding a storage provider

You can easily add a storage provider to OpenScape Endpoint Management.

Step by Step

1) Select ☁ **Storage provider** from the left menu.
   A list of existing storage providers is displayed (if any).
2) Click **+ New** in the top right corner of the screen.
   The **Add Provider** window appears.

3) Enter the details of the new provider:

- From the **Type** drop-down list select the desired provider type:

  The following options are available:

  - S3
  - HTTPS
- In the **Name** field, enter a custom name for your provider.
- In the **URL** field, enter the URL of your provider.
- In the **Access Key** field, enter access key associated with your provider.
- In the **Access Secret** field, enter access secret associated with your provider.
- In the **Bucket Name** field, enter access secret associated with your provider.
- In the **Region** field, enter the region in which your storage provider is located.
- Switch the **Start Scan of Storage Provider** slider to:

  ON (green), in you want to start scanning the provider.

  OFF (gray), if you don't want to scan the provider.

NOTICE: All fields are mandatory and must be filled in to create a new storage provider.

4) Click **Submit**.
A new storage provider is created.

5) Click **X** at the top of the **Add Provider** window to return to **Storage provider**.

10.4 Editing details of a storage provider

You can easily edit the details of an existing storage provider.

Step by Step

1) Select ☁ **Storage provider** from the left menu.
A list of existing storage providers is displayed (if any).

2) Locate the storage provider you want to edit and click ⋮ to the right, then select **Edit**.

NOTICE: If the list is too long, you can filter it to quickly find the provider you are looking for.

For more information, see Filtering the storage providers list on page 121.

The **Edit Provider** window opens.

3) Edit the details of storage provider:

   - From the **Type** drop-down list one of the available provider types: **S3** or **HTTPS**.
   - In the **Name** field, edit the name for your provider.
   - In the **URL** field, enter the URL of your provider.
   - In the **Username** field, enter username associated with your provider.
   - In the **Password** field, enter password associated with your provider.
   - Switch the **Start Scan of Storage Provider** slider to:

     ON (green), in you want to start scanning the provider.

     OFF (gray), if you don't want to scan the provider.

   NOTICE: All fields are mandatory and must be filled in to edit the details of the storage provider.

4) Click **Submit**.
   The details of your storage provider are updated.
5) Click **X** at the top of the **Edit Provider** window to return to **Storage provider**.

10.5 Deleting a storage provider

You can easily delete a storage provider that is not needed anymore.

Step by Step

1) Select ☁ **Storage provider** from the left menu.
   A list of existing storage providers is displayed (if any).
2) Scroll through the list of storage providers to locate one or more providers that you want to delete.

   NOTICE: If the list is too long, you can filter it to quickly find the provider/s you are looking for.

   For more information, see Filtering the storage providers list on page 121.

3) Tick the check box next to one or more storage providers, then click **Delete** at the top right of the screen.

   Alternatively, you can delete a storage provider at a time by clicking ⋮ at the right of the provider, then selecting **Delete** from the drop-down menu.
4) Click **Confirm** to proceed with the deletion.

Deleted providers are no longer available in the storage providers list.

Next steps

If you want to make available again a storage provider that you have deleted previously, you must add it again. For more information, see Adding a storage provider on page 122.

11 Certificates

You can view a list of certificates available on your OpenScape Endpoint Management administration app in the **Certificates** tab. You can also view the details, download or delete certificates that are not needed anymore.

You can refresh the list of certificates at any time by clicking ↻ at the top right of the screen.

You can customize the view of the certificates list by clicking ▥ at the top right of the **Certificates** tab.

The following actions are possible:

- Switch the sliders to **ON** (green) or **OFF** (black) to show or hide columns.
- Click ▾ or ▴ to change the order of the columns.

  When finished, click **Ok** to save you changes

> **NOTICE:** Currently, specific certificates for OpenScape Endpoint Management can not be changed. All certificates are created upon first installation.

The ▭ **Certificates** tab displays the following information about a certificate:

- **Common Name** - the name of the certificate.
- **Issuer** - the entity who has issues the certificate.
- **Certificate type** - the type of the certificate.
- **Valid until** - the date until the certificate is available.
- **Private key** - the private key of the certificate.
- **Usage** - the purpose of the certificate.

11.1 Creating a certificate

You can easily create certificates on your OpenScape Endpoint Management administration app.

Step by Step

1) Select ▭ **Certificates** from the left menu.
   A list of existing certificates is displayed (if any).

2) Click **+Create** at the top right part of the screen.
   A pop-up window is displayed and you can configure the following fields:

   - **Certificate authority for signing** - select one of the available options from the dropdown list:
     - **Create new certificate authority**,
     - **osem - secure mode CA (old)**,
     - **osem - Internal CA (default)** or
     - **osem - Secure mode CA (current)**
   - **Certificate type** - the following options are available:
     - **Server certificate** or
     - **Client certificate**
   - **Subject** - click ✎ to edit the subject information:
     - **Common name**,
     - **Country**,
     - **Location**,
     - **State or province**,
     - **Organization**,
     - **Organizational unit**.

     Then click **Update** to confirm.
   - **Subject alternative name information** - subject alternative names can be specified as IPv4, IPv6 addresses or DNS names. Use a comma as separator when providing multiple entries. Example: 1.2.3.4,test.local
   - **Certificate lifetime** - select from the dropdown list:
     - **180 days**,
     - **90 days**,
     - **1 year**,
     - **2 years** or
     - **3 years**
   - **Private key** - read-only
   - **RSA key length** - the following options are available:
     - **2048 bit** or
     - **4096 bit**

3) Click **Submit** to create the certificate.

The newly created certificate is visible in the certificates list.

11.2 Uploading a certificate

You can easily upload a certificate to your OpenScape Endpoint Management app.

NOTICE: You can only upload one certificate at a time.

Step by Step

1) Select **Certificate** from the left menu.

   A list of existing certificates is displayed (if any).
2) Click **Upload** at the top right of the app.
   The **Upload certificate** window opens.
3) Click **Choose file** and select the file you want to upload.

   You can only select one file at a time.

   The following details are displayed for the file you have selected: file name and file size.
4) Click **Upload certificate**.

Upon successful upload, the new file is displayed in the files list.

11.3 Downloading a certificate

You can easily view the certificate information on your OpenScape Endpoint Management administration app.

Step by Step

1) Select **Certificates** from the left menu.
   A list of existing certificates is displayed (if any).
2) Click ⋮ on the right of the certificate.
3) Select **Download** from the drop-down menu.

   The file is downloaded to your computer.

11.4 Certificate information

You can easily view the certificate information on your OpenScape Endpoint Management administration app.

Step by Step

1) Select **Certificates** from the left menu.
   A list of existing certificates is displayed (if any).
2) Click ⋮ on the right of the certificate.

3) Select ⓘ
   A pop-up window will be displayed with the following information:
   - **Subject**
   - **Issuer**
   - **Certificate type**
   - **Serial**
   - **Valid until**
   - **Valid from**
   - **Key usage**
   - **Subject alternative name**
4) Click **X** from the top right corner to exit the certificate information window.

11.5 Deleting app certificates

You can easily delete certificates that are not needed anymore on your OpenScape Endpoint Management administration app.

Step by Step

1) Select **Certificates** from the left menu.
   A list of existing certificates is displayed (if any).
2) Scroll through the list of certificates to locate one or more certificates that you want to delete.
3) Tick the check box next to one or more certificates, then click **Delete** at the top right of the screen.

   Alternatively, you can delete a certificate at a time by clicking ⋮ at the right of the certificate, then selecting **Delete** from the drop-down menu.
4) Click **Confirm** to proceed with the deletion.

Deleted certificates are no longer available in the certificates list.

Next steps

If you want to make available again a certificate that you have deleted previously, you must add it again.

12 Jobs

Jobs are created by user actions (configuration, file deployment, etc.).

In this section you can view a list of available jobs and their execution details as well as delete jobs that are not needed anymore from the **Jobs** tab. You can also filter the jobs list to find specific ones easier.

You can refresh the list of jobs at any time by clicking ↻ at the top right of the screen.

You can customize the view of the jobs list by clicking ▥ at the top right of the **Jobs** tab.

The following actions are possible:

- Switch the sliders to **ON** (green) or **OFF** (black) to show or hide columns.
- Click ▾ or ▴ to change the order of the columns.

  When finished, click **Ok** to save you changes

The **Jobs** tab displays the following information about a job:

- **Type** - the job type.
- **State** - the job execution status.
- **Planned execution** - the time planned execution of the job.
- **Execution time** - the duration of the job execution.

12.1 Filtering the jobs list

If the jobs list is long, you can filter it to quickly find the one you are looking for.

Step by Step

1) Select **Jobs** from the left menu.

A list of existing jobs is displayed.

2) Click **Filter** in the top right of the screen and enter one or more filter terms:

- From the **State** drop-down list, select the job state you want to filter by.

  The following states are available for each job: created, active, partial successful, success, timeout, failed.
- And select to filter:
  - All jobs that have been executed **After** a certain date.
  - All jobs that have been executed **Before** a certain date.

3) Click **Apply**.

The jobs that match the filtering you have applied are displayed (if any).

Next steps

To cancel the current filter, click ⊗ above the **Type** column.

12.2 Viewing job details

You can view details of a job's execution and additional information about the job.

Step by Step

1) Select **Jobs** from the left menu.
A list of existing jobs is displayed (if any).

2) Scroll through the list of jobs to locate the one of which you want to see details.

> **NOTICE:** If the list is too long, you can filter it to quickly find the one you are looking for.
>
> For more information, see Filtering the jobs list on page 129.

3) Click ⋮ to the right of the desired job, then select **Details**.

For each job, you can view the following information:

- Details about the job: the initiator, state and execution time of the job.
- Details about the clients and users for which the job was executed: the E164 number of the client, the hardware type associated with the client, the client's MAC address and the job execution state.

12.3 Deleting a job

You can easily delete one or more jobs that are not needed anymore.

Step by Step

1) Select **Jobs** from the left menu.

A list of existing job is displayed.

2) Scroll through the list of jobs to locate one or more files that you want to delete.

> **NOTICE:** If the list is too long, you can filter it to quickly find the job/s you are looking for.
>
> For more information, see Filtering the jobs list on page 129.

3) Tick the check box next to one or more jobs, then click **Delete** at the top right of the screen.

Alternatively, you can delete a job at a time by clicking ⋮ at the right of the job, then selecting **Delete** from the drop-down menu.

4) Click **Confirm** to proceed with the deletion.

Deleted jobs are no longer available in the jobs list.

13 OpenScape Endpoint Management Configuration

You can configure your OpenScape Endpoint Management administration app from the **Configuration** tab.

The **Configuration** tab allows you to configure the following options on your administration app:

- **DCMP** - configure the app for DCMP operation.
- **E-Mail** - set an email address to be used for security alerts.
- **Interfaces**- configure app interfaces.
- **Licensing**- manage app licenses.
- **Mobility** - configure mobility settings.
- **Other** - configure additional settings.
- **Ports** - set communication ports.
- **SNMP** - configure the app for SNMP operation.
- **Secure mode** - enable the secure mode operation.
- **Security** - configure additional settings for secure mode operation.

Next steps

You can use the search functionality to easily locate specific configuration settings. For this, enter the configuration item you are looking for in the search field below **Configuration**. The configuration items that match the search term you have entered will be displayed (if any).

13.1 Configuring DCMP operation

As an administrator, you can configure OpenScape Endpoint Management for DCMP operation.

Step by Step

1) Select ⚙ **Configuration** from the left menu.
2) Click **DCMP**.
3) Configure the DCMP settings:
    - Select one of the DCMP operation modes available: **Automatic** (default), **Disabled**, **Enabled.**
    - Enter the URL of the DCMP server node.
    - Enter the time interval after which OpenScape Endpoint Management sends a query for new jobs.

      You must specify a value in minutes, in the 1 - 1440 range.
    - Indicate whether DCMP server runs in secure mode by selecting **Yes** or **No**.
4) Click **Submit**.

A confirmation message is displayed and the DCMP settings are updated.

13.2 Configuring email settings

You can configure OpenScape Endpoint Management with email functionality and send security alerts when specific events are triggered.

Step by Step

1) Select ⚙ **Configuration** from the left menu.
2) Click **E-Mail**.
3) Configure the email settings:
    - Enter the email server address and server port.
    - Enter the Username and password for SMTP server authentication.
    - Select one of the operation modes available for email security: **TLS**, **STARTTLS**, **Disabled**.
    - Enter the subject of the emails sent by OpenScape Endpoint Management or keep the default one (`OpenScape Endpoint Management`).
    - Enter an email address to be used by OpenScape Endpoint Management to send security alerts over email or keep the default one (`no_reply@mitel.com`).
    - Enable sending security alerts via Email by selecting **Yes** or **No**.
    - Enter the emails addresses of the recipients who should receive security alerts via email.
4) Click **Submit**.

A confirmation message is displayed and the email settings are updated.

13.3 Configuring interface settings

You can configure interface settings for OpenScape Endpoint Management.

Step by Step

1) Select ⚙ **Configuration** from the left menu.
2) Click **Interfaces**.
3) Configure the security settings:
    - Enter the cipher suites used for default mode interface.
    - Enter the cipher suites used for secure mode interface.
    - Enter the cipher suites used for DCMP interface.
    - Enter the cipher suites used for API and UI server interface.
    - Enter the cipher suites used for metrics interface.
    - Select the minimum TLS version for default mode interface.
    - Select the minimum TLS version for secure mode interface.
    - Select the minimum TLS version for DCMP interface.
    - Select the minimum TLS version for API and UI server interface.
    - Select the minimum TLS version for metrics interface.

    The following minimum TLS versions are available: **TLSv1**, **TLSv1.1**, **TLSv1.2**, **TLSv1.3**.

4) Click **Submit**.

A confirmation message is displayed and the security settings are updated.

13.4 Configuring app licenses

OpenScape Endpoint Management requires a license to operate.

You can edit or view the Cloud license key associated with your account and the License Locking ID.

13.5 Configuring mobility settings

You can configure mobility settings for your OpenScape Endpoint Management administration app.

Step by Step

1) Select ⚙ **Configuration** from the left menu.
2) Click **Mobility**.
3) Configure the mobility settings:
    - Enter the time interval (in seconds) after which forced logon activity is triggered.
    - Enter the time interval (in seconds) after which forced logoff activity is triggered.
    - Indicate whether mobility is operated with enhanced security by selecting **True** or **False**.
4) Click **Submit**.

A confirmation message is displayed and the mobility settings are updated.

13.6 Configuring other settings

You can configure additional settings for your OpenScape Endpoint Management administration app.

Step by Step

1) Select ⚙ **Configuration** from the left menu.
2) Click **Other**.

3) Configure the following additional settings:

- Enter the URL of the WPI and API server node.
- Enter the log level for OpenScape Endpoint Management by selecting one of the following: Log, Off, Error, Warn, Info, Debug, All!!! Heavy!!!
- Enter the Time Zone of the OpenScape Endpoint Management server by selecting the appropriate from the list.
- Enter the time interval (in seconds) after which a running job is marked as failed.
- Indicate whether you want to enable an integrated file server by selecting **Yes** or **No**.
- Enter a value (in Kilobytes per seconds) to limit the bandwidth of the integrated file server.
- Enter a limit value (in seconds) to determine how long diagnostic files are kept in the database.

  The value must be in the 7 - 180 days range.
- Enter a value (in days) to limit the lifetime of jobs. Jobs will be deleted after a certain amount of time has passed since their creation.

4) Click **Submit**.

A confirmation message is displayed and the settings are updated.

13.7 Configuring port settings

You can configure the ports that OpenScape Endpoint Management uses for communication.

All ports are default ports and server ports can be changed.

Step by Step

1) Select ⚙ **Configuration** from the left menu.
2) Click **Ports**.
3) Configure the communication ports:

- Enter the default port for communication with clients.
- Enter the secure port for communication with clients using mutual TLS.
- Enter the server port for DCMP communication with clients.
- Enter the server port for communication with the API.
- Enter the server port for communication with the Metrics server.

4) Click **Submit**.

A confirmation message is displayed and the list of ports is updated.

13.8 Configuring SNMP settings

You can configure the OpenScape Endpoint Management app to operate in SNMP mode.

Step by Step

1) Select ⚙ **Configuration** from the left menu.
2) Click **SNMP**.
3) Configure the SNMP settings:
   - Select one of the SNMP versions available: **SNMP v1**, **SNMP v2**, **SNMP v3**.
   - Enter the IP address to be used to send SNMP Traps.
   - Enter the SNMP trap community string.
   - Enter the engine ID of the SNMP Trap.
   - Enter the authentication key of the Hashed SNMP Trap.
   - Enter the private key of the Encrypted SNMP Trap.
   - Select the one of the following hashing protocols for the SNMP Trap: **None**, **MD5**, **SHA**, **SHA-224**, **SHA-256**, **SHA-384**, **SHA-512**.
   - Select one of the following the encryption types for the SNMP Trap: **None**, **DES**, **AES**, **AES-256 Blumenthal**, **AES-256 Reeder**.
4) Click **Submit**.

A confirmation message is displayed and SNMP settings are updated.

13.9 Configuring secure mode operation

You can configure OpenScape Endpoint Management to operate in secure mode.

Step by Step

1) Select ⚙ **Configuration** from the left menu.
2) Click **Secure mode**.
3) Configure the mobility settings:
   - Enter the PIN to be used for secure mode operation.

     You must provide a value in digits. Only values between 8 - 32 digits are possible.
   - Enter the length of the PIN for secure mode operation with individual PIN.

     Only values between 8 - 32 digits are possible.
   - Enter the default lifetime of a certificate used for secure mode.

     You must provide a value in seconds. Only values between 1 hour and 3 years are possible.
   - Enter the default renewal time of a certificate used for secure mode.

     You must provide a value in seconds. Only values between 1 day and 30 days are possible.
   - Select one of the options available for the default key length of the RSA private key used for secure mode: **1024**, **2048**, **4096**.
   - Select one of the options available for the default curve of the ECDSA private key used for secure mode: **NIST P-256**, **NIST P-348**, **NIST P-521**.
4) Click **Submit**.

A confirmation message is displayed and the settings for secure mode are updated.

13.10 Configuring security settings

You can configure security settings for OpenScape Endpoint Management.

Step by Step

1) Select ⚙ **Configuration** from the left menu.
2) Click **Security**.
3) Configure the security settings:
   - Select the digest-algorithm used to create session and refresh token: HMAC SHA-256, HMAC SHA-512, RSASSA-PKCS1-v1_5 SHA-256, RSASSA-PKCS1-v1_5 SHA-512, ECDSA P-256 and SHA-256 and ECDSA P-256 and SHA-512.
   - Select the time-based one-time password (TOTP) hash algorithm: SHA-1, SHA-256.
   - Select to run Metrics server via TLS by selecting **No** or **Yes**.
   - Select PKCS12 container file hash algorithm: SHA-1, SHA-256, SHA-512.
   - Select PKCS12 container file encryption algorithm: AES-128-CBC, AES-192-CBC, AES-256-CBC

     NOTICE: PKCS12 files that are being uploaded into OpenScape Endpoint Management app directly have to be encoded with AES - 256 - CBC

     encryption algorithm.

   - Select to validate if the storage provider connection is secure by selecting **No** or **Yes**.
4) Click **Submit**.

A confirmation message is displayed and the security settings are updated.

mitel.com