A MITEL
PRODUCT
GUIDE

Unify OpenScape Endpoint Management

OpenScape Endpoint Management V1 R2

Administrator Documentation
12/2025

A31003-S2312-M100-01-76A9

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/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 administering clients, users and groups as well as using 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 in 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 Concept and features

2.1 Supported clients

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

- Desk Phone Familiy (CP710, CP700, CP700X, CP600, CP600E, CP410, CP400, CP210, CP205, CP200, CP110, CP100, IP55G, IP35G, IP 35G Eco)
- OpenStage Family (OS80, OS60, OS40, OS20E, OS20, OS15)
- Mitel 69XX Family (6905, 6910, 6915, 6920, 6930, 6940, 6970)
- Mitel 68XX Familiy (6863i, 6865i, 6867i, 6869i, 6873i)
- OpenScape Personal Edition
- OpenScape Fusion
- Mediatrix Analog adapter (MX 3631, MX 3632, MX 4102, MX 4104, MX 4108, MX 4116, MX 4124, MX 4401, MX 4402, MX 4404, MX C710, MX C711, MX C731, MX G7, MX S716, MX S724)
- HG3500

2.2 Deployment scenarios

The following deployments are possible for OpenScape Endpoint Management:

- **Standalone and Cluster deployment based on OSEM Container Appliance**

  OpenScape Endpoint Management Appliance is installed in a "one-click" solution on either a Hypervisor System or Barbone Server. For further information on how to install, please see OSEM Container Appliance Installation
- Integrated OpenScape 4000

  In the case of this deployment, OpenScape Endpoint Management is part of the OpenScape 4000 installation.

2.3 License information

You can view the license status and additional license information on the Dashboard.
The OpenScape Endpoint Management administration app supports CloudCLA and it must be licensed for the 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 the Features "Mobile Users" and "Connectors", you will need to buy licenses based on the amount that meets the needs for your deployment scenario.

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

In the **License** section of the Dashnoard, you can view the following details:

- whether the license is in a grace period
- the validity of the license
- the remaining days until expiration
- the number of licenses used
- the number of licenses available

3 OpenScape Endpoint Management Container Appliance Installation

This section provides information on installing the **OSEM Container Appliance**, based on **OpenSUSE MicroOS**. The process is the same for both standalone OSEM installation and the cluster installation.

Requirements

> **NOTICE:** This admin guide covers the basic requirements at the time of writing this guide. For an up-to-date list of resources, please always check the Virtual Machine Resourcing and Configuration Guide and the OSEM release notes for the version you plan to install.

The minimum hardware requirements for each server running OSEM Container Appliance (including OSEM application)

Type	CPU (min / rec)	RAM (min / rec)	HDD (min / rec)
Standalone	1 core / 2 cores	4 GB / 8 GB	30 GB / 100 GB
Cluster*	2 cores / 4 cores	8 GB / 16 GB	50 GB / 800 GB

*for each of the nodes in the 3 Node cluster

In terms of hard disk capacity for a cluster installation. During cluster installation, the actual size reserved for OSEM is calculated based on the available free storage. Below is an example of storage reserved with different total HDD capacities

Free HDD space	Database	Backup	Files	Others
50 GB	20 GB	5 GB	5 GB	5 GB
250 GB	150 GB	35 GB	35 GB	15 GB
500 GB	300 GB	70 GB	70 GB	30 GB
800 GB	500 GB	100 GB	100 GB	30 GB

Depending on the size of your managed clients, choose the minimum hardware requirements when managing up to 500 clients. Choose the recommended hardware requirements when managing more than 500 clients.

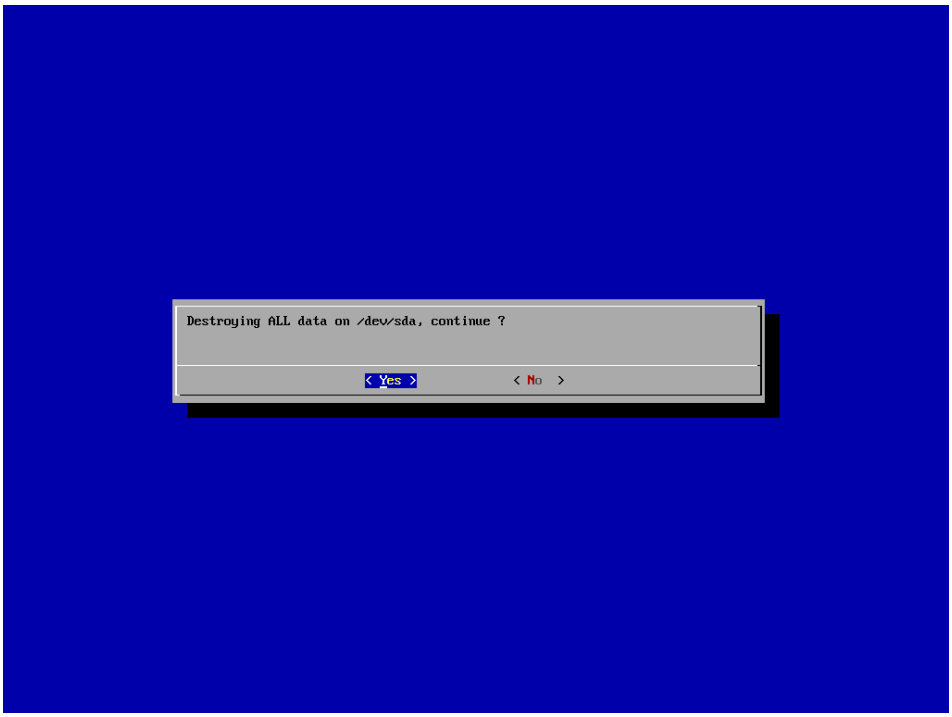
When one of the following applies, we recommend choosing the cluster setup with the same hardware requirement rules from above:

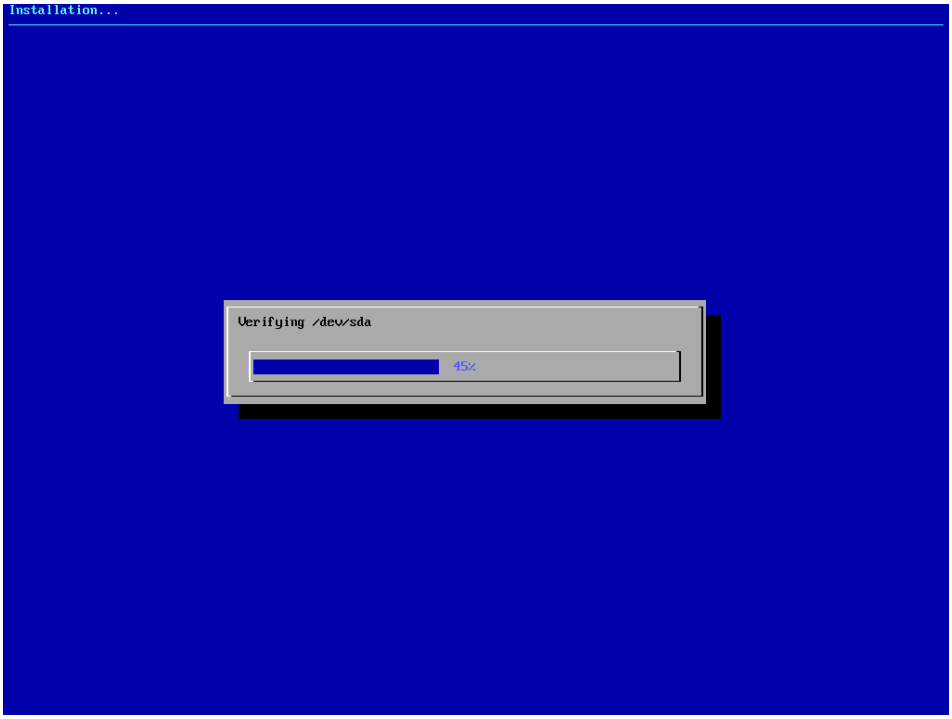
- Redundancy / Failover is a required functionality.
- You are managing more than 10000 mobile users
- You are managing more than 50000 clients

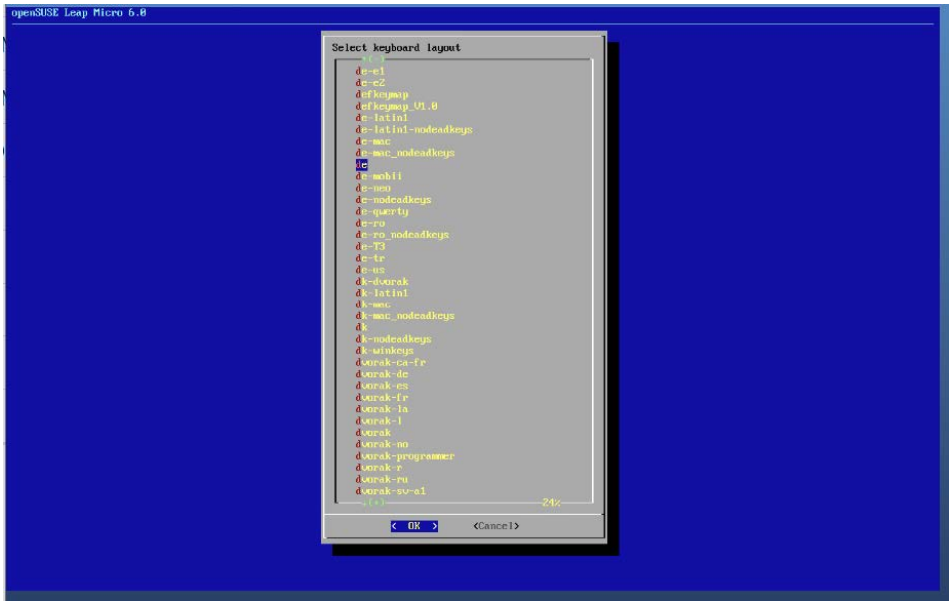
3.1 Initial Appliance installation

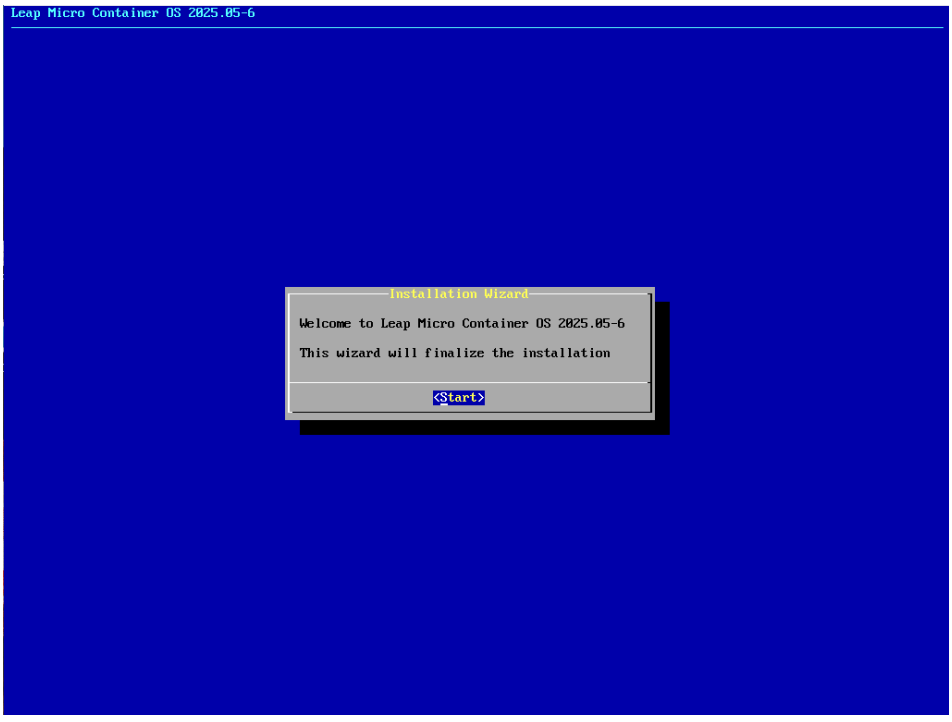
You need to either mount the ISO file in your virtual environment or write it to a USB device for installation on bare-metal hardware using Rufus.

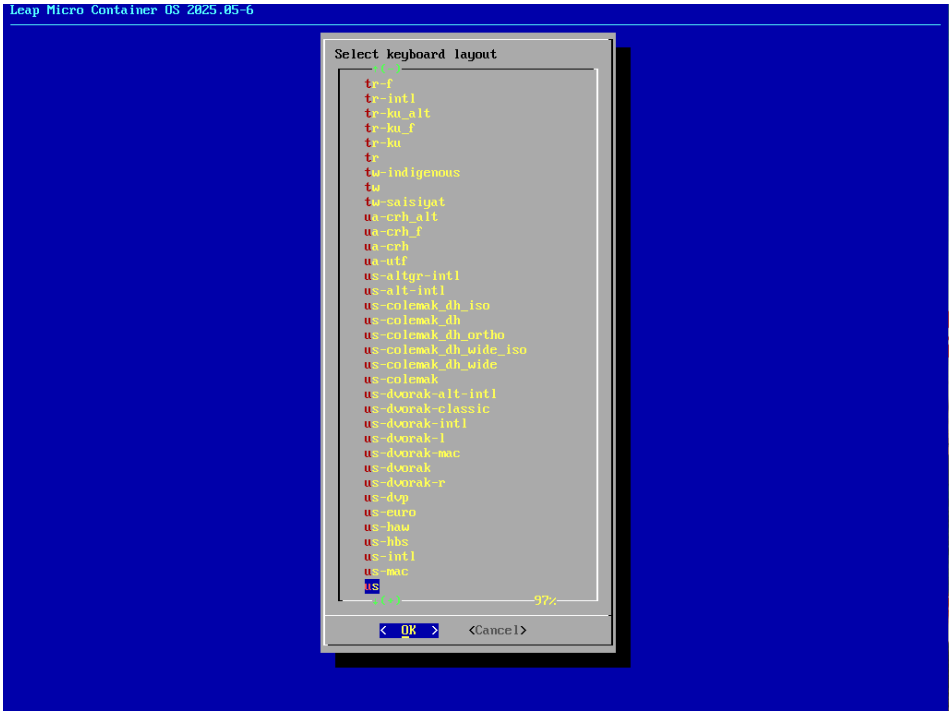
When configuring a fixed IP address for the network interface, make sure you set IPv4 Configuration mode to “manual” (not “automatic”)

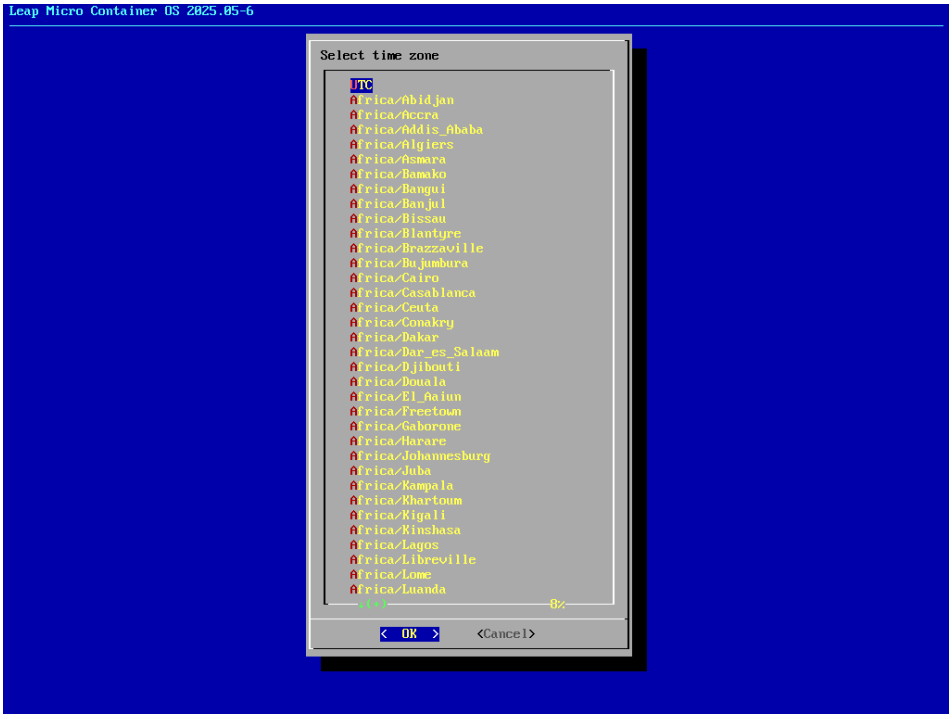


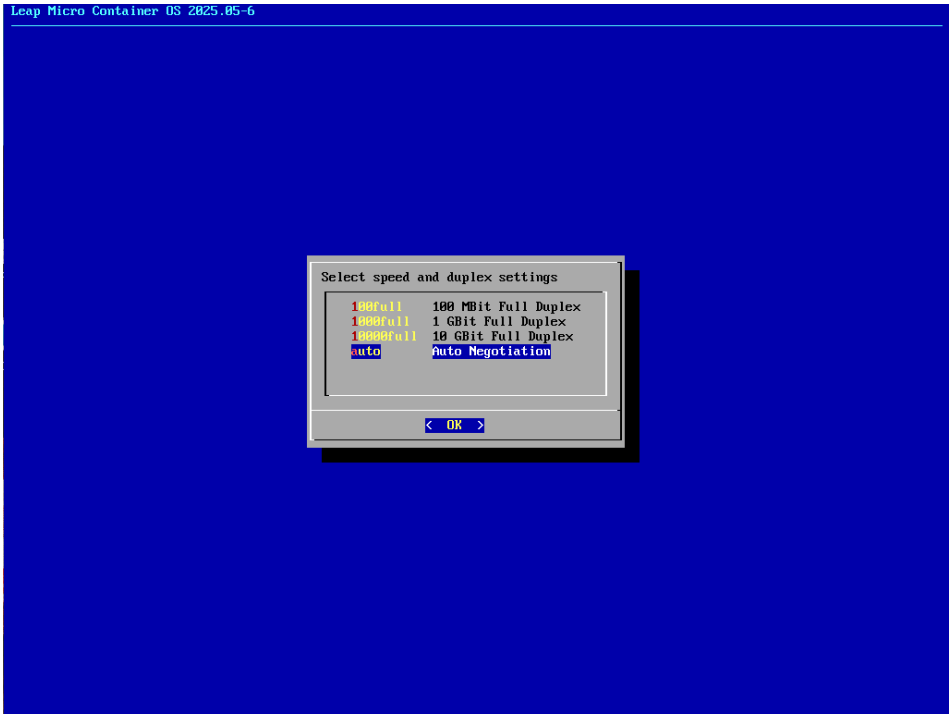


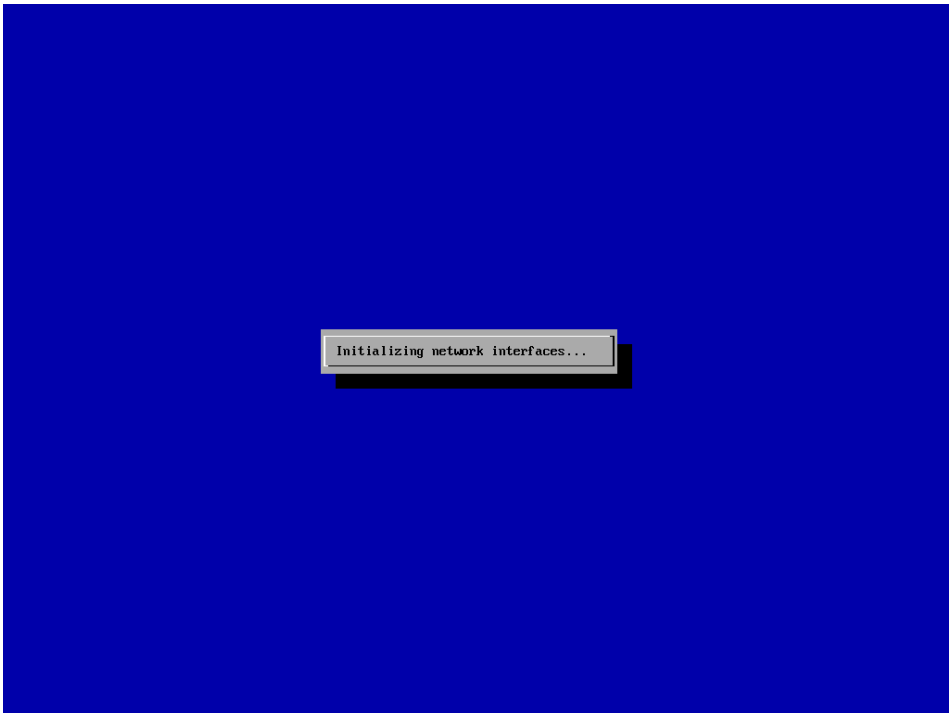

openSUSE Leap Micro 6.0
Select keyboard layout
< OK >
<Cancel>

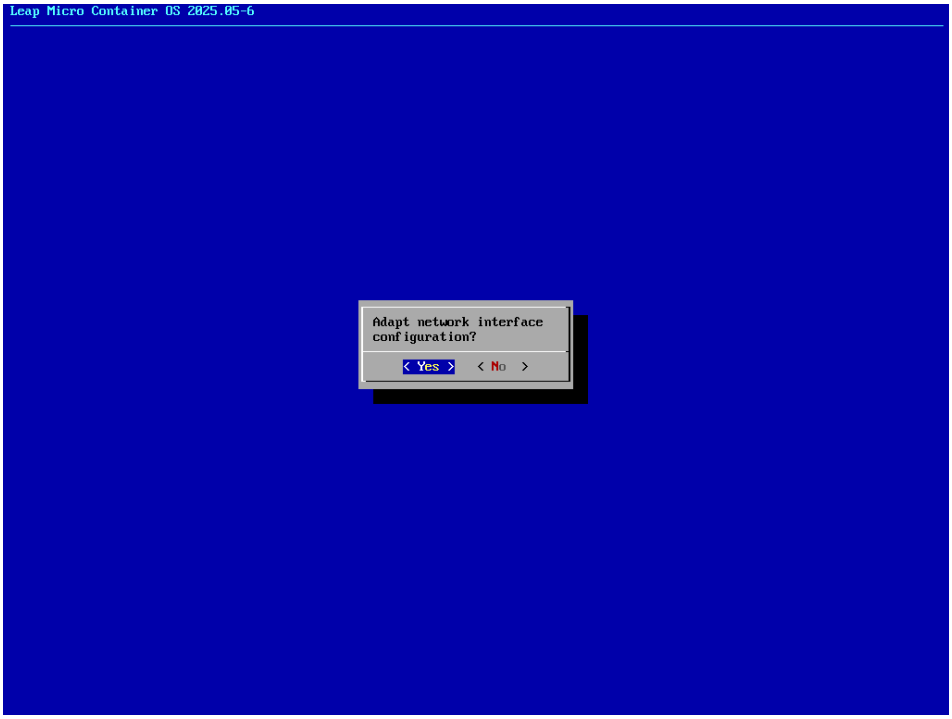

Leap Micro Container OS 2025.05-6
Installation Wizard
Welcome to Leap Micro Container OS 2025.05-6
This wizard will finalize the installation
<Start>

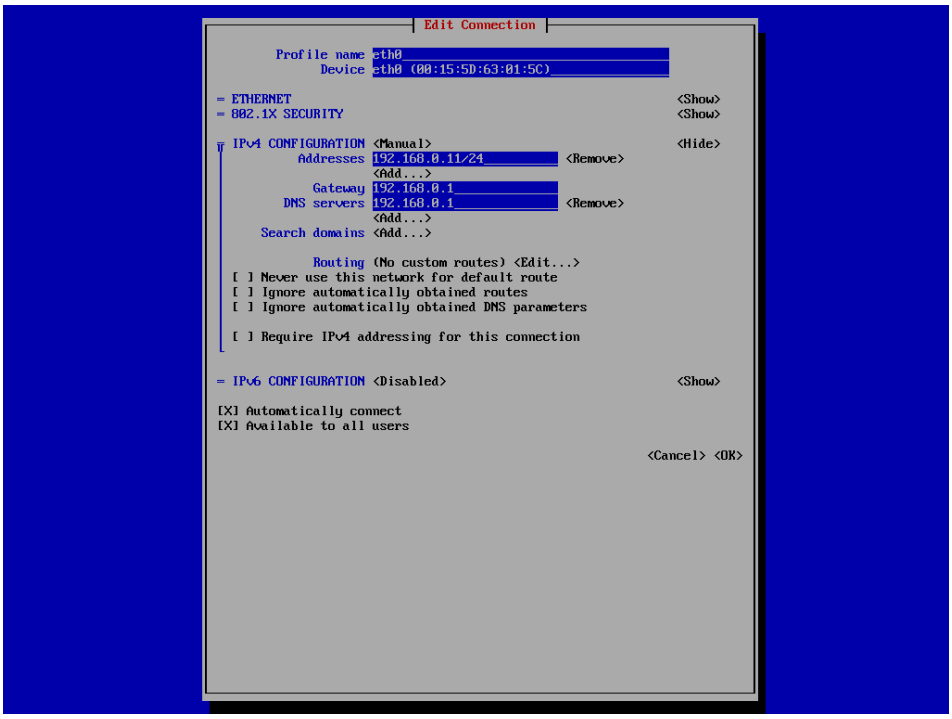

Leap Micro Container OS 2025.05-6
Select keyboard layout
tr-f
tr-intl
tr-ku_alt
tr-ku_f
tr-ku
tr
tw-indigenous
tw
tw-saisiyat
ua-crh_alt
ua-crh_f
ua-crh
ua-utf
us-altgr-intl
us-alt-intl
us-colemak_dh_iso
us-colemak_dh
us-colemak_dh_ortho
us-colemak_dh_wide_iso
us-colemak_dh_wide
us-colemak
us-dvorak-alt-intl
us-dvorak-classic
us-dvorak-intl
us-dvorak-l
us-dvorak-mac
us-dvorak
us-dvorak-r
us-dvp
us-euro
us-haw
us-hbs
us-intl
us-mac
US
97%
< OK >
<Cancel>

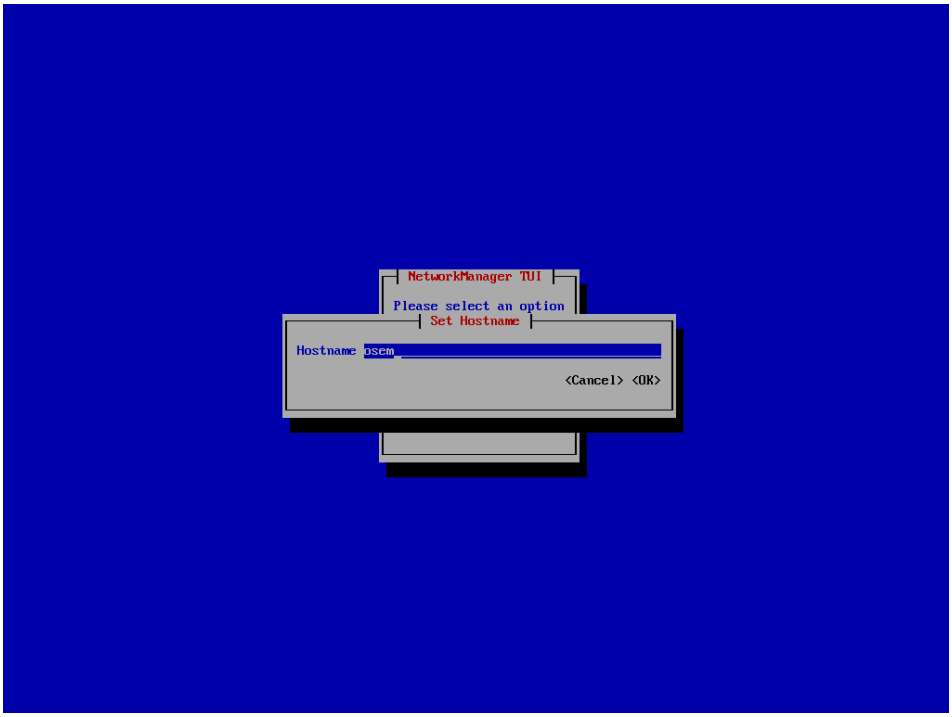

Leap Micro Container OS 2025.05-6
Select time zone
UTC
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara
Africa/Bamako
Africa/Bangui
Africa/Banjul
Africa/Bissau
Africa/Blantyre
Africa/Brazzaville
Africa/Bujumbura
Africa/Cairo
Africa/Casablanca
Africa/Ceuta
Africa/Conakry
Africa/Dakar
Africa/Dar_es_Salaam
Africa/Djibouti
Africa/Douala
Africa/El_Aaiun
Africa/Freetown
Africa/Gaborone
Africa/Harare
Africa/Johannesburg
Africa/Juba
Africa/Kampala
Africa/Khartoum
Africa/Kigali
Africa/Kinshasa
Africa/Lagos
Africa/Libreville
Africa/Lome
Africa/Luanda
8%
< OK >
<Cancel>

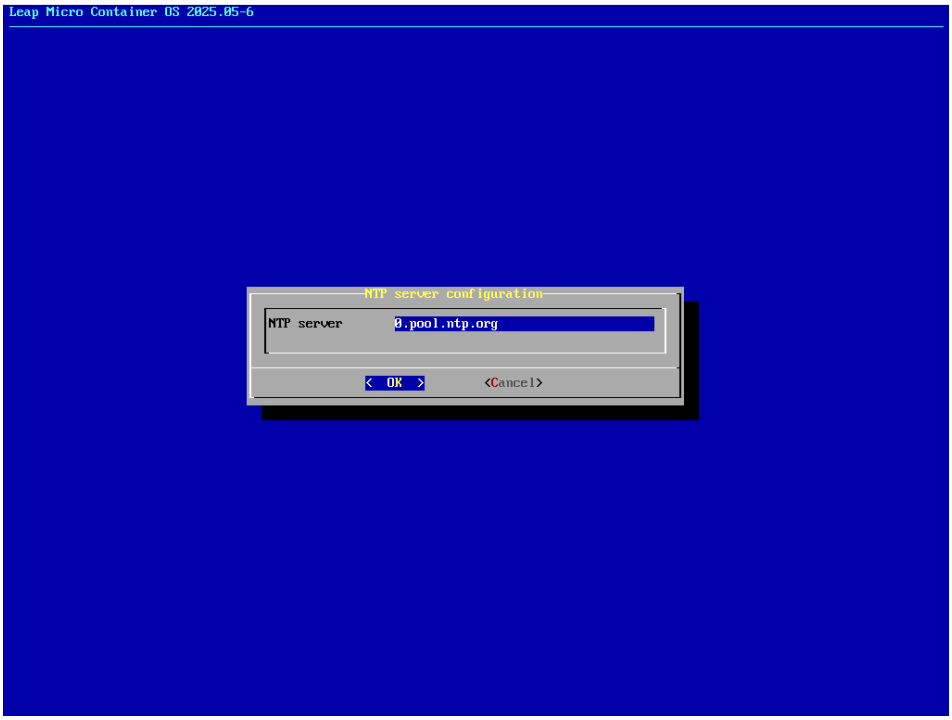

Leap Micro Container OS 2025.05-6
Select speed and duplex settings
100full 100 MBit Full Duplex
1000full 1 GBit Full Duplex
10000full 10 GBit Full Duplex
auto Auto Negotiation
< OK >

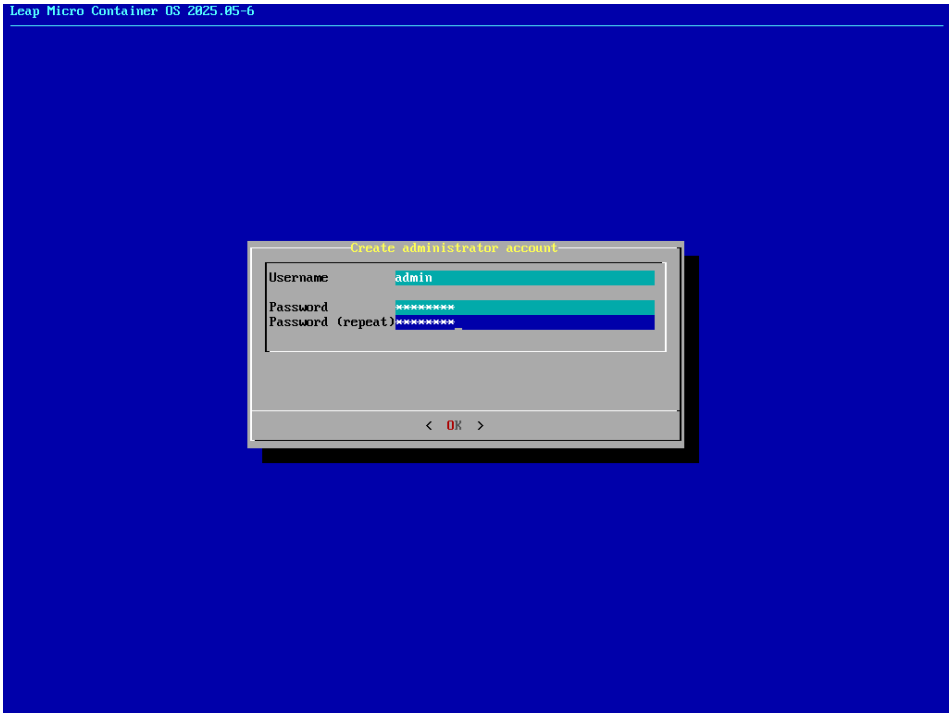

Initializing network interfaces...


Leap Micro Container OS 2025.05-6
Adapt network interface configuration?
< Yes >
< No >


Edit Connection
Profile name eth0
Device eth0 (00:15:5D:63:01:5C)
= ETHERNET <Show>
= 802.1X SECURITY <Show>
IPv4 CONFIGURATION <Manual> <Hide>
Addresses 192.168.0.11/24 <Remove>
<Add...>
Gateway 192.168.0.1
DNS servers 192.168.0.1 <Remove>
<Add...>
Search domains <Add...>
Routing (No custom routes) <Edit...>
[ ] Never use this network for default route
[ ] Ignore automatically obtained routes
[ ] Ignore automatically obtained DNS parameters
[ ] Require IPv4 addressing for this connection
= IPv6 CONFIGURATION <Disabled> <Show>
[X] Automatically connect
[X] Available to all users
<Cancel> <OK>


NetworkManager TUI
Please select an option
Set Hostname
Hostname osem
<Cancel> <OK>


Leap Micro Container OS 2025.05-6
NTP server configuration
NTP server 0.pool.ntp.org
< OK >
<Cancel>


Leap Micro Container OS 2025.05-6
Create administrator account
Username
admin
Password
Password (repeat)
< OK >


Leap Micro Container OS 2025.05-6
container-os login:

IMPORTANT:

- The server should be configured with a static IP address to avoid the added complexity and potential failures associated with DHCP dependencies.
- To configure fixed speed and duplex settings after the installation, use the following command to adapt the interface settings.

```
sudo nmcli connection modify eth0
 802-3-ethernet.auto-negotiate no 802-3-
ethernet.speed 1000 802-3-ethernet.duplex
 full
restart
```

3.2 Advanced configuration

For the advanced configuration which may include installing additional packages or update the installed packages of the operating system, make sure the installation ISO file is available either

- attached on a USB device to the physical machine
- attached as CD-ROM to the virtual machine
- copied as ISO file to the machine into the folder /var/tmp/

If you are running a cluster and after you have finalized the cluster setup, you can upload new ISO images to the primary node (node-1) and run the following command to sync the ISO file between the nodes

```
sync-nodes
```

System Information

To get some basic system information, run the following command
`system-info`

VM-Tools

In case you need to install open-vm-tools because you are running in a VMware environment, run the following command
`install-vm-tools`

Update Appliance

To update the packages of the operating system, run the following command:
`update-appliance`

and confirm the package update/installation.

A reboot is recommended after upgrading operating system packages
`restart`

Reset

To reset OSEM Container Appliance and to remove current OSEM installations, run:
`reset-appliance`

IMPORTANT:

In a cluster environment, you must run the reset activity on kube-1 node first, this will uninstall OSEM and cleanup all related data to it. After this has been finished, run the reset command on nodes kube-2 and kube-3.

3.3 Prepare Standalone

The standalone OSEM installation uses Docker and Docker Compose.

Prepare the operating system

The ISO file used to install the operating system includes all necessary packages. Please make sure the ISO file is available as described here: Advanced configuration on page 18

Run the following command to install required packages for standalone operation:

`prepare-standalone`

Install OpenScape Endpoint Management

Copy the latest OpenScape Endpoint Management RPM packages to the local repository at /opt/local-repo. When the sha256 file is provided, the hash will be checked before extracting and installing the RPM files.

Run the following command to install OSEM for the first time.

`deploy-osem`

If multiple Ethernet interfaces are detected, you must select the primary OSEM interface. Additionally, you can choose a different interface for admin access of OSEM (aka management interface, API, Admin UI)

Update OpenScape Endpoint Management

To update to a newer version, simply copy the new RPM packages file to the/opt/local-repo folder and run the following command.

```
deploy-osem
```

Get Logs

To retrieve logs from your OSEM installation, use the following command.

```
osem-logs
```

To view logs in real time on your system, run

```
osem-logs -f
```

If you want to store logs into a file from the last hour, run the following command: `osem-logs --since 60m > /tmp/wpi.log`

3.4 Prepare Cluster

The OSEM cluster installation uses Kubernetes RKE2. It is expected that the cluster will have three nodes. For cluster setup, all nodes must be on the same subnet, and multicast traffic must be supported in the network to finalize the setup.

Prepare the operating system

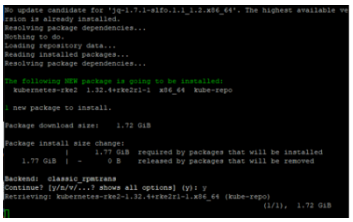
The ISO file used to install the operating system includes all necessary packages. Please make sure the ISO file is available as described here: Advanced configuration on page 18

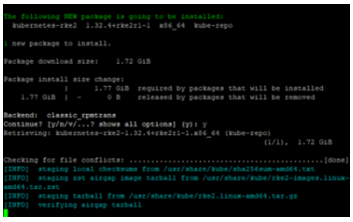
Run the following command to install the required packages for cluster operation on all three nodes in your cluster.

```
prepare-cluster
```

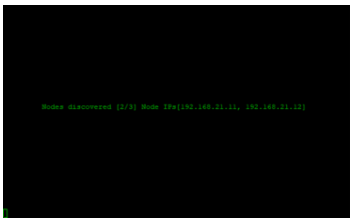
Wait for the cluster setup to finish. While nodes are being identified, you will be updated with the current state. The overall process will take some time to complete.

The node with the lowest numerical IP address will be the first node in the cluster (node-1). Nevertheless, a high-availability cluster will be installed, but all primary cluster operations will be performed on this node. During the installation process, you will be shown the node IDs to learn which node is the first node (node-1)



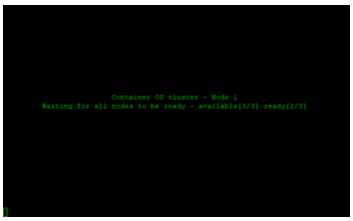


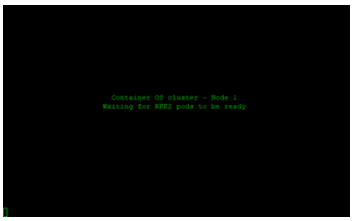

Starting node discovery


Nodes discovered [2/3] Node IPs[192.168.21.11, 192.168.21.12]


Container OS cluster - Node 1
Waiting for primary node to be ready

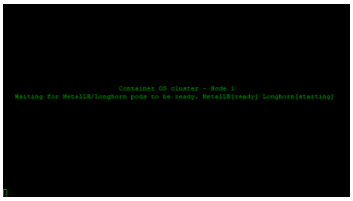

Container OS cluster - Node 1
Waiting for all nodes to be ready - available[1/3] ready[1/3]


Container OS cluster - Node 1
Waiting for all nodes to be ready - available[3/3] ready[2/3]


Container OS cluster - Node 1
Waiting for RKE2 pods to be ready


Container OS cluster - Node 1
Extracting Longhorn images


Container OS cluster - Node 1
Waiting for MetalLB/Longhorn pods to be ready. MetalLB[waiting] Longhorn[waiting]



Install OpenScape Endpoint Management

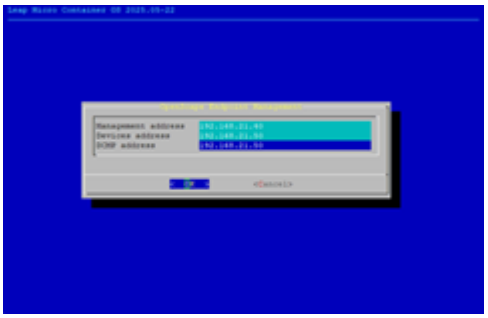
Compared to the ‘prepare-cluster’ command, the installation of OpenScape Endpoint Management must only be done from a single node in the cluster (node-1 is the clear recommendation)

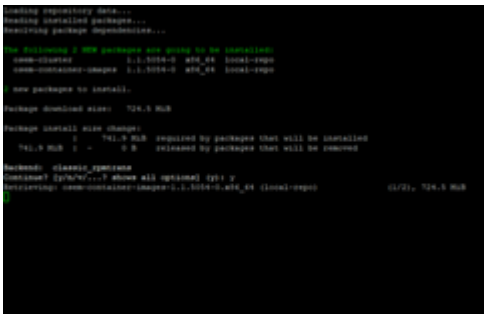
Copy the latest OpenScape Endpoint Management RPM packages to the local repository at **/opt/local-repo on node 1 of the cluster**. When the sha256 file is provided, the hash will be checked before extracting and installing the RPM files.

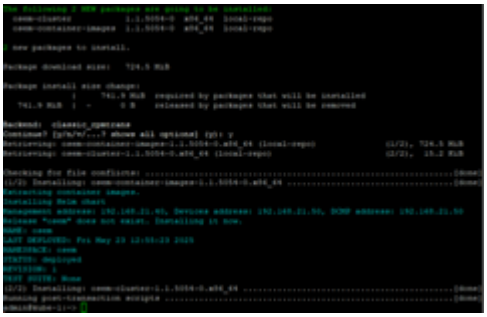
Run the following command to install OSEM for the first time.

```
deploy-osem
```

During the first installation, you must choose free IP addresses on the same subnet. OSEM uses the Metallb load balancer to handle incoming traffic. This component handles the given IP addresses. It is OK to use a single IP address for all interfaces.







Afterwards, the OSEM admin UI is available on the management address provided

The license locking ID will be bound to the node in the cluster, from which you installed OpenScape Endpoint Management by running the command ‘deploy-osem.’

Even if you have to reinstall the cluster from scratch, as long as you run the initial installation on the same node, the locking ID will remain.

Update the Kubernetes cluster.

To update the Rancher Kubernetes Engine (RKE2), go node by node and update the primary node (node-1) last.

Please make sure the ISO file is available as described in Advanced configuration on page 18.

Run the following command to update the Kubernetes cluster: `kube-update`

Get Logs

To retrieve logs from your OSEM installation, use the following commands.

```
osem-logs-wpi
```

```
osem-logs-api
```

```
osem-logs-couchdb
```

To view logs related to client communication in real time on your system, run

```
osem-logs-wpi -f
```

If you need to investigate the OSEM API logs, run the following command

```
osem-logs-api -f
```

And the same about CouchDB

```
osem-logs-couchdb -f
```

If you want to store logs into a file from the last hour, run the following command: `osem-logs-wpi --since=60m > /tmp/wpi.log`

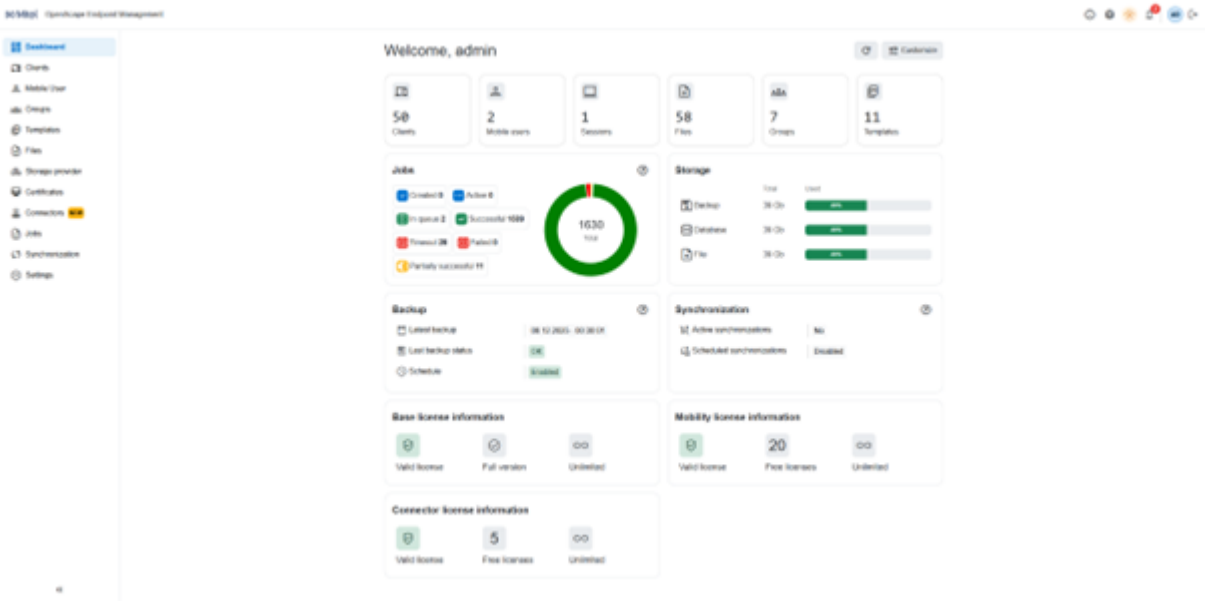
4 Getting started with OpenScape Endpoint Management

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

4.1 Main interface

The OpenScape Endpoint Management "Dashboard" page allows you to view statistics of the registered clients and users, active sessions, uploaded files, number of groups, running or finished jobs, license information along with various configuration options.

It also 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, language options, app theme customization, the notifications panel and your profile details from the top right of the app.



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 dashboard at any time, click on the **Mitel** 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.

You can customize the dashboard by selecting the relevant information to be displayed.

4.2 Signing in and out

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

4.2.1 Initial setup wizard

Follow the steps below to sign in to the 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.

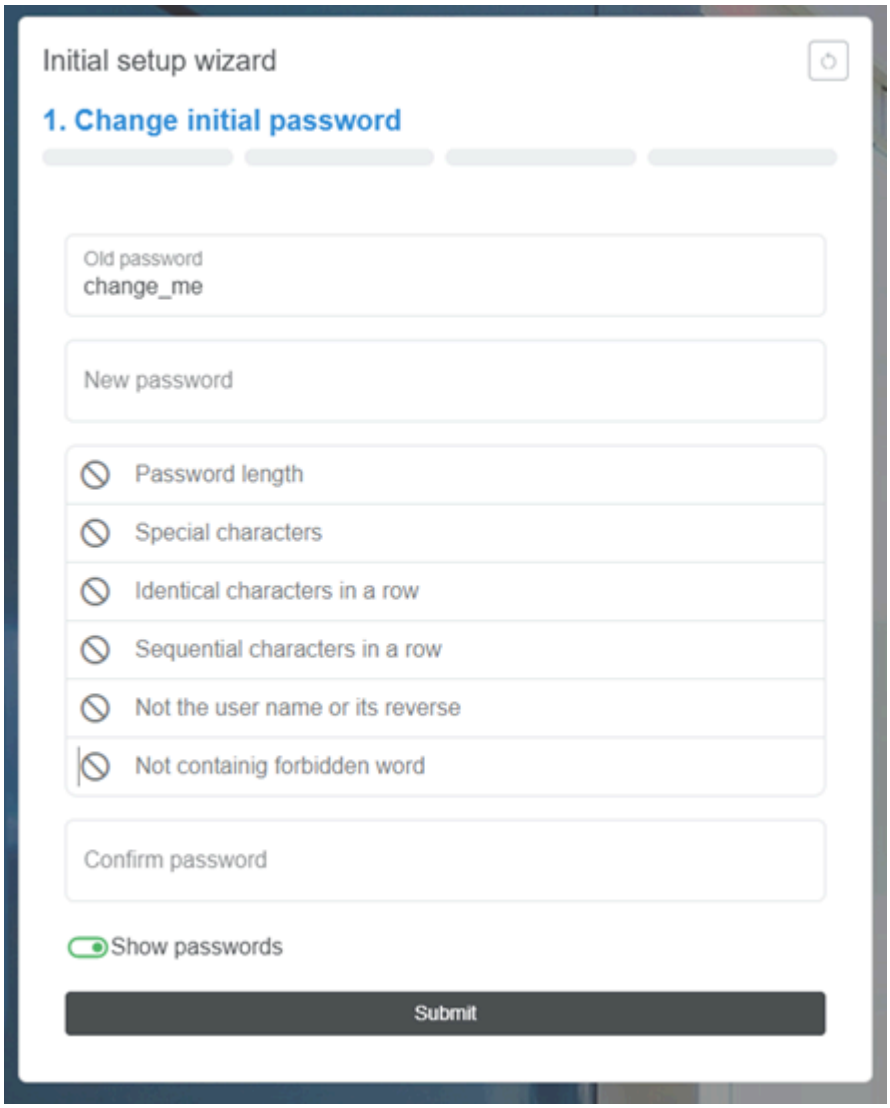
You can click on the top right of the login screen to select the language in which you wish to display the app.

The following languages are available:

- English (default)
- German

2) Enter the default username: **admin** and password: **change_me**.

3) Click **Login** and change the initial password.



4) Enter the default password in the Old password field, choose a new password, and confirm your chosen password.

5) Click **Submit**

6) **Activate Multi Factor Authentication**
At this point, you can choose to enable Multi Factor Authentication, or you can skip the MFA activation and enable it at any point later in time via your user configuration.

7) Click **Submit** or **Skip**

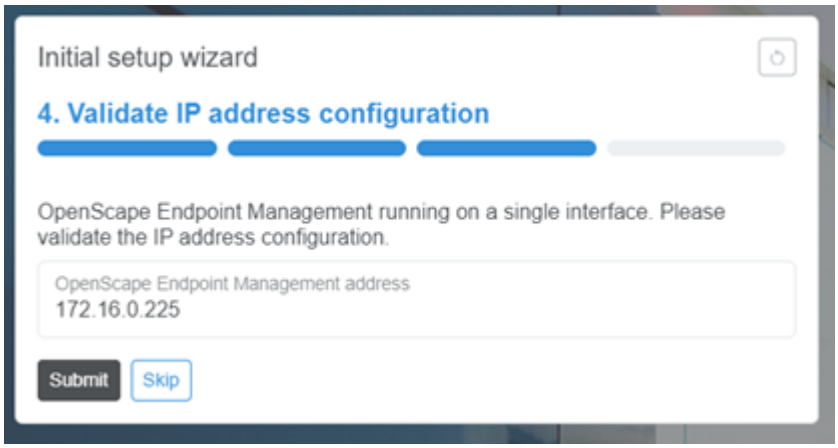
8) Add Import DLS or OSEM Backup. You can choose to either upload an OSEM Backup from a previous OSEM installation or choose a DLS export to be imported into OSEM.
If you choose to add a personal password for the OSEM Backup encryption, please enter the password.

9) Click **Upload and import** or **Skip**.

DLS restore supports Mobile Users, DLS Locations get matched into OSEM Groups, DLS templates/Profiles will be matched to OSEM

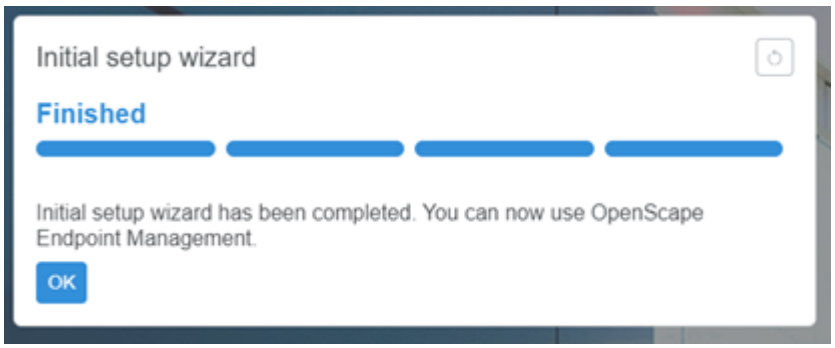
Templates. If you choose not to import a DLS export, please note that you will not be able to upload after finishing the **Initial Setup** steps.

Validate IP address configuration.



10) If you installed the OSEM Container Appliance with a single Ethernet interface, confirm the IP address that you want to use for the OSEM Application.

11) Click **Submit** or **Skip**.



12) Click **OK** to finish the initial setup wizard.

4.2.2 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 ⊕ on 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 dashboard.

4.2.3 Signing out

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

4.3 Viewing app information

You can view the information of the OpenScape Endpoint Management'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 can be accessed by selecting **What's new** section.
- Under the License section, you will find the **EULA** (End User License Terms for OpenScape Endpoint Management).
- The **TPSI** (Third Party Software Information for OpenScape Endpoint Management).
- You can also download **open -source** licenses. By clicking on the Open-Source license, the license will be automatically downloaded.
- If you click on the **Open API documentation** you are navigated to a new browser tab that opens a Swagger UI to all API calls for the OSEM Rest API. You will need to authorize with a token for experiment on this tab with the API calls.
- OSEM comes with a visual low-code Node-Red Platform. You can access this Platform with the OSEM login credentials.
- Clicking on the Feedback link will bring you to the Mitel User Voice communication. https://mitel.uservoice.com/ Here you can share your feedback outside of official Bug or Change Request reports.

4.4 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 28.
- 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.

4.5 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.

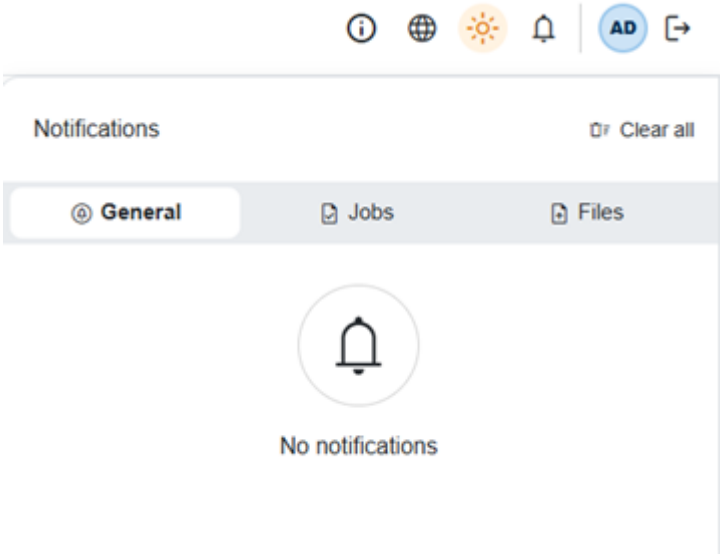
You can change the theme from the top bar of the app:

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

4.6 Viewing notifications

Notifications keep you informed about important events and actions in the OSEM system. They appear in the user interface and alert you to things like job progress, file operations, and general system updates.

Notifications are displayed in the notification area of the OSEM web interface. You'll see them pop up for a few seconds, and you can review recent notifications in the notification panel.



Types of Notifications

- **Job Notifications**

  You'll receive notifications when jobs are created, updated, completed, or if they fail.

  Example: "A backup job has completed successfully" or "A scheduled job has failed."

- **File Notifications**

  Notifications are sent when files are uploaded, deleted, or modified.

  Example: “File upload completed” or “File was deleted.”
- **General Notifications**

  These cover other important system events, such as warnings, status changes, or system messages.

  Example: “System maintenance scheduled for tonight” or “A new update is available.”

4.7 Managing your account

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

4.7.1 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 or select **Account management** from the **Settings** menu.
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 with your account. For more information regarding language settings, see Changing the language settings on page 29.

   A window opens allowing you to update your email address or language.
4) When you finish 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.

4.7.2 Updating password

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

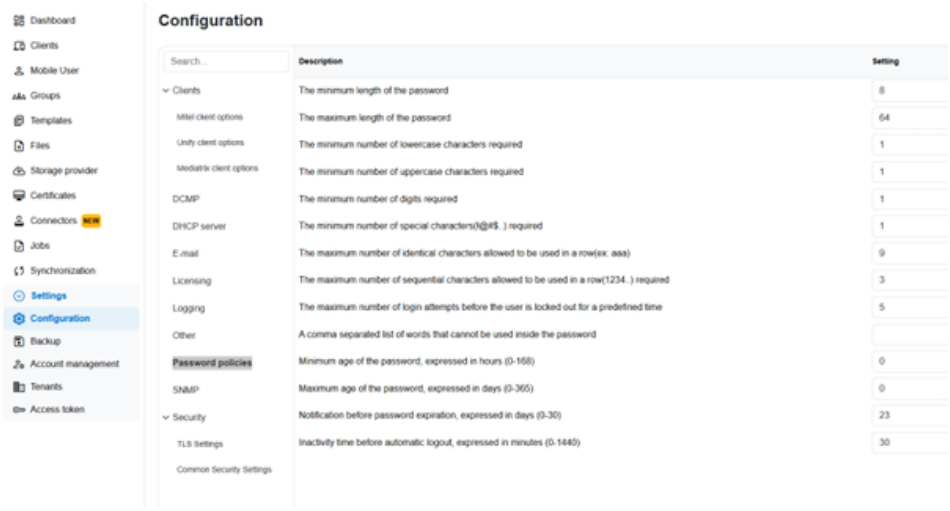
The chosen password has to follow the configured Password Policy found under Settings -> Configuration -> Password Policies. Only a User with the Default Admin or Server Admin rights can change the Password Policies.

4.7.2.1 Password policies

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

The chosen password has to follow the configured Password Policy found under Settings -> Configuration -> Password Policies. Only a User with the Default Admin or Server Admin rights can change the Password Policies.

Current configurable policies and their properties:



- Minimum length of password:
  - the minimum number of characters that a password must have
  - default: 8
  - minimum value: 8
- Maximum length of a password:
  - the maximum number of characters that a password must have
  - default: 64
  - maximum value: 64
  - minimum value: -

  There is **no validation between the minimum and maximum values** (i.e a user can set a minimum of 50 and maximum of 20)
- Minimum number of lowercase characters:
  - the minimum number of lower case characters that a password must have (ex: 'a')
  - default: 1 (enabled by default)
  - maximum value: 64
  - minimum value: 0
- Minimum number of uppercase characters:
  - the minimum number of upper case characters that a password must have (ex: 'A')
  - default: 1 (enabled by default)
  - maximum value: 64
  - minimum value: 0 (disabled)

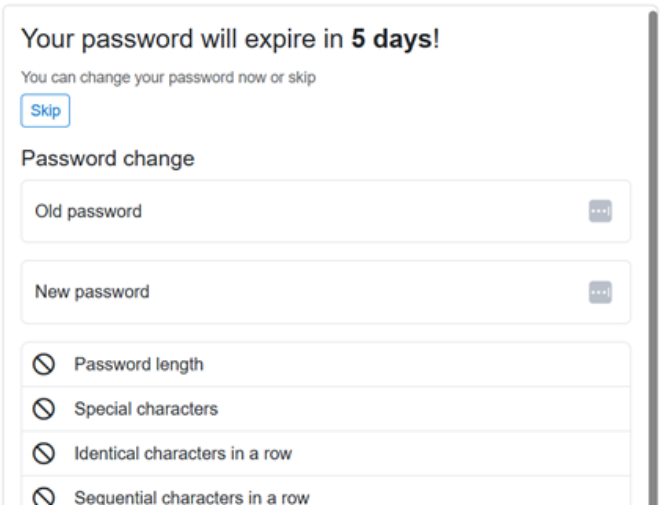
- Minimum number of digits:
  - the minimum number of digits that a password must have (ex: '1')
  - default: 1 (enabled by default)
  - maximum value: 64
  - minimum value: 0 (disabled)
- Minimum number of special characters:
  - the minimum number of special characters that a password must have (ex: '*')
  - default: 1 (enabled by default)
  - maximum value: 64
  - minimum value: 0 (disabled)
- Maximum number of identical consecutive characters:
  - the maximum number of identical consecutive characters that a password must have (ex: 'aaa')
  - default: 3 (enabled by default)
  - maximum value: 64
  - minimum value: 3
- Maximum number of sequential consecutive characters:
  - the maximum number of sequential consecutive characters that a password must have (ex: 'abc')
  - default: 3 (enabled by default)
  - maximum value: 64
  - minimum value: 3
- Maximum number of failed logins:
  - the maximum number of failed logins after which a user is locked out
  - default: 5 (enabled by default)
  - maximum value: 64
  - minimum value: 0
- A comma separated list of forbidden words
  - user inputed list of words separated by ',' that are not allowed in a password
  - default: defaults to an empty string, but is combined with a predefined list of words. The predefined list is stored in */src/common/words* and contains 100 words. **Leaving the setting empty does not disable the setting**. The 100 words are always forbidden. Initial source of the list comes from https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt
- Minimum age of password
  - How much time, expressed in hours, must pass after a password change before a user can change the password again
  - default: 0 (disabled by default). 0 means the user can change the password immediately after a previous password change
  - maximum value: 168
  - minimum value: 0 (disabled)

- Maximum age of password
  - After how much time, expressed in days, must the password be changed
  - default: 0 (disabled by default). 0 means the password does not expire
  - maximum value: 365
  - minimum value: 0 (disabled)
- Notification before password expiration
  - **If the password has a maximum age**, this setting is used to notify the user that the password will expire and must be changed. The user will be notified at every login for the X days left until expiration, where X represents the user's set value
  - default: 4 (enabled by default)
  - maximum value: 30
  - minimum value: 0 (disabled)
- Inactivity time before automatic logout
  - After how many minutes of inactivity do we automatically log out the user
  - inactivity is defined as: OSEM tab is not in focus OR is in focus but no mouse movement/ clicks/ scrolls/ keypresses for X minutes
  - default: 10 (enabled by default)
  - maximum value: 99
  - minimum value: 1

Next steps

Password will expire notification

If the password has a maximum age and the value for notification before password expiration is >0, at every login the user will see:



The user can skip or change the password with the Password Change form.

If the password has expired, the skip option is not present.

4.7.3 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.

4.7.4 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-digit code is generated inside the authenticator app.
5) Provide the 6-digit 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.

4.7.5 Registering a new account - Account management

As the user with the "Default admin" role, you can register a new account, provide contact information and assign specific roles.

Step by Step

1) Select **Settings** menu.
2) Click on **Account management**

   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 **Roles** 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 31.

4.7.6 Creating an access token

An Access Token is a secure, unique string that allows you or an application (for example, CMP or OS4K Manager) to access OSEM's API or services without

using your main password. Tokens can be created, managed, and revoked from your user interface.

Step by Step

1) Select **Settings** on the left menu.
2) Click on **Access token**

   You are navigated to the **Access token** area.
3) Click **+ New** on the top right.
4) Enter the details of the new account:
   - In the **Name** field, enter the user name you are assigning to the new access token to log in to the app.
   - In the **Expires at** field, you can set the expiration date of the token. You can choose from:
     – No expiration
     – 180 days
     – 365 days
     – 730 days

     By default, the **No expiration** option is selected.
   - Enter the password, and in the **Confirm Password** field, enter the password again.
   - From the **Roles** list, select the role/s you want to assign to the new access token.
5) Click **Submit**.
   A confirmation window with the new access token is displayed.

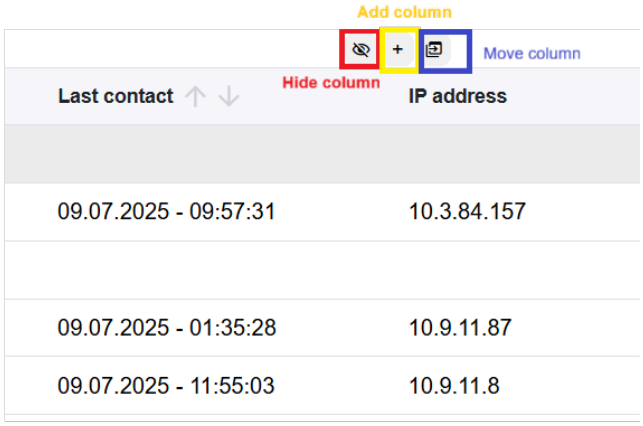
   After entering a Name for the token and selecting the expiration and assigned Roles, the new access token is created and can be copied to the clipboard from the confirmation window.

NOTICE: Please save the token now, as it cannot be shown again later.

4.8 Table Header Options

Each **table header cell** provides the following options:

- **Hide column** – Hides the selected column from view.
- **Add column** – Adds a new column to the table.
- **Resize column** – Adjusts the width of the selected column.
- **Move column** – Changes the position of the column within the table.



Managing Table Columns

Hide a Column

1) Hover over the column you want to hide.

NOTICE: Static columns cannot be hidden.

---

2) Click **Hide**.**Add a Column**
3) Hover over the column **in front of which** you want to add the new column.

NOTICE: Static columns cannot be added, and no columns can be placed between static columns.

)
4) Click **Add**.
5) Select the column you want to display.

Move a Column

1) Hover over the column you want to move.

NOTICE: Static columns cannot be moved.

---

2) Click and hold **Move**.
3) While holding the button, drag the cursor horizontally to reposition the column.
   - Columns cannot be moved past the **static column area** on the left side of the table.
4) Release the button to complete the move.

Resize a Column

1) Hover over the column you want to resize.

   A **lateral bar** appears on the right edge of the column.
2) Click and hold the lateral bar.

3) While holding, move the cursor horizontally to adjust the column width.

NOTICE:

The column cannot be resized beyond its **minimum width** limit.

4) Release the button to finish resizing.

5 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).

  E.g. 4989700732406.
- **Type**

  Supported workpoint device type.

  E.g. CP600, CP410, etc.
- **Device ID**

  Will be used as the unique device identifier.

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

  Represents the software version type used by the client.

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

  The last interaction with the device is presented in the form of date and time.

  E.g. 20.09.2023 - 16:50:42.
- **Registration server**

  The registration Server used by the client

- **Features**

  The features available for the client. When a feature icon is displayed in 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 47

  – **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 to the device**:

    The device can have direct access or could require DCMP (only supported by Desk Phone and OpenStage Device Family) or STUN (only supported by Mitel 69XX and 68XX).

  – **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.

5.1 Create Plug&Play 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.
   - Select the **Hardware class** 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 47.
   - Select the **Template** from the drop-down list. For more information about the templates, please see chapter Templates on page 68.
   - Select if you want to activate the Plug&Play (P&P) profile with **Plug&Play profile activated**. If not selected, you will not be able to use this Profile for P&P.
   - Select if you like to use a number pool by checking **Use as number pool profile**.
5) Click **Create**.
   A confirmation message is displayed at the bottom center of your browser screen.

5.2 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.

The Scan might show more devices than are actually able to register with OSEM; this could be due to several reasons, such as the client already being registered with a different management system, or OSEM not supporting the client but responding to the Scan itself.

5.3 Configuring client settings

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

5.3.1 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: OSEM tries to read the contact IP address of the client; in some instances, it can not be displayed. You can only open the WBM for the client if the client's IP and the IP of the PC where you open the OSEM application are routed to each other.

5.3.2 Sync data

With **Sync data**, you can force a refresh of the client data; OSEM will create a Synchronize configuration job and read all data from the client and update the OSEM database.

5.3.3 Configuring client parameters

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

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

This is a central menu for displaying and administering clients' parameters. The **Configuration for client** section displays the following information:

- **Search function:**You can also use the **Search** area to find a specific configuration parameter of the client.
- On the top right corner, you can Submit your changes, Refresh data, or**Discard changes**.
- You can minimize the **Configuration for the client** window by using the minimization icon (_) on the top right corner of the window.

The Configuration for the client lists all configurable items for all OSEM-supported Clients. To get an insight into the Configuration items themselves, please refer to the Admin Guide for the specific client you would like to configure.

All Admin and User Guides for the Clients can be found in the Mitel Document Center.

5.3.4 Applying templates

The "Apply Templates" section in the GUI allows you to assign one or more configuration templates to selected clients. You can assign templates to specific clients even if the client is already part of a Group and the group has templates configured.

When you use this feature, you can perform the following actions:

- select templates from a list (with filtering and multi-select).
- choose to apply templates immediately or schedule them for later.
- reset all assigned templates

5.3.5 Deploying client files

In this section you can deploy files for 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, or 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 filter options:

- Enter a name or the 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, or 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 the file operation is executed and is then confirmed by the message **Operation completed successfully**.

5.3.6 Configuration file

For some Clients, OSEM will display the configuration file that OSEM automatically creates for your Client. Clients that use configuration files instead of a configuration interface include the Mitel 68XX and 69XX Device Family, as well as the Mediatrix Device Family.

5.3.7 Copying client settings

In case of hardware changes or factory reset of a client, you can easily copy the configuration of a client and therefore activate a Plug&Play profile.

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 the 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 (not changeable in this step)
       - Secure Mode
4) Click **Submit**.

5.3.8 Generating a template

You can easily generate a template based on the confuguration of the selected client.

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 - template only applied at the time the client registers for the first time with the OSEM.
     – Default template - template gets applied every time the client registers with the OSEM.
     – Disabled template – In case you only want to create a template but ensure that it’s not applied to any client.
   - Select **true** or **false** for the **Mobile User Template** – if true, then the template will only be applied to Mobile Users
   - 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. The higher the Rank, the higher the configuration priority. E.g., if two templates have the same configuration item, the configuration item in the template with the higher rank will be applied last and therefore will show up at the client.
   - From the **Clients** drop-down list, select the device/s you want to make the template applicable for.

     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 to.

     If no client is selected, then all clients 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.
   - You can select **restrictions for software deployment**, which will limit the weekdays when the Software gets automatically deployed.
4) Click **Submit**.

5.3.9 Resetting client configuration settings

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

Step by Step

1) Click ⋮ on the client's right.
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**.

5.3.10 Diagnostics

When a problem occurs on a connected device, OSEM is capable of retrieving diagnostic data from it. The current devices that support uploading diagnostic data to OSEM are:

- OpenStage
- OpenScape Desk Phone IP / CP
- Mitel 69XX

The following type of diagnostic data can be uploaded:

- Trace files
- Security log files
- Wireshark trace files

The file upload mechanism and APIs to access the diagnostic data are already in place, so this story is purely about the UI implementation of accessing and managing the diagnostic files.

For the OpenScape and OpenStage family, you can actively download the Diagnostic data by selecting the +New button and confirming the action in the pop-up window.

Diagnostic data can be downloaded or deleted via the ⋮ Menu.

5.3.11 Jobs

In this section, you can view all the Jobs that have been applied to the selected client.

5.3.12 Enabling secure mode

If the client supports secure communication, you can enable it following the next steps. The following options are available:

- **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.

5.3.13 Reset secure mode

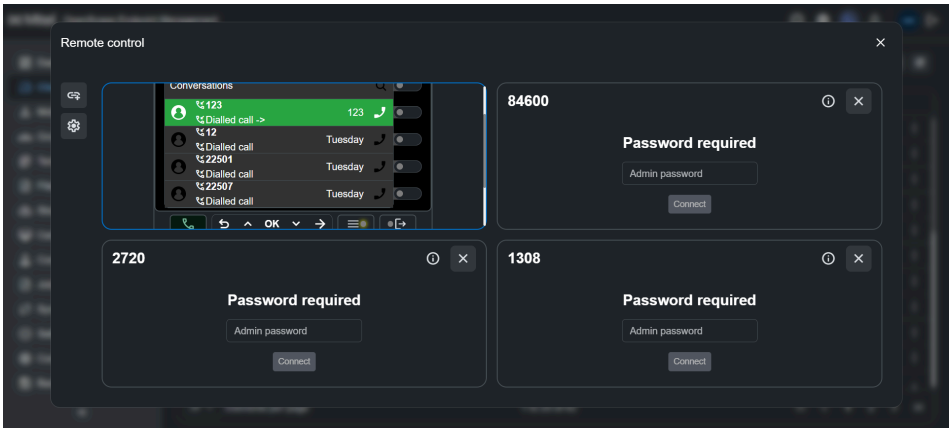
You can disable secure mode of a client that has secure mode enabled.

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).

5.3.14 Remote control

For supported clients, OSEM offers remote control of a selected client.



The remote control can be opened from the Clients page via two options:

- client menu → Remote control

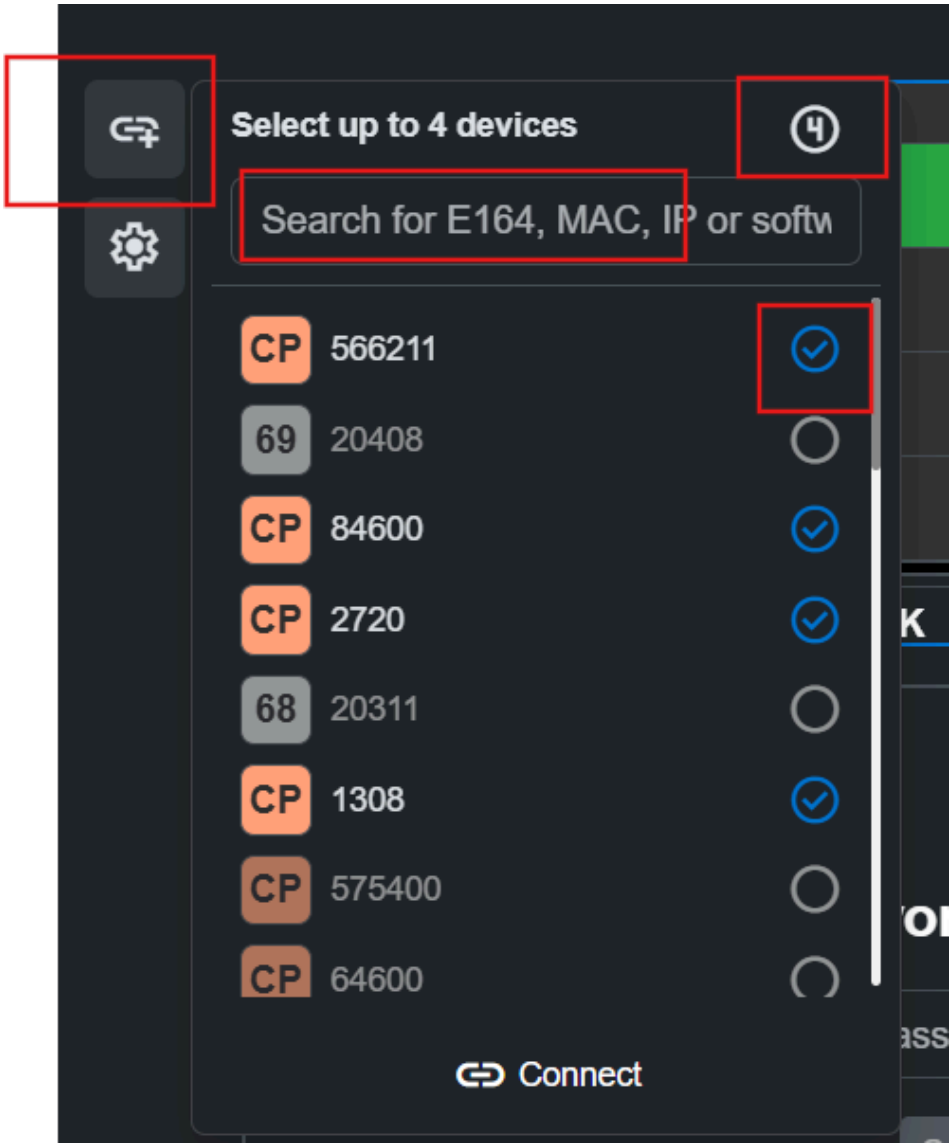
or

- select multiple phones → More button on the header → Remote control(users can select as many phones as desired, only the first 4 are sent to the component)

The remote control window is then split into two:

- On the left side, there are the Connections management button and the Settings button
- On the right side, there are the open connections divided into a grid(2x1 for two phones, 2x2 for three or four phones.

Connection management button

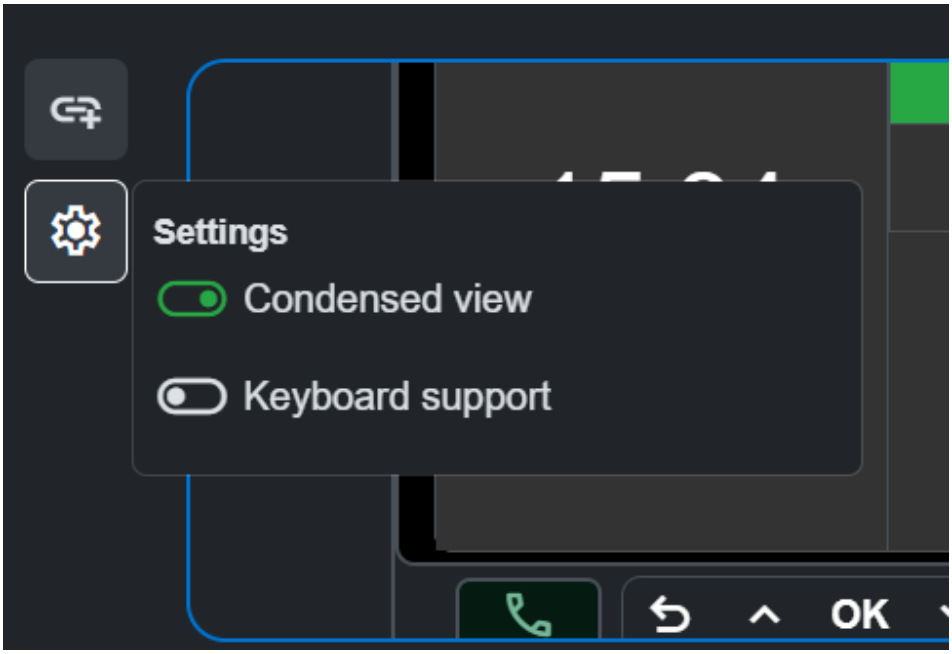


On the top right, there is a counter for the selected devices. It displays the number of currently selected devices. Clicking on it deselects all selected devices.

When opening the Connection management window, a maximum of 50 compatible devices are displayed. Users can then use the Search input to look for specific phones(based on E164/ MAC/ IP)

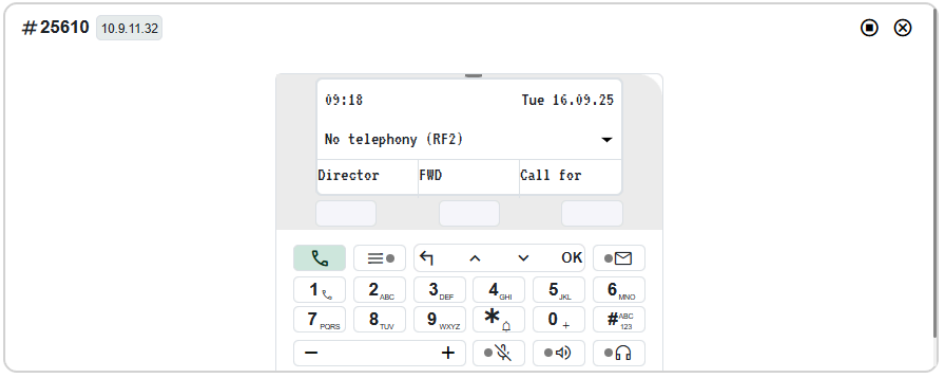
Users can then select 1 to 4 devices to be remotely controlled. After selection is complete, users will click Connect, and the devices will be connected.

Settings



Condensed view

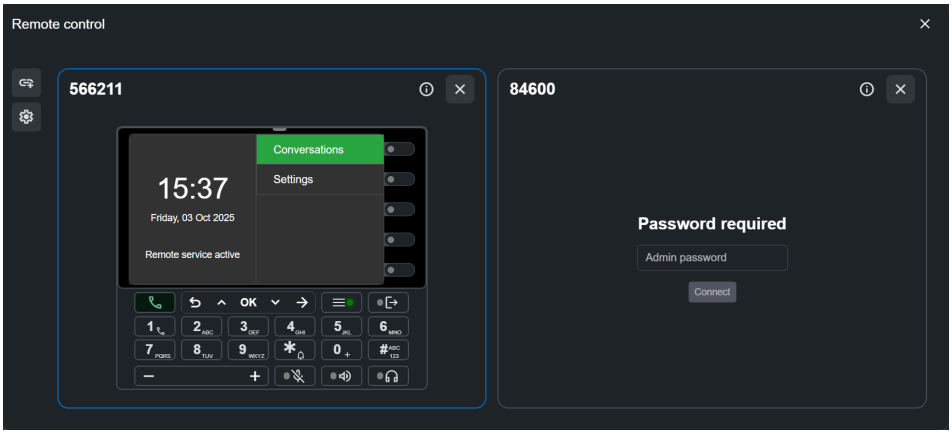
Renders the phones in a more compact view. If disabled, it does full renderings. Affects all open connections, so either all are displayed as condensed, or none is condensed.



Keyboard support

Specific keyboard keys can trigger actions on a device. They include the numeric keys, the Enter key(which triggers OK), and the Arrow keys(which trigger Menu actions)

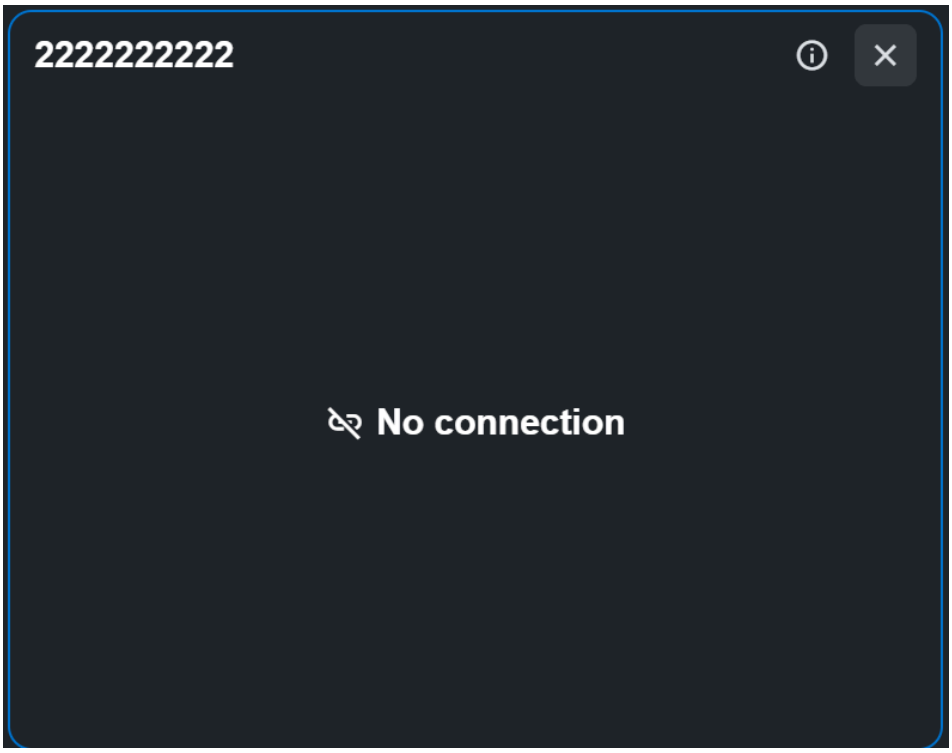
When keyboard support is enabled, pressing a key triggers an action on the currently selected connection. The presently selected connection is highlighted via a blue border.



The connection container

The header displays the E164 number. Two buttons are rendered on the right: the Info and Close buttons. The info button shows the SIP/HFA property, the hardware type, and the IP address. The close button closes the connection.

When opening a connection, the user is prompted for the password first. After entering the password, a "No connection" message is displayed. This message persists until the phone sends the first message. This state indicates that OSEM has initiated the connection and is waiting for the phone to respond.



Phone connection

With an active connection, users can see what the phone is currently displaying on the screen, receive updates about button presses via an animation, trigger button presses, see the states of the LEDs, make calls, etc.

5.3.15 Delete

You can delete 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**.

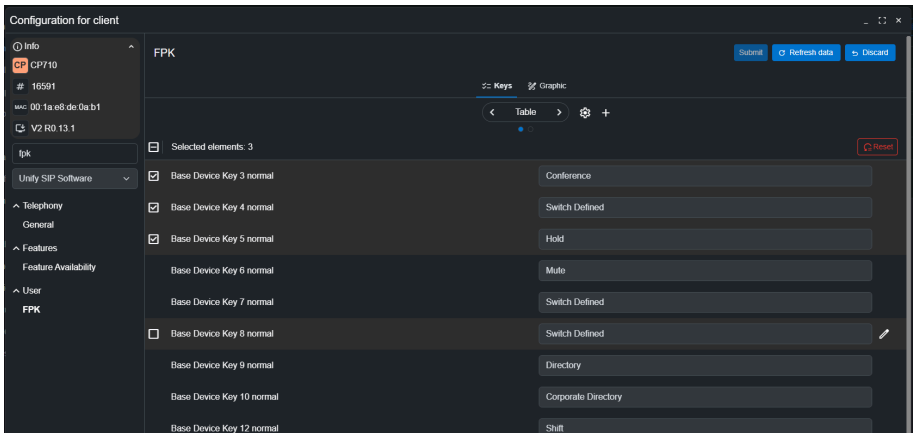
     NOTICE: Once a client is deleted, it will no longer appears in the Clients list.

     A client can show up after it was manually deleted from the OSEM if the OSEM is still configured in the individual client as a Configuration server.
   - Click **Cancel**, to quit the action and close the pop-up window.

5.4 Enhanced FPK Programming

Users can now display FPK data in two ways: **Keys** and **Graphic**.

1) **Keys**



Reset keys

Hovering a key displays a checkbox on the left and the Edit button on the right.

Selecting at least one Key via the checkbox displays a small header. The header contains a global checkbox with two states (some chosen keys or all keys selected), a text field showing how many keys are chosen (or All keys

selected), and a Reset button. Clicking on the reset button resets the chosen keys.

All keys/ selected keys

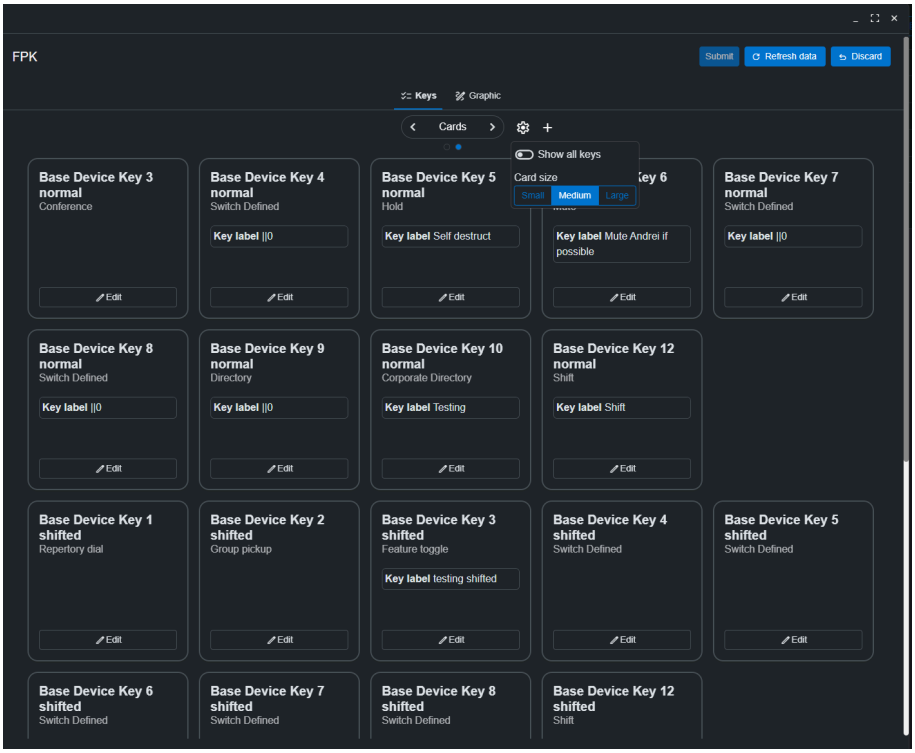
By default, we display just the configured keys. To show all of them, click on the Settings button(near the Table/ Cards view switcher) and then the Show all keys toggle.

Add key

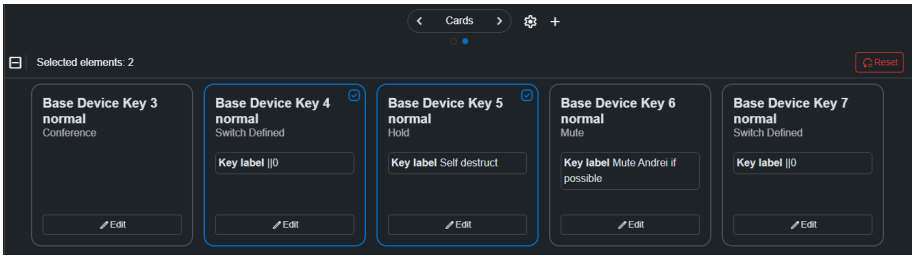
To add a key, click the + button (near the Table/ Cards view switcher).

Cards

Keys can also be displayed as Cards. In this mode, Keys are separated based on their belonging (Base Device keys normal, Base Device keys shifted, etc.).



Increasing the card size displays more data per card. Keys can be selected from this view by clicking on the Card.



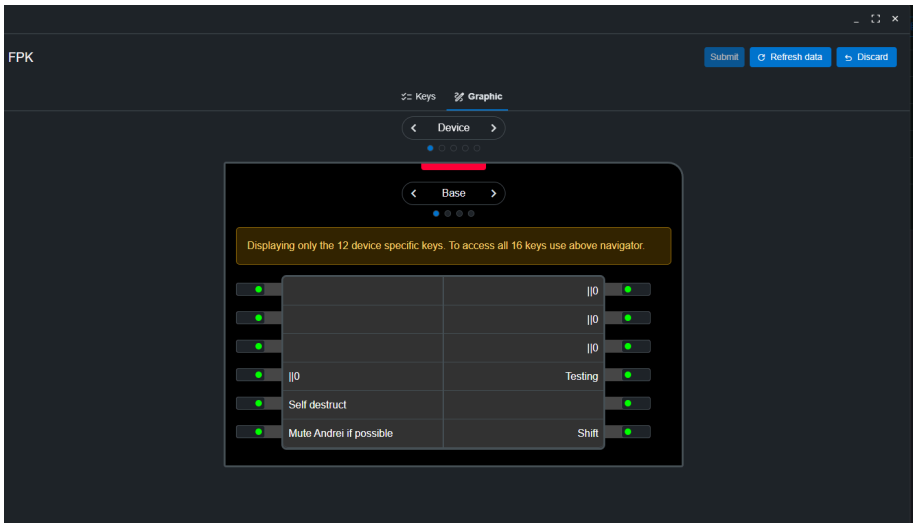
2) Graphic

Keys can be represented Graphically. The user can switch between the Device keys and external module keys(where applicable).

For specific phone models (like CP700), we can also display Base/Shifted keys or Base all/Base shifted keys.

This mode should help the user identify the keys on the actual hardware.

Keys can be edited by clicking the FPK button near the displayed key.



5.5 Number Pool Profiles

A Plug&Play profile can be used as a so-called number pool profile.

A number pool profile will be assigned to a new and unknown client when it first contacts OSEM and does not have an E164 number assigned, and there is no specific Plug&Play profile for this client available (Mac-based)

OSEM will check whether a number pool profile is available that is not currently assigned to any client, and will apply that profile to the new client.

OSEM will track if the client receives a new number afterwards. If this is the case, the number pool profile assigned to this client will be available again for other new clients.

A number pool profile can be created manually from the UI or API.

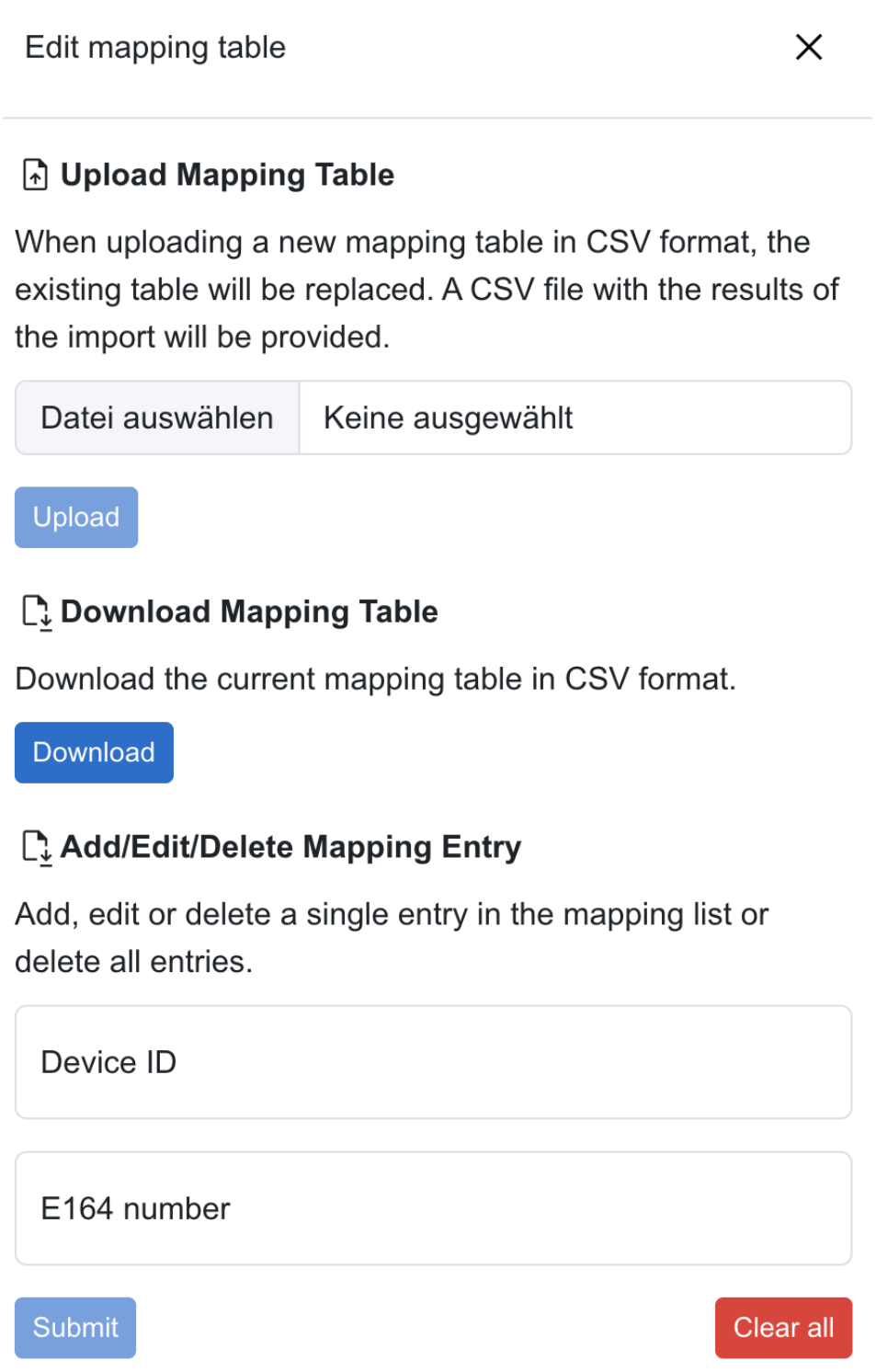
When there is a synchronization created between OSEM and an OS4K or OSV system, you can decide to automatically enable the number pool profile for all Plug&Play profiles created. This is extremely useful if you have a separate Business Group in your OpenScape Voice system dedicated solely to number pool profiles.

5.6 Mapping table

This feature enables customers to associate an **E.164-based Plug & Play profile** synchronized from systems such as **OpenScape 4000 (OS4K)** with the corresponding physical client (either a softclient or a hardphone).

When softclients are used, there is no straightforward or automatic method to input the **E.164 number** upon software startup. Therefore, customers prefer to match clients using the **Windows account name**.

The new functionality can be accessed from the **Clients** table. Selecting the **“Mapping table”** button opens the menu for editing entries in the Mapping table.



Adding Entries

New entries can be added by specifying either a **Windows account name** or a **MAC address**.

- Use the **Windows account name** to match a *softclient* such as **OpenScape Fusion**.
- Use the **MAC address** to match a *hardphone* such as the **CP700**.

You can either add a **single entry** manually or **upload a CSV file** with multiple entries.

When adding a single entry, it will be **appended** to the list.

If the provided ID (account name or MAC address) already exists, the corresponding record will be **updated**.

This enables quick updates of existing records.

When uploading a CSV file, the uploaded data **replaces** the entire mapping table.

After the upload, a **response file** is generated containing the import result for each entry.

Possible issues may include:

- Invalid mapping ID (must be a MAC address or Windows account name)
- Invalid E.164 number length

Deleting Entries

You can:

- Delete a **single entry** by providing its ID.
- Delete **all entries** by leaving the ID field empty.

Downloading Entries

You can **download** the complete mapping table to verify that all records are correct.

6 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.
- **Templates assigned**
  Displays the mobile templates assigned to the selected client.

6.1 Registering a new mobile 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 **Create new user** window is displayed.
3) Add the information regarding the new user:
   - In the **E164** field, enter the user's number (mandatory).
   - If a Software Type is selected, it will limit the configuration items to the software type instead of offering all configuration items.
   - In the **Password** field, enter the password associated with user's account (mandatory).
   - In the **Confirm password** field, enter again the password (mandatory).
   - You can select if a password change is forced when the mobile user logs in for the first time
   - Select any mobile template you wish to apply to this mobile user
4) Click **Register**.

   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.

6.2 Configuring a user account

You can easily configure a user's account.

Step by Step

1) Select **Mobile users** from the left menu
2) Click on the icon ⋮ and select **Configure**

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

1) Forced Logging in or Logging out a user on page 58
2) Configurations for clients, users and templates
3) Deleting a user on page 60

6.2.1 Forced 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.

  Click **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.

  Click **Confirm**.

6.2.2 Home phone

A home phone is an end device assigned to a SIP mobile user.

When a mobile user is being logged off from a device, OSEM needs to check if there is a “home phone” configured for this mobile user. If a home phone is configured, the mobile user will automatically be logged on to this home phone.

- If the device (the home phone) has a different mobile user logged in, this user will not be logged off.
- The home phone has to be available for a mobile user to log in; otherwise, nothing will happen

From the Mobile user Table, click the options for a single user, select “Set home phone,” and select an available device from the list.

The feature can be removed from a single phone by clicking the options menu and selecting “Remove home phone” for a single user or selecting multiple users.

When removing the home phone, the user should confirm the action via an additional pop-up window.

6.2.3 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) Click on the icon ⋮ and select **Configure**

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

- **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 Submit your changes **Refresh data** or **Discard changes**.
- You can minimize the **Configuration for user** window by using the minimization icon _on the top right corner of the window.

The **Configuration for user** includes all configurable items for all OSEM-supported Clients. To get an insight into the Configuration items themselves, please refer to the Admin Guide for the specific client you would like to configure.

All Admin and User Guides for the Clients can be found in the Mitel Document Center.

6.2.4 Managing templates

The "Manage Templates" section in the GUI allows you to assign one or more configuration templates to selected clients.

When you use this feature, you can perform the following actions:

- select templates from a list (with filtering and multi-select).
- reset all assigned templates

6.2.5 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.
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 - Account management on page 36.

7 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.

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 68.
- **Active filters**

  Indicates the filters used to group members, these are highlighted in green color and contain IP addresses and Server addresses.

7.1 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 the 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 68.
- From the **Timezone** drop-down list, select the timezone for the group.

  For more information about the templates, see Group timezone on page 65.
- 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.

  The filter for these fields has to be written as a Regular Expression.

  If you enable **automatic mobile user logoff, you can set the time of day when logged-in mobile users should automatically log off**.

  NOTICE: 24-hour time format is used.

  Example:

  Hours 0 Minutes 0; all logged-in clients will be logged off at midnight of the selected timezone.

  Hours 13 Minutes 15; all logged-in mobile users will be logged off at 1:15 p.m.

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.

7.2 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 68.
   - From the **Timezone** drop-down list, select the timezone for the group.

     For more information about the templates, see Group timezone on page 65.
   - 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.

7.3 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.

7.4 Regular Expression

Introduction

Regular expressions (often called regex or regexp) are powerful sequences of characters that define a search pattern. They're used for string matching within text, allowing you to search and match strings based on a specified pattern. A

regular expression may contain literals or special characters with a predefined meaning.

Elements of a regular expression

- Anchors: Assert the start and end position of a line. ^ (caret) matches the start, and $ (dollar sign) matches the end.
- Character class: Enclosed in square brackets [ ], defines a set of characters to match. For example, [aeiou] matches any vowel.
- Capturing group: Parentheses ( ) are used to create groups, used to treat multiple characters or subpatterns as a single unit.
- Quantifiers: Specify the number of occurrences of the preceding character, character class, or group. Common quantifiers include * (zero or more), + (one or more),? (zero or one), and {} (exact number or range).
- Alternation: | (pipe). It allows you to specify alternatives, matching either the pattern on the left or the one on the right.
- Negation: ^ (caret). Used inside a character class. Matches any character not listed in the character class. [^aeiou] matches any character that is not a vowel.
- Escape character: \ (backslash). It is used to escape a special character, allowing you to match it as a literal. Also used for encoded characters, e.g., \x20 matches a white space character.
- Special character:. (dot) matches any character except new line, \w matches any word character, \d matches any digit, \s matches any whitespace character.

Examples

Some example regular expressions to be used within Openscape Endpoint Management.

IP address range

The following examples can be used for matching IP address ranges:

Regular Expression	Description
192\.168\.0\.((2[5-9])|(3[0-9]))	Starting at **192.168.0.25** until **192.168.0.39**
192\.168\.1\.[0-9]{1,3}	All addresses within subnet **192.168.1.0/24**

Device types

The following examples can be used for matching specific device types:

Regular Expression	Description
CP[67].*	Matches **CP600**, **CP700**, **CP700X** and **CP710**
^CP700$	Matches **CP700** but not **CP700X**

7.5 Group timezone

Groups can set time zones for clients. The list of time zones is the same as the one used for the configuration of the server timezone.

Time zones can be set by adding or editing groups:

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.

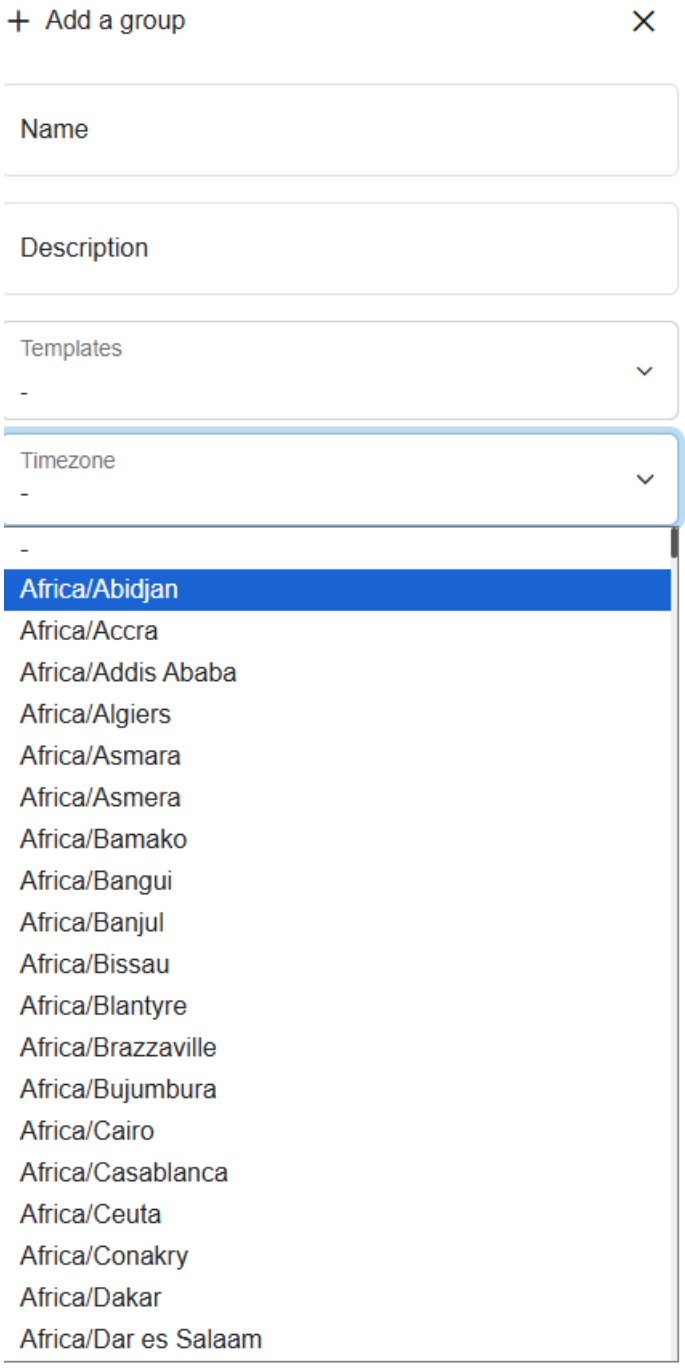
5)

NOTICE:

If no timezone is set for a client, it defaults to the server timezone.

The timezone of a client can be easily inspected via the Features option in the table:

In the **Timezone** drop down section you can select the group timezone.



6) Click **Submit** to register the new group.

The timezone of a client will be **the timezone of the latest Group that was submitted** (new groups or existing groups that were edited).

We recommend using only one group to set the timezone for all clients from a certain timezone. Using multiple groups will get things confusing.

Currently, **the timezone can be reset** only by deleting all groups that set a timezone for the client and then making the client re-contact OSEM.

When deploying files for clients from different timezones, one job per timezone will be created.

The future Job Planned execution time can be inspected, in Jobs.

8 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.

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

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

When creating a template, you can choose to create either an **onboarding** or a **default** template.

- The **default** template is applied to a device in the following cases:
  - when the device starts up
  - when the device sends local configuration changes
  - when the device configuration is refreshed
  - when the templates are assigned to the device

  Only the delta configuration will be sent to the device (the difference between the actual device configuration and what should be configured according to the template).
- The **onboarding** template will only be applied on the very first time the device contacts OSEM and
  - There is no device profile available but the device can be matched to a group that has onboarding templates assigned.
  - There is a plug-and- play profile available (and enabled) that has an onboarding template assigned.

8.1 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 – template only applied at the time the client registers for the first time with the OSEM.
     – Default template – template gets applied every time the client registers with the OSEM
     – Disabled – In case you only want to create a template but ensure that it's not applied to any client.
   - Select true or false for the **Mobile User Template** – if true, then the template will only be applied to Mobile Users
   - 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 8.

     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.

     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.
   - You can select **restrictions for software deployment** , which will limit the weekdays when Software gets automatically deployed.
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.

8.2 Deleting a template

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 68.

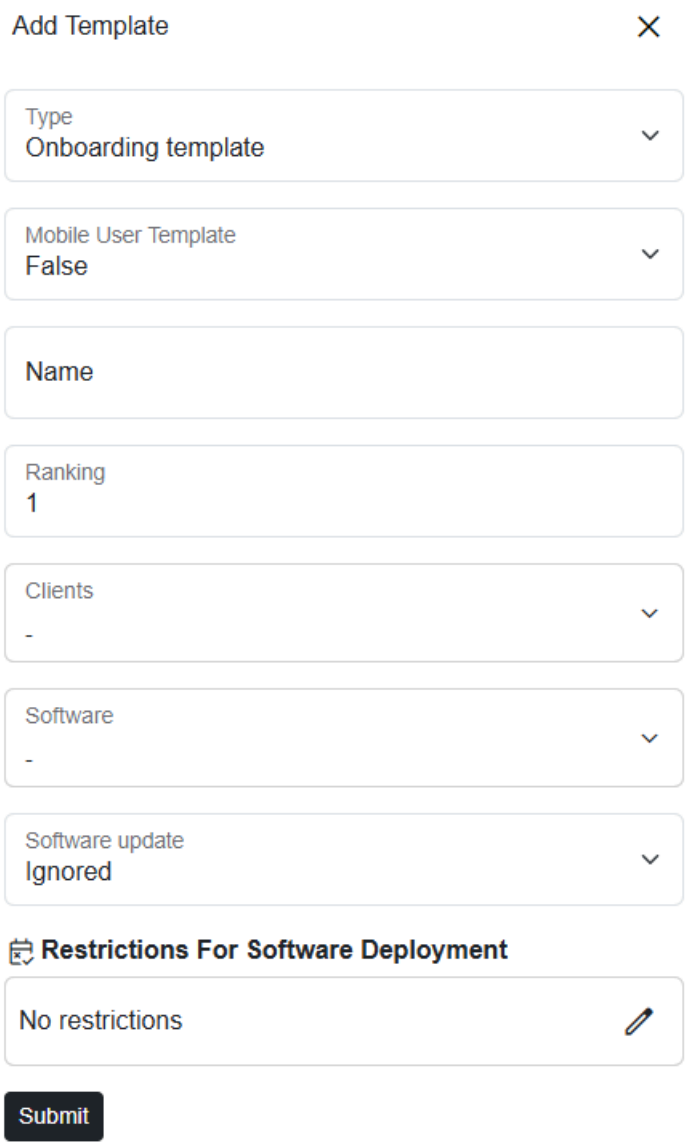
8.2.1 Template restrictions

As an administrator, you can allow users to define **software deployment restrictions** based on a **7-day schedule (Monday to Sunday)**.

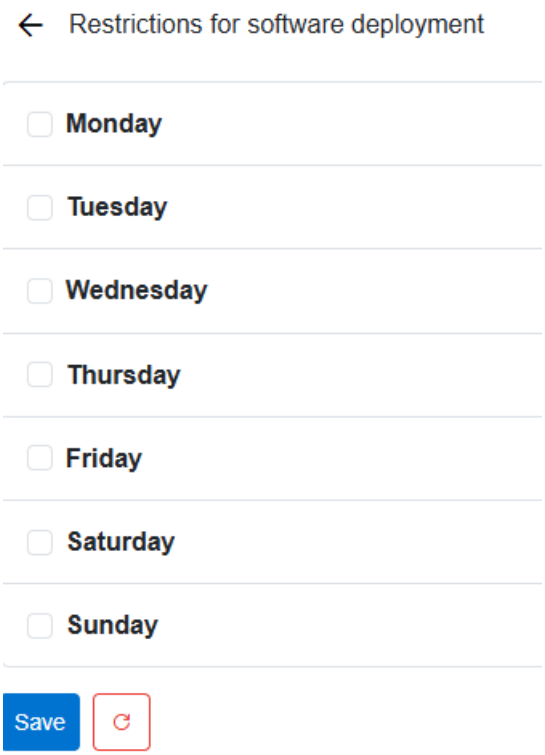
Restrictions can be configured in two ways:

- By specifying **time intervals** (e.g., `hh:mm - hh:mm`), or
- By marking an **entire day** as restricted.

Restrictions are created and managed through the **Template window**, where a summary of the current configuration is displayed.



Clicking on the **Edit** button opens an overlay window where intervals can be edited:



Within the overlay, users can:

- **Click on a day** without setting a time interval → the entire day will be restricted.
- **Click on a day** and define a specific time interval → restrictions apply only during that interval.
- **Click on an enabled day** again → all restrictions for that day are removed.

> **NOTICE:**
>
> Enabling restrictions for all seven days is not permitted, as this configuration is invalid.

8.2.2 Template Client Configuration

Similar to the direct Client you can view and manage the configuration of your template client by using the **Assign Configuration** section.

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

This is a central menu for displaying and administering clients' parameters. The **Configuration for client** section displays the following information:

- **Search function:**You can also use the**Search**area to find a specific configuration parameter of the client.
- On the top right corner, you can Submit your changes, Refresh data, or Discard changes.

- You can minimize the**Configuration for the client** window by using the minimization icon (_) on the top right corner of the window.

The Configuration for the client lists all configurable items for all OSEM-supported Clients. To get an insight into the Configuration items themselves, please refer to the Admin Guide for the specific client you would like to configure.

All Admin and User Guides for the Clients can be found in the Mitel Document Center .

For the E.164 Field and the MAC you can use variables as a wild card placeholder:

%%{variable,params}

Example: %%{e164,$-4}

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.

The **Files** tab displays the following information about files:

- **Filename** - the name of the file.
- **Storage** - the type of storage.
- **Type** - the file type.
  - **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.
- **Size** - the size of the file.
- **Supported clients** - the clients that the file is available for.
- **Software version** - the software version of the file.

9.1 Uploading a file

You can easily upload a new file to your OpenScape Endpoint Management app.

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.

9.2 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.
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 more easily.

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 **Storage provider** tab displays the following information about a provider:

- **Type** - OSEM support S3 or https as a file download server.
- **Name** - the name of the storage provider.
- **URL** - the IP Address or the URL of the storage provider.
- **HTTPS specific:**
  - **Username** - Your HTTPS user you have configured in your HTTPS server; leave empty if no username is used to secure the HTTPS server
  - **Password** - Your https password you have configured in your HTTPS server; leave empty if no password is used to secure the HTTPS server

  S3 specific:

  - **Access Key** - A unique, 20-character identifier (like a username), provided by your S3 server provider
  - **Access Secret** - A secret, 40-character alphanumeric string (like a password), provided by your S3 server provider
  - **Bucket Name** - A globally unique, user-defined name for a storage container in S3
  - **Region** - A geographical area where your S3 bucket and its data are physically located (e.g., us-east-1 for North Virginia or eu-central-1 for Frankfurt).

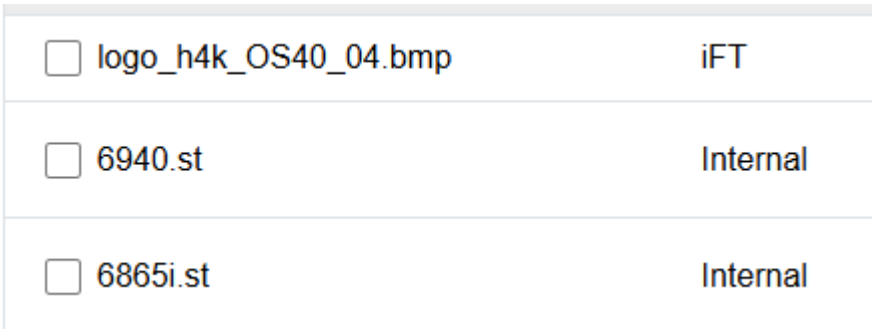
  After you enter all mandatory fields and before clicking submit, you can select whether to scan the file provider directly by enabling **Start Scan of Storage Provider.**

10.1 Scanning for a storage provider

You can scan your storage provider for new or changed files at any time by clicking and then selecting **Scan**; you need to confirm that you want to start the scan.

A running scan is indicated by the blinking circle next to the provider's name.

Once the scan has finished, OSEM will display the number of files it found and that are usable on the OSEM. The Scanned Files will show up under the Files Section of OSEM with the Provider name as a label.



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.

NOTICE: 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.
- **Truststore** - OSEM provides a Truststore for certificate storage. This Icon shows if the certificate is part of this storage.

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:

- **PKI Connector**
  - If “**Default Internal**” is selected, you have the following options:
    - **Certificate authority for signing**-select one of the available options from the dropdown list:
      - **Create a new certificate authority**
      - Or select one of the already available certificate authorities
    - **Certificate type**-the following options are available:
      - **Server certificate**
      - **Client certificate**
      - **Certificate authority**
    - **Subject**-click to edit the subject information:
      - **Common name**,
      - **Country**,
      - **Location**,
      - **Stateor province**,
      - **Organization**,
      - **Organizational unit**
    - **Subject alternative name information**-Subject alternative names can be specified as IPv4, IPv6 addresses, or DNS names. Use a comma as a separator when providing multiple entries. Example: 1.2.3.4,test.local
    - **Certificate lifetime**-select from the dropdown list. The offered time depends on whether you create a CA or a Certificate.
    - **Private key** - RSA-based key or EC-based key - locked to the key that is used by the selected CA
    - **RSA key length** or **Elliptic curve**
  - Alternatively, you can select any PKI Connector you have created under the **Connectors** section of the OSEM.
    - **Subject**-click to edit the subject information:
      - **Common name**,
      - **Country**,
      - **Location**,
      - **Stateor province**,
      - **Organization**,
      - **Organizational unit**
    -
    - **Subject alternative name information**-Subject alternative names can be specified as IPv4, IPv6 addresses, or DNS names. Use a comma as a separator when providing multiple entries. Example: 1.2.3.4,test.local
    - **Private key** - RSA-based key or EC-based key
    - **RSA key length** or **Elliptic curve**

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: Uploading certificates is only possible in PEM (.crt) or PKCS12/PFX (.pfx) format. A private key can only be uploaded via a PKCS12/PFX file.

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.

By clicking on the right of the certificate or CA, you can select to download the certificate or CA as PEM or PKCS12. PEM will only export the certificate or CA, while PKCS12 will download the certificate and CA with its corresponding key.

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 Connectors - PKI Connector Support

Creating a PKI Connector

OSEM supports **PKI Connectors**, which can be categorized into two types:

- **External Connectors** — based on **SCEP** and **NDES** protocols
- **Internal Connectors** — based on internal business logic

External PKI Connectors

External PKI Connectors manage the configuration of all certificate-related items, such as **extensions**, **subject** , **validity period**, and more. To manage these configuration items, please check the Admin Guide for our PKI Solution. In SCEP, you should find them under certificate profile, and in NDES, under certificate template. Using external connectors, OSEM only requests a certificate with a specific CN; all the configuration items are added externally

Internal PKI Connector

For the Internal PKI Connector, configuration items are set via the UI during Internal Connector creation.

11.5.1 Connector Configuration

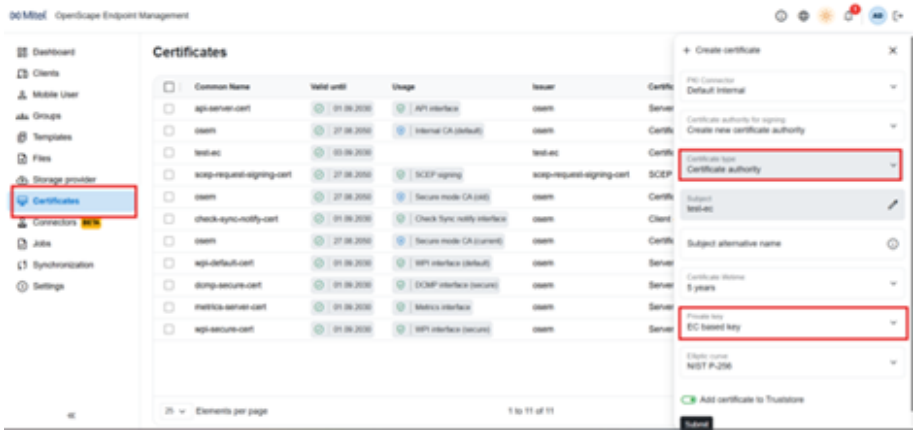
11.5.1.1 Instructions for Internal Connector

You can easily create certificates on your OpenScape Endpoint Management administration app.

Step by Step

1) Select **Certificates** from the left menu to create a root CA certificate.
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:



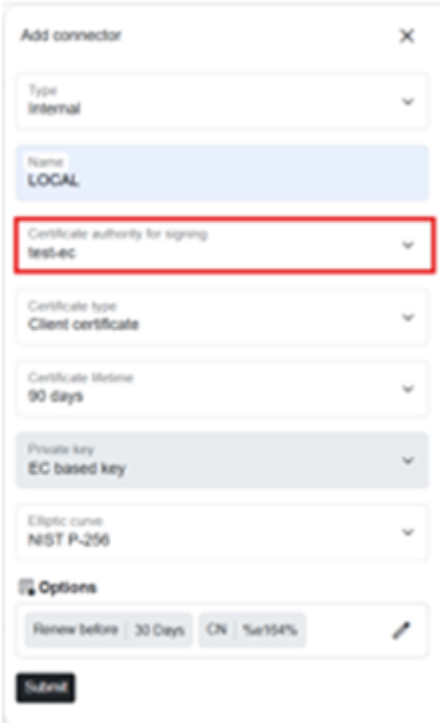
NOTICE: The Private Key type will be extended to all certificates signed by this CA. Therefore, the subsequent Connector type will require this Private Key type.

3) Click **Submit** to create the certificate.

4) Select the **Connector** area in the left side menu

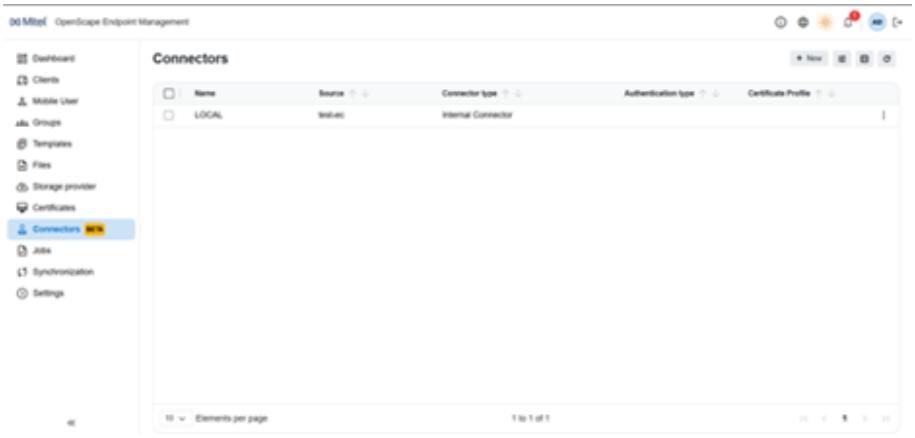
5) Click **+New** at the top right part of the screen.

6) Set the type as **Internal** and fill in the following details:



- **Type**: Internal - for Internal PKI Connector;
- Simple Certificate Enrolment Protocol - for SCEP;
- Network Device Enrollment Service - for NDES.
- **Name**: The internal name, something meaningful, what this connector is about.
- **CA for signing**: The CA certificate created in step 2.
- **Certificate lifetime**: The number of days the created certificates will be valid.
- **Private Key**: The Private key type that the created certificates will have.
- **Eliptic curve**: The Eliptic curve that the created certificates will have.
- **Options**: Used internally by OSEM for: Renew before - used to trigger a renewal certificate job;
- **CN** (Common name): CN in the certificate request.

7) Click **Submit** to create the connector and your PKI Connector should be displayed in the table.



The newly created PKI connector should be visible in the connectors list.

11.5.1.2 Instructions for External Connector

You can easily create certificates on your OpenScape Endpoint Management administration app.

Step by Step

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

2) Click **+New** at the top right part of the screen.

You can either select **Simple Certificate Enrolment Protocol** or **Network Device Enrollment Service**
A right side menu is displayed and you can configure the following fields:

- For SCEP select the type as **Simple Certificate Enrolment Protocol**.

The inputs are explained below

Name: The internal name, something meaningful, what this connector is about.

Address: The URL of the SCEP server.

Certificate Profile: If you have certificate profiles in your SCEP, specify one; otherwise, leave it empty.

Authentication type: None - for no authentication; Challenge - if you are using a challenge password.

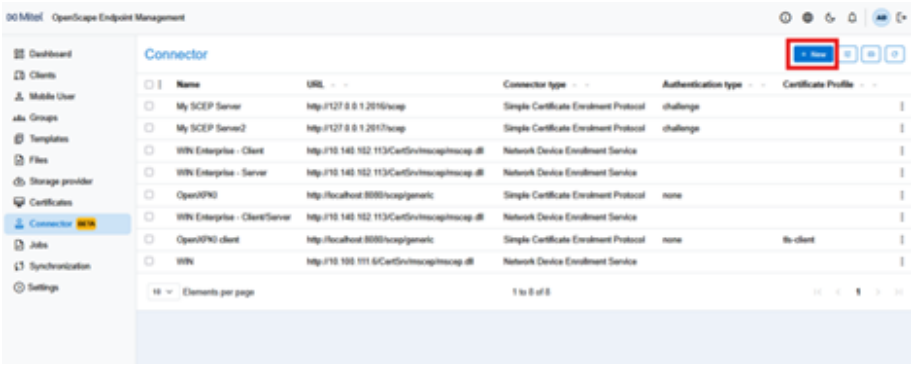
Options: Used internally by OSEM for: Renew before - used to trigger a renewal certificate job; CN - used to be able to customize the CN in the certificate request.

11.5.2 OSEM and NDES

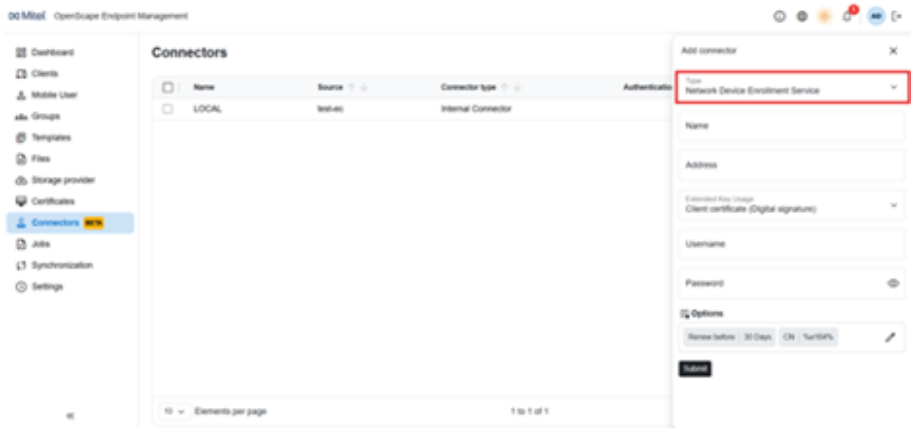
In this section you can find detailed explanations about using Network Device Enrollment Service in OpenScape Endpoint Management administration app.

Step by Step

1) Select **Connectors** from the left menu.
   A list of existing connectors is displayed (if any).
2) Click **+New** at the top right part of the screen.



3) Select **Network Device Enrollment Service**
A right side menu is displayed and you can configure the following fields:



- For NDES select the type as **Network Device Enrollment Service**. The inputs are explained below:

  Name: any name to refer to the adding Connector.

  Address: the NDES server URL. For example: http://<ip>/mscep/mscep.dll. It must end with '/mscep/mscep.dll'.

  The **Extended Key Usage**: the purpose of the certificate that this NDES generates. OSEM uses it to define the Certificate Type.

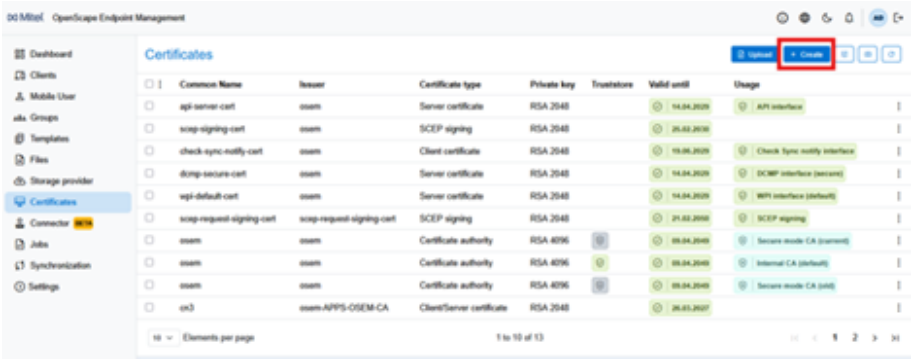
  Username: the NDES User username created in the Domain Controller machine. It is used to get the challenge.

  Password: the password of the aforementioned NDES User.

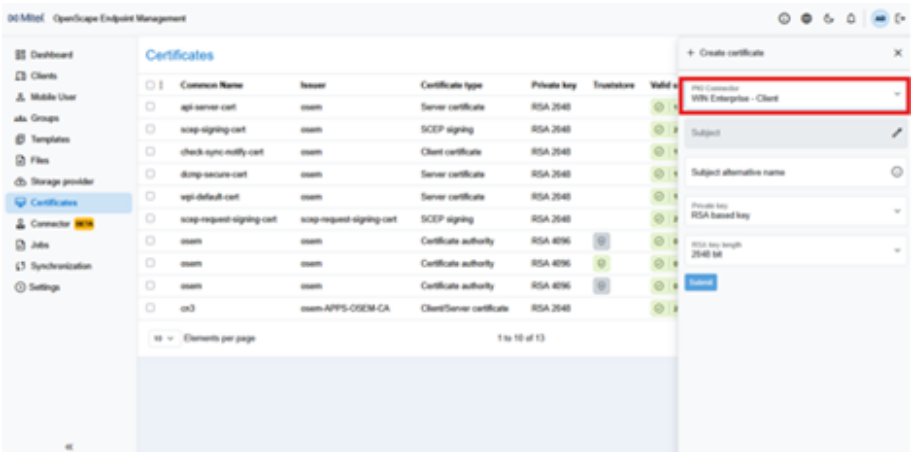
  Options: Used internally by OSEM for: Renew before - used to trigger a renewal certificate job; CN - used to be able to customize the CN in the certificate request.

4) **Enrol for a certificate using the NDES**.

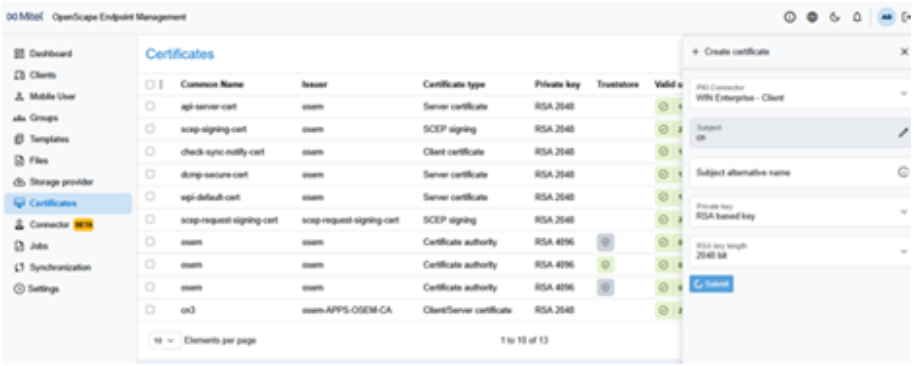
5) Go to the **Certificates** page and click on the **Create** button.



6) Select the created PKI Connector, in this case, the previously created NDES Server.

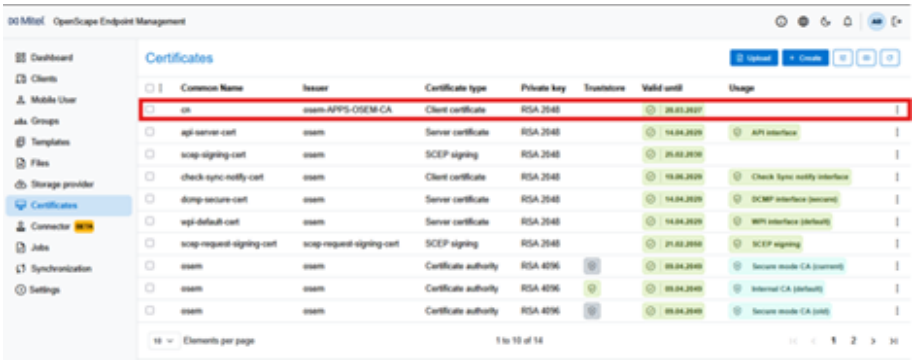


7) Add the certificate configurations



8) Click **Submit**.

If successful, you will see the Certificate appear like any other certificate.

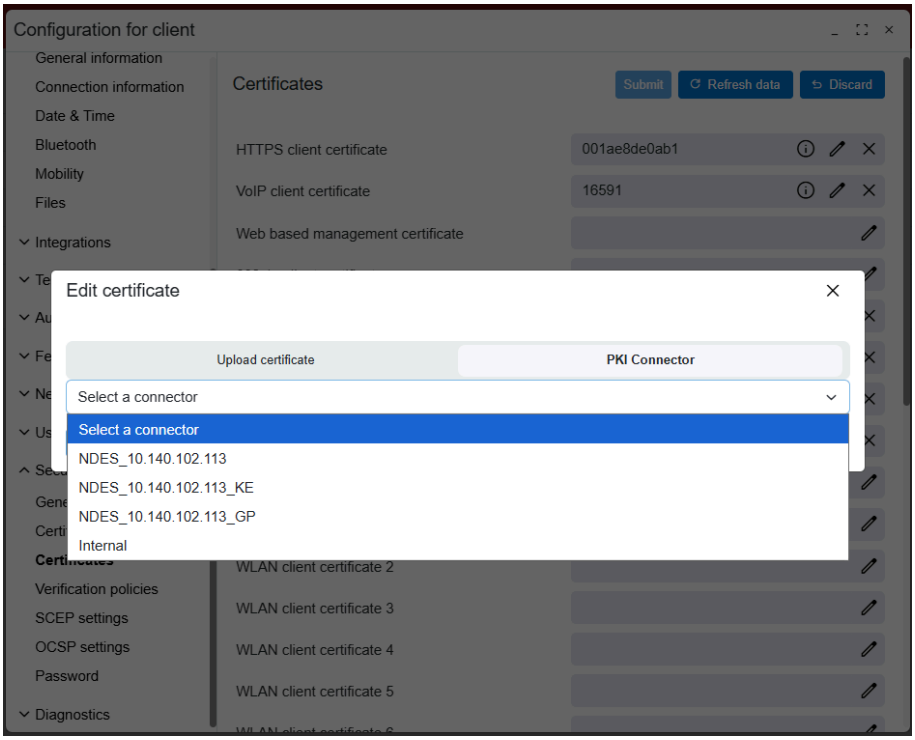


11.5.3 Adding a certificate to a client using a PKI Connector

Adding a certificate to a client through a PKI Connector has been simplified. The dedicated **Connectors** tab is now available in the **Edit Certificate** section.

The process for assigning a certificate using a PKI Connector is outlined below:

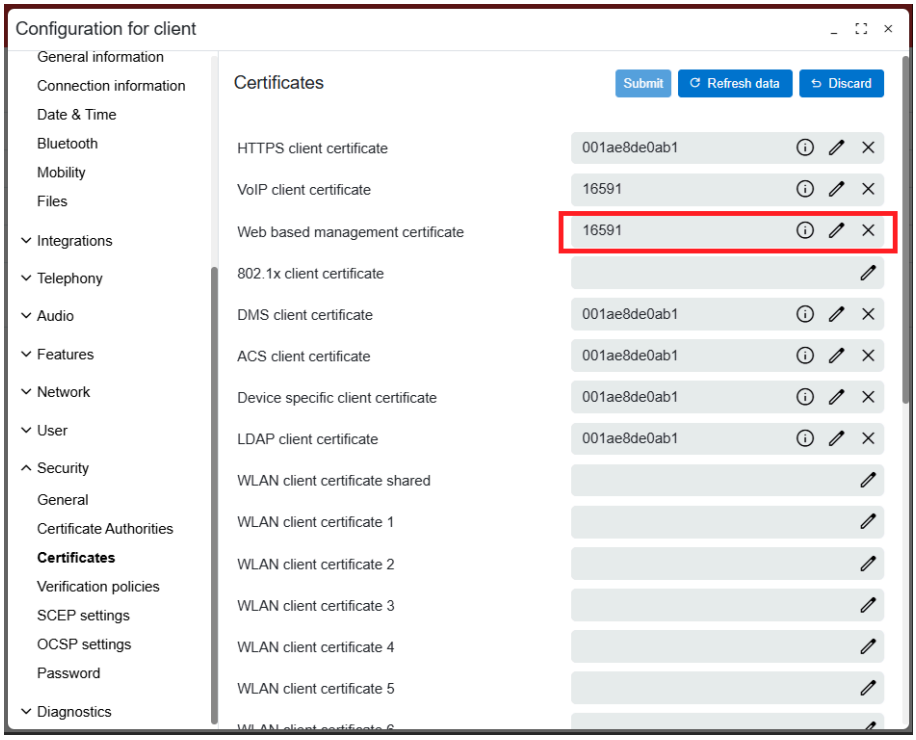
1) When a PKI Connector is selected and submitted through a client interface (e.g., Web-based Management Certificate), the interface retains the PKI Connector details until the client communicates with OSEM.



2) A Write Configuration job is created in OSEM, waiting for the client to communicate.

3) When the client communicates, OSEM will request a certificate from the PKI Connector (CN=e164 if available, if not, the MAC address will be used).

4) With the certificate acquired from the PKI Connector, OSEM saves it in the Certificates database and writes it to the phone. Client Configuration will now show the certificate instead of the Connector.

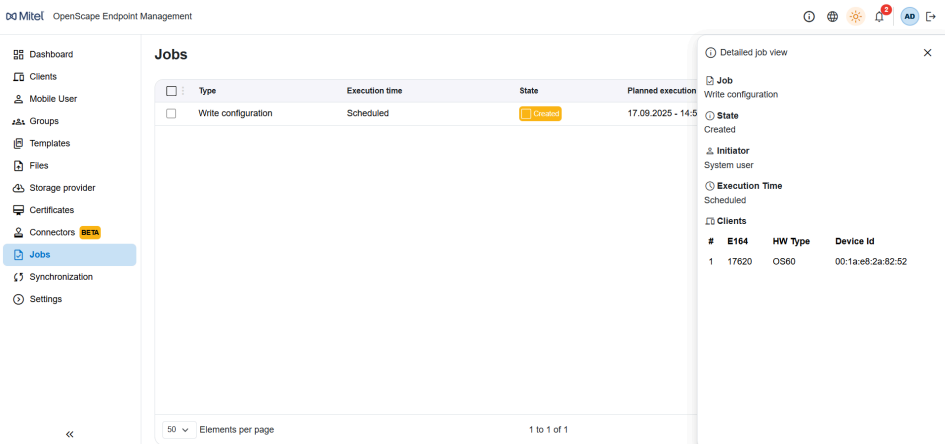


11.5.4 Automated Certificate renewal

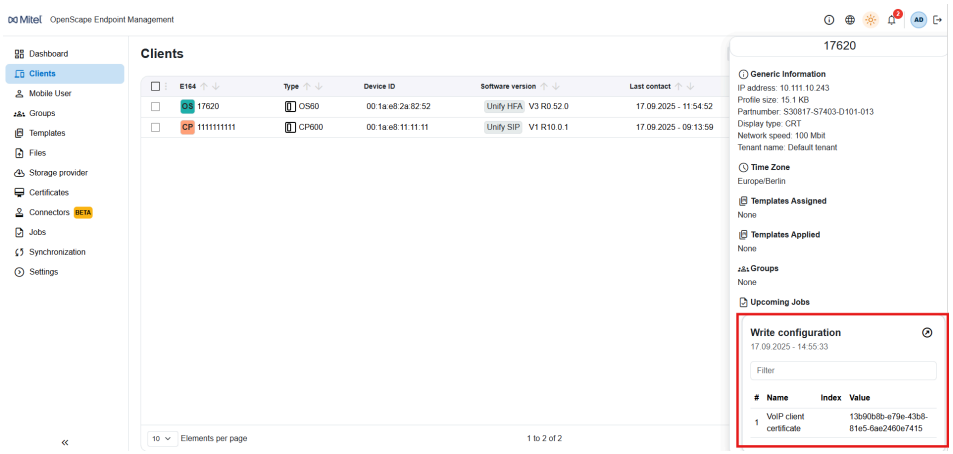
Certificate renewal for clients is automated in OSEM. The **Renew before** parameter defined during Connector creation is read, and if a certificate is nearing expiration, a renewal job is automatically triggered.

If the expiring date is less than 24 hours, the renewal job runs immediately. Otherwise, the job is scheduled at a random time during the day. After the renewal is completed, the old certificate is automatically deleted.

The scheduled job can be viewed in the **Jobs** area:



It can also be checked in the **Client > Features > Info** section.


Mitel OpenScape Endpoint Management
Dashboard
Clients
Mobile User
Groups
Templates
Files
Storage provider
Certificates
Connectors BETA
Jobs
Synchronization
Settings
Clients
E164
Type
Device ID
Software version
Last contact
OS 17620
OS60
00:1a:e8:2a:82:52
Unify HFA V3 R0.52.0
17.09.2025 - 11:54:52
CP 1111111111
CP600
00:1a:e8:11:11:11
Unify SIP V1 R10.0.1
17.09.2025 - 09:13:59
10 Elements per page
1 to 2 of 2
17620
Generic Information
IP address: 10.111.10.243
Profile size: 15.1 KB
Partnumber: S30817-S7403-D101-013
Display type: CRT
Network speed: 100 Mbit
Tenant name: Default tenant
Time Zone
Europe/Berlin
Templates Assigned
None
Templates Applied
None
Groups
None
Upcoming Jobs
Write configuration
17.09.2025 - 14:55:33
Filter
Name
Index
Value
1 VoIP client certificate
13b90b8b-e79e-43b8-81e5-6ae2460e7415

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 more easily.

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

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.
- **Initiator** - displays the user who triggered the job. You might see jobs triggered by the “System user”; this is the internal process of the OSEM itself and mainly shows up for any automation triggers, like **automatic mobile user logoff**.

12.1 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.
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.

13 Synchronization

You can schedule recurrent synchronizations between OpenScape Endpoint Management and OpenScape 4000 or OpenScape Voice systems. The operation will add Plug & Play softphones or hardphones based on the user's preferences.

You can refresh the list of the synchronized systems at any time by clicking at the top right of the screen.

NOTICE:

If you enable synchronization and you already have clients registered in the OSEM that overlap with the numbering of the synchronized clients, you will see ‘duplicate’ entries.

NOTICE:

Syncronized Plug & Play Devices will stay in the Client List after usage, their profile will automatically deactivate. If you don’t like to see the Profiles you can use a filter to hide them.

OSEM uses the Element Manger Function and API of the PBX Systems therfore OSEM needs to be either manually triggered to sycnrozie configuration changes or a shedule for automatic syncronization has to be set.

13.1 OpenScape Voice Synchronization

As an administrator, you can schedule a recurrent synchronization for OpenScape Voice.

Step by Step

1) Click **+New** on the left menu.
   You are navigated to the **Add system for synchronization** area and you can add a new system.
2) Configure the following settings:
   - **Type** – The Type of the System that you want to connect to.
   - **System Name** – A free text field where you can give the connection a name to make sorting easier for your needs.
   - **CMP address** – the IP or DNS of the system that you want to connect to
   - **User name** & **Password**– The User and Password you configured on the PBX that will be used for the synchronization.
   - **Switch Name** - Please set a switch name if multiple switches are being managed via the same Common Management Portal. If left empty,

the first switch name provided from the list of switches will be set automatically.

- **Frequency of synchronization**:
  - **Scheduled** – Allows the scheduling by day of the week and time of the day. Time set as 24h. e.g 0 hours o Minutes is Midnight.
  - **Recurrent** – Allows automatischeduling by Minutes.
- **Create Plug&Play Profile for Softphone** – select if you like to add the synchronized Plug & Play profile for SoftClients like OpenScape Fusion.
- **Create Plug&Play Profile for Hardphone** – select if you like to add the synchronized Plug & Play profile for Desk Phones, like OpenScape CP devices.
- **Create number pool profiles** – marks all syncronized elements as pool profiles they are stored and marked as available for assignment. When a new Plug & Play device is registered and set to use a number pool, it can automatically take an available number and configuration from these pool profiles.

3) Click **Submit**.

After clicking the **Submit** button, OSEM will try to contact the OpenScape Voice. If successful, a new tab will appear asking you to select the Business groups that you would like to use from synchronization. If none are selected all avalible Business groups will be synchronized.

13.2 OpenScape 4000 Synchronization

As an administrator, you can schedule a recurrent synchronization for OpenScape 4000.

Step by Step

1) Click **+New** .
You are navigated to the **Add system for synchronization** area and you can add a new system.

2) Configure the following settings:

- **Type** – The Type of the System that you want to connect to.
- **System Name** – A free text field where you can give the connection a name to make sorting easier for your needs.
- **Assistant address** – the IP or DNS of the system that you want to connect to
- **User name** & **Password**– The User and Password you configured on the PBX that will be used for the synchronization.
- **Prefixesconfigured**:
  - **Node ID** & **Prefix** - During synchronization, the system checks the device's Virtual Node ID (node_id) and looks for a matching entry in the configured prefix list. If a match is found, the corresponding prefix is prepended to the device's extension number. This ensures

that each device gets the correct full number based on its node association.

- **Frequency of synchronization**:
  - **Scheduled** – Allows the scheduling by day of the week and time of the day. Time set as 24h. e.g 0 hours o Minutes is Midnight.
  - **Recurrent** – Allows automatischeduling by Minutes.
- **Create Plug&Play Profile for Softphone** – select if you like to add the synchronized Plug & Play profile for SoftClients like OpenScape Fusion
- **Create Plug&Play Profile for Hardphone** – select if you like to add the synchronized Plug & Play profile for Desk Phones, like OpenScape CP devices.
- **Set prefix for SIP devices** – If enabled, the prefix is prepended to the extension for SIP devices, just as it is for other device types. If disabled, SIP devices will use their extension number without a prefix, regardless of the node's prefix settings. This allows you to control number formatting for SIP endpoints separately from other device types.
- **Create number pool profiles** – marks all syncronized elements as pool profiles they are stored and marked as available for assignment. When a new Plug & Play device is registered and set to use a number pool, it can automatically take an available number and configuration from these pool profiles.

14 Multi-Tenancy in OpenScape Endpoint Management

The **multi-tenancy** feature in OSEM enables administrators to manage configurations and resources for multiple tenants (organizations or customers) within a single deployment. Each tenant has its own isolated data and configuration, ensuring clear separation and enhanced security.

When multi-tenancy is enabled, resources such as **clients**, **templates**, **groups**, and **files** are logically separated between different organizations.

OSEM supports both **single-node** and **multi-node (clustered)** deployments, allowing multiple customers to be served securely from a shared infrastructure.

Access to OSEM is password-protected. The multi-tenancy model further improves security by isolating data between tenants, preventing cross-tenant access.

Tenant Management

Only the user with the **default admin role** can create and manage tenants in OSEM.

Each tenant has its own **tenant administrator**, who serves as the equivalent of the system administrator but has access limited to that specific tenant. The tenant administrator can perform administrative tasks such as creating additional administrator accounts within their tenant.

Similarly, the **tenant manager** role corresponds to the server administrator but is restricted to managing resources belonging to the tenant only.

Data Management and Tenant Lifecycle

- When a **new tenant** is created, existing data (clients, users, groups, tenants) cannot be moved into it. Such data remains in the **default tenant**, and new entities must be created manually within the new tenant.
- When a **tenant is deleted**, the system administrator can choose to either:
  - Permanently delete all associated tenant data, or
  - Move the data back to the **default tenant**.

Client-to-Tenant Assignment

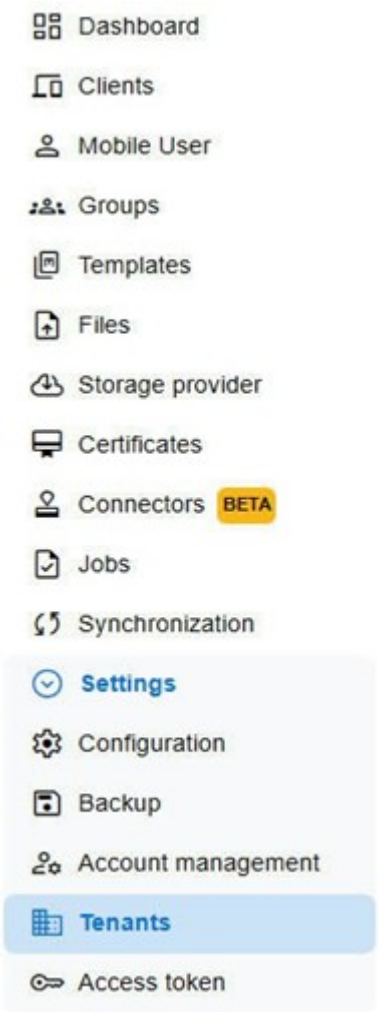
When clients connect to OSEM, the system determines which tenant each client belongs to. This assignment can be based on one or more of the following criteria, depending on tenant configuration:

- **E.164 number**
- **IP address**
- **Server address** (configured on the device)

NOTICE: Only Clients that are not yet registered with the OSEM are automaticly assigned to a Tenant. If a client is already registered with the OSEM before the Tenant was created, then you will have to remove the Client from the OSEM and trigger a new registration.

If a client is not yet associated with any tenant, OSEM attempts to assign it automatically by:

1) Comparing the client's attributes against the tenant's matching criteria (E.164 number, IP address, server address).
2) Using the **tenant ID** from a matching plug-and-play profile.



When a client is configured with an E.164 number for the first time and has not been assigned to a tenant yet, OSEM re-evaluates the assignment.

Once a client has been assigned to a tenant, **it cannot be moved** to another tenant.

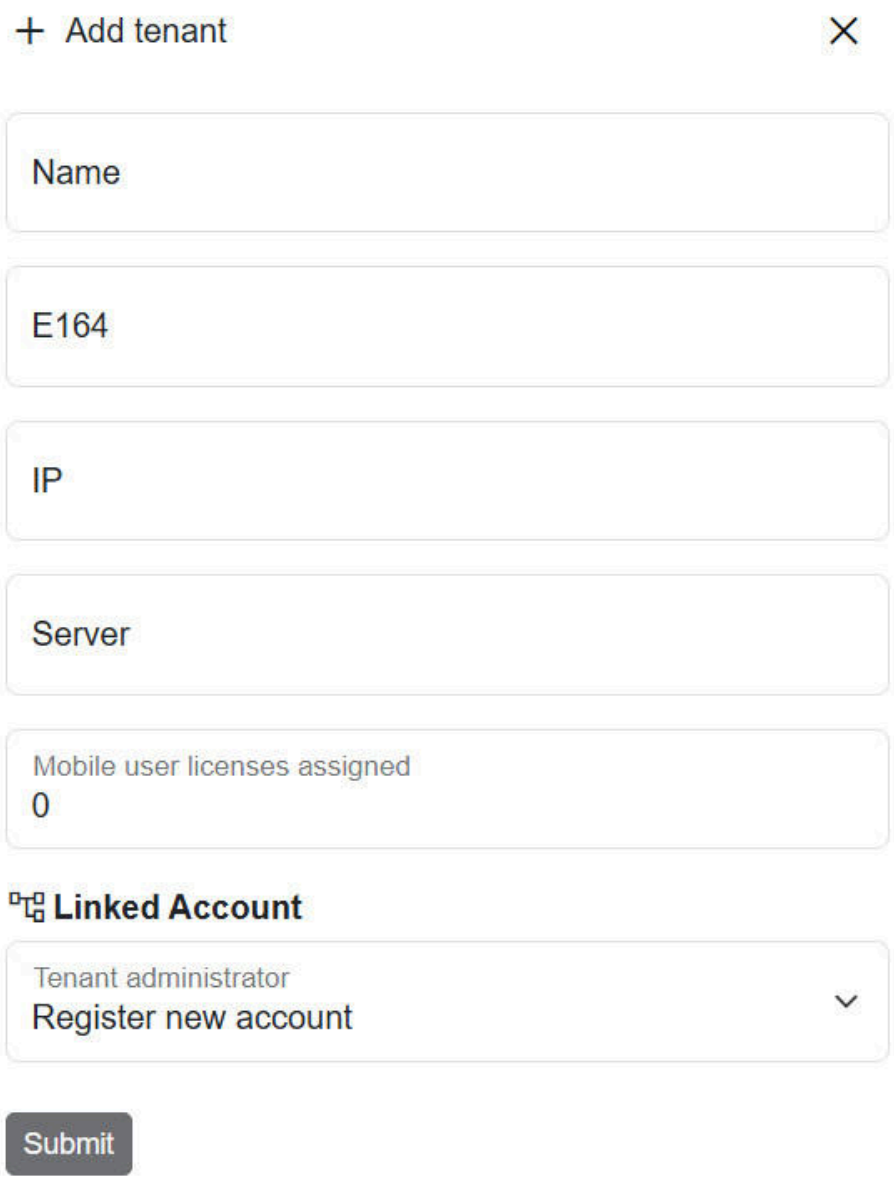
14.1 Create a Tenant

To create a new tenant as a system administrator follow the next steps:

Step by Step

1) Navigate to the **Tenants** section under Settings.

2) Click the **New** button to start the tenant creation process.



3) Enter the required tenant details. Clients can be assigned to this tenant based on E.164 number, IP address range, or server address. If multiple criteria are defined, all must match for a client to be assigned to the tenant. All input fields support regular expressions, allowing flexible matching for client identification.You can either select an existing tenant administrator account from the dropdown list (the account must not be assigned to another tenant) or create a new administrator account during the tenant creation process.

A newly created tenant administrator is required to change the password at first login, similar to any newly created user account. A yellow icon indicates that the user is logged in with a tenant account.

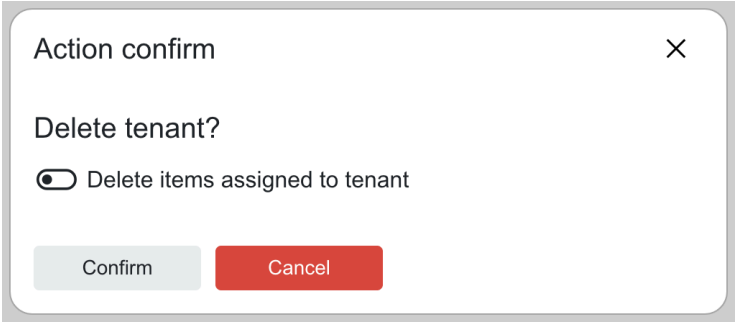
14.2 Delete a Tenant

When deleting a tenant, you can choose to remove all data associated with that tenant, including all administrator accounts.

Step by Step

1) Navigate to the **Tenants** section under Settings.

2) Select the tenant you want to delete.



The tenant will not be displayed in the list.

15 Backup/Restore

OSEM provides the option of backing up and restoring DB data.

The backup can be triggered either:

- manually, by the user
- automatically, by scheduling a backup
- automatically by other parts of the code when performing certain operations

Restore is available by:

- uploading a backup
- restoring from a stored backup file

Backups will be stored in a directory and referenced by DB entries. The UI will allow the user to see all available backups, filter backups, restore from backups, trigger a backup, and modify the backup schedule.

Every database except the “Backup” database itself can be exported. From a UI perspective, DBs will be grouped in topics:

- Clients
  - clients, items, diagnostics
- Users
  - users
- Groups and Templates
  - templates, groups
- Files
  - providers, files
- System
  - config, jobs, certificates, admins*, tokens, licenses

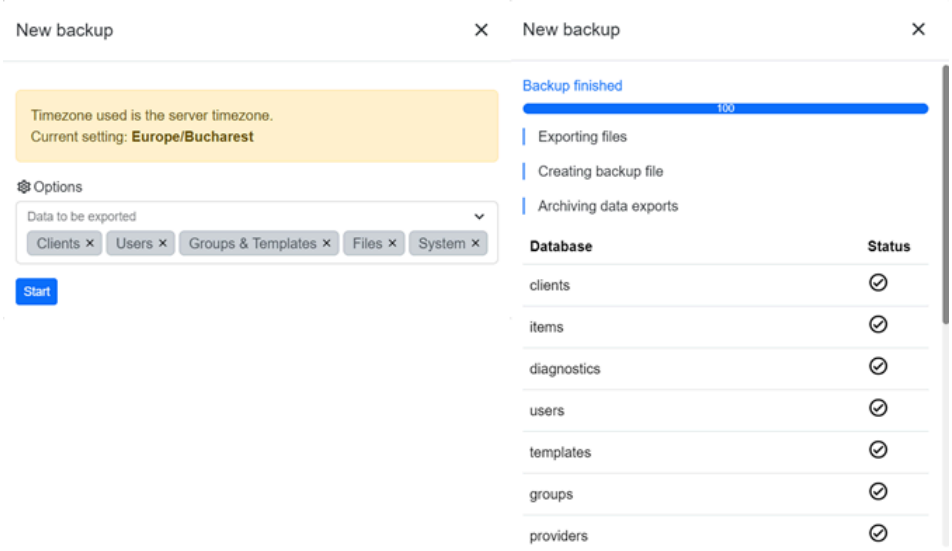
*The ‘Default admin’ is excluded from the exports and will not be overwritten or changed when restoring a Backup.

Each backup has four options:

- a detailed view of the backup
- the option to download the backup file
- the option of restoring from an existing backup
- the option of Reset and restore
- option to Delete

15.1 New backup

The user will have the possibility of triggering a backup via the header button. After selecting the table topics to be exported, the process should start, and the SSE should keep the UI up to date with the backup process.



Step by Step

1) Click **Backup** on the left menu.
You are navigated to the **New Backup** area and you can create a new backup.

2) Select the data to be exported. Database tables are grouped in "topics" as follows (topic - tables to be exported):

- Clients ("clients", "items", "diagnostics")
- Files ("providers", "files"). The files topic includes the files folder containing all the files sorted in OpenScape Endpoint Management.
- Groups ("templates", "groups"),
- System ("config", "jobs", "certificates", "admins", "tokens", "licenses", "synchronization") The system topic does not include 'dcmp-url'.
- Users ("users") The users topic does not include the admin account.
- Password: the password topic is only necessary if the backup needs to be encrypted. It is not possible to import from this backup if you can't remember your password.

3) Click **Start**,

After clicking the **Start** button, a progress bar is displayed with more information about the status.

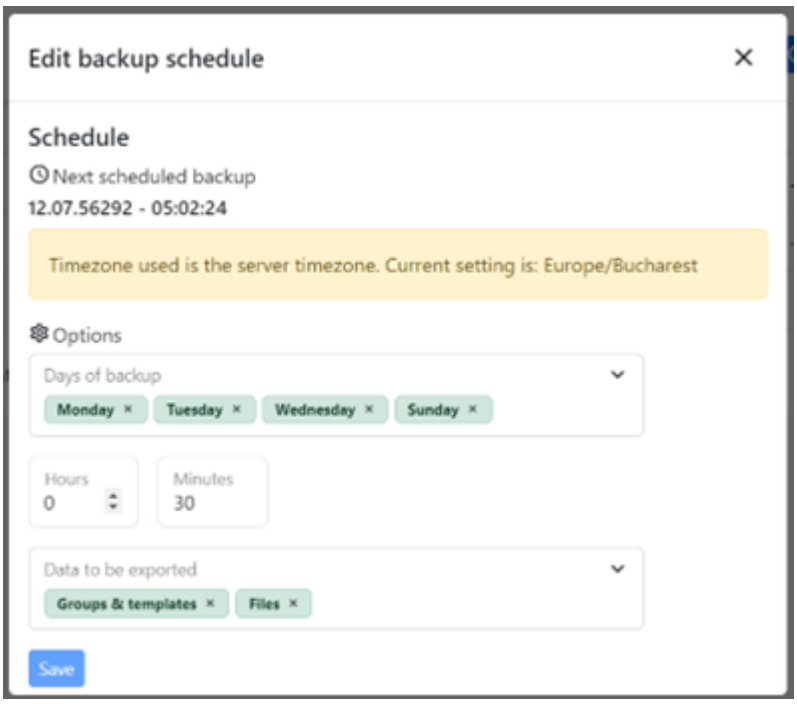
15.2 Scheduler

The user will also have the possibility of changing the scheduled backup behavior. The options provided will be:

- days of backup, Mo to Su
- hour and minutes
- table topics to be exported

Date/ time used in the backup/ schedule process will be according to the timezone of the OSEM, configurable from Configuration → Other. The user

is notified via a small component. Implementation details can be found in the *Implementation Details* section.



You can schedule backups of the OpenScape Endpoint Management database.

Step by Step

1) Click **Schedule** on the left menu.
   In this area you are informed of the next scheduled backup.
   You are navigated to the **Edit backup schedule** area and you can schedule a new backup.
2) Select the days, hours and the data for scheduling the backup.
3) Click **Save**.

15.3 Restore/Reset and restore

The user can restore or reset and restore from an existing backup.

When **restoring, any table that is not part of the backup will be left untouched**.

When **resetting and restoring, any table that is not part of the backup will be deleted and recreated**.

15.4 Encryption

The data.zip file is encrypted by default. The user can provide their own private password.

- In the scheduler, the value will be stored as a backup-schedule-password in defaults.js.

- Part of the API request when creating a new backup.

16 OpenScape Endpoint Management Configuration

You can configure your OpenScape Endpoint Management administration app from the **Settings -> Configuration** tab.

The **Configuration** tab allows you to configure the following options on your administration app:

- **Clients** - configure the app for
  - Mitel client options,
  - Unify client options,
  - Mediatrix client options.
- **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.
  - **TLS Settings**
  - **Common Security Settings**

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).

16.1 Support of Mitel 6900 & 6800 IP phone series

16.1.1 Onboarding prerequisites

Before you begin, ensure the following settings are configured in your OSEM system under Settings > Configuration > Clients > Mitel Client Options:

- **Enable STUN connectivity service**: YES
- **Enable Multicast DNS service discovery**: YES
- **Automatic installation of Mitel SIP software**: YES
- **Plug&Play via E164 number for Mitel devices**: YES

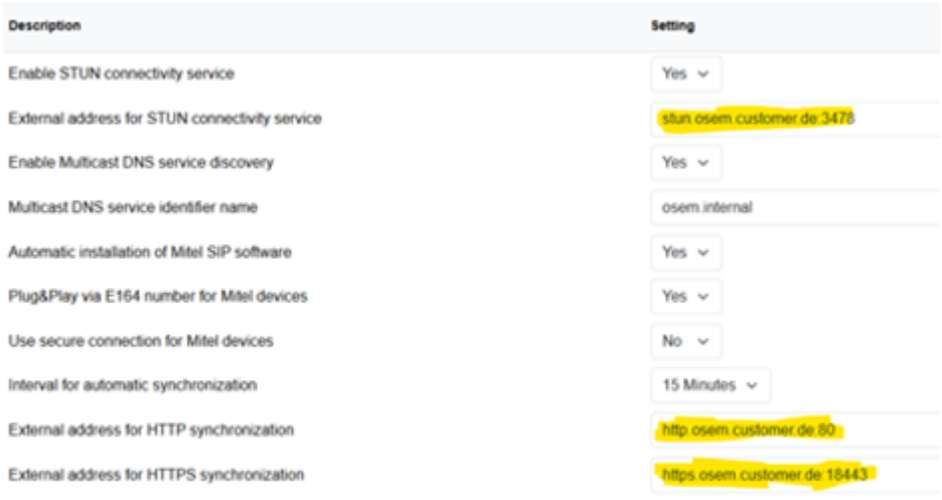
Description	Setting
Enable STUN connectivity service	Yes
External address for STUN connectivity service	
Enable Multicast DNS service discovery	Yes
Multicast DNS service identifier name	osem.internal
Automatic installation of Mitel SIP software	Yes
Plug&Play via E164 number for Mitel devices	Yes
Use secure connection for Mitel devices	No
Interval for automatic synchronization	15 Minutes
External address for HTTP synchronization	
External address for HTTPS synchronization	

Depending on your network setup, OSEM will either use TR-069 or STUN for connecting to the device.

In standard routable networks, TR-069 will be used to contact the device. Depending on the automatic synchronization interval setting, the device will additionally contact OSEM.

In case OSEM cannot reach the device directly, e.g., when the device is behind NAT, STUN will be used to keep the connection open between the device and OSEM.

By default, the default IP addresses of OSEM are assigned for the TR-069 and STUN connections. In case you have home worker phones to connect to OSEM, you must provide a public IP or FQDN that forwards traffic from the public network to OSEM.



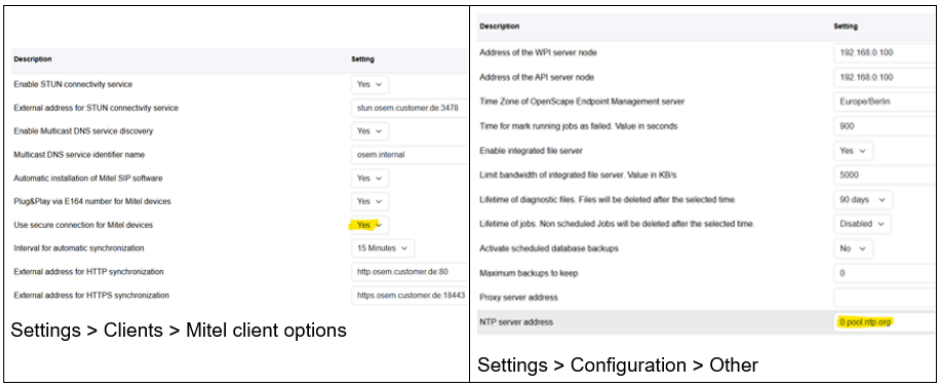
Description	Setting
Enable STUN connectivity service	Yes
External address for STUN connectivity service	stun.osem.customer.de:3478
Enable Multicast DNS service discovery	Yes
Multicast DNS service identifier name	osem.internal
Automatic installation of Mitel SIP software	Yes
Plug&Play via E164 number for Mitel devices	Yes
Use secure connection for Mitel devices	No
Interval for automatic synchronization	15 Minutes
External address for HTTP synchronization	http.osem.customer.de:80
External address for HTTPS synchronization	https.osem.customer.de:18443

The FQDN configuration below is just an example. The external ports can be changed; you can see the default ports of the interfaces above.

In case you want to change from the default HTTP port 80 to a different port, change the external address for HTTP synchronization and forward the external traffic from this new port to the OSEM port 80.

In case you want to use secure communication between OSEM and the device, a few things must be taken into account.

Enable secure connection for Mitel devices and configure a valid NTP server that will also be configured on the Mitel devices.



If you also plan to use external access to OSEM, remember to create new certificates for the relevant interfaces (WPI default), which include the external address as a subject alternative name (SAN)

NOTICE: The Mitel phone must be running SIP firmware that supports **Autodiscovery via Multicast DNS (mDNS/ Plug&Play)**, i.e., version 6.0.0 or newer for both Mitel 6800 and 6900 series phones. Other options are configuring the OSEM IP via DHCP option 66 or manual configuration.

16.1.2 Onboarding steps

Perform a factory reset on the phone via the WBM and restart the device.

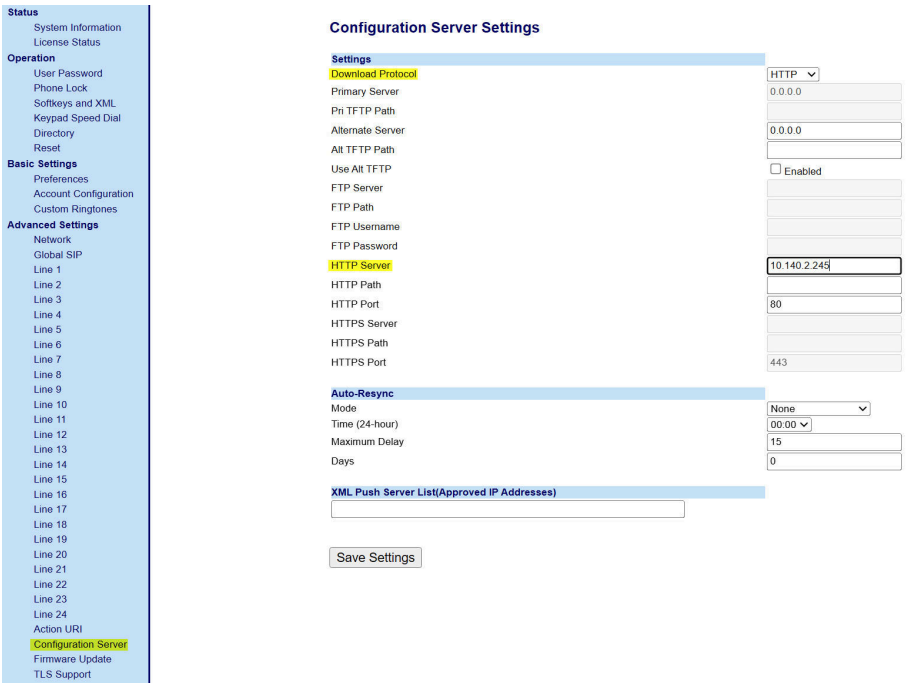
If auto-discovery is not working, you must configure the phone with the IP address of the OSEM server.

This can be achieved either via the phone's Web-Based Management (WBM) interface or via the phone menu as described below.

Step by Step

1) **Using the phone WBM**: In the WBM, navigate to **Configuration Server Settings**.
2) Set **Download Protocol** to HTTP.

3) Enter the OSEM IP address under **HTTP Server**.

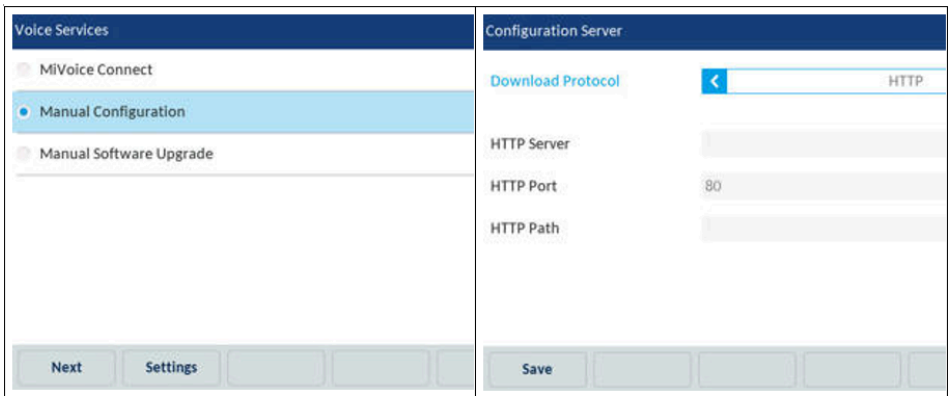


The device will reboot automatically.

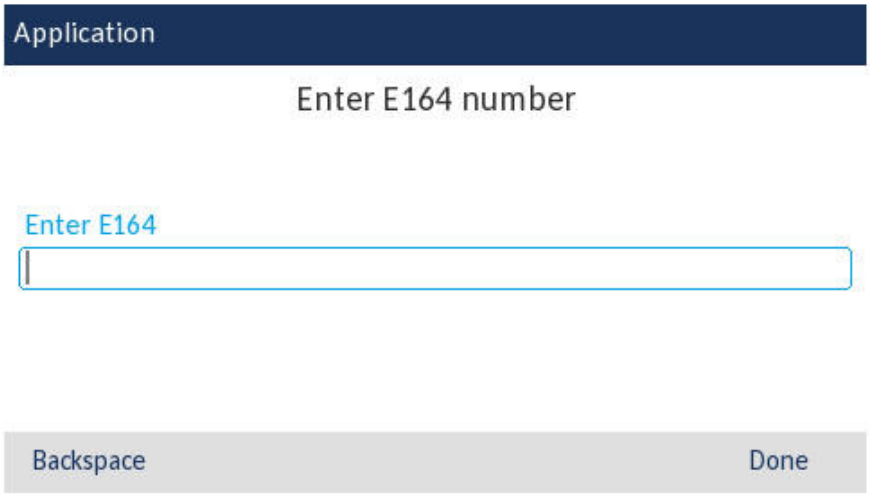
4) **Using the On-Screen menu**

The device will reboot automatically.

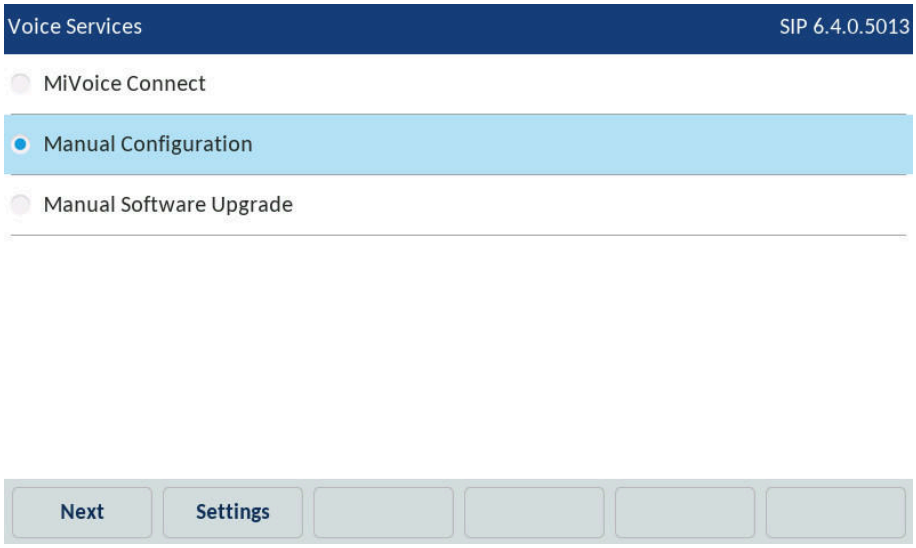
You can also configure the OSEM IP address on the on-screen menu of the device, in case the auto-discovery functionality did not work.



5) If the device does not have a Plug&Play profile that assigns a phone number automatically, you will be prompted to enter the E. 164 number on the device.



6) This configuration can be done also via the phone menu directly. In the Voice services prompt select **Manual configuration**



16.2 Devices Contact-Me Proxy – DCMP

For DCMP, you can set the following configurations:

- **Devices Contact-Me Proxy (DCMP) operational mode**
  - **Disable** – disabled DCMP OSEM wide
  - **Automatic** – OSEM uses internal automatic mechanisms to check if the DMCP protocol has to be used for each client. If OSEM can not contact the Client directly, DMCP will be set.
  - **Enabled** – DCMP will be enabled system-wide for each client connected to the OSEM

- **Address of the DCMP server node** – this configuration item reflects the interface address where OSEM accepts incoming connections from clients and devices. The address can be configured during the initial setup wizard.

  The item can be configured as an IP address or a DNS name.

  In most cases, an IP address will be used. If you want OSEM to be reachable via an internal (non-public) DNS name, you need to configure that DNS name as the address of the DCMP server node. Remember also to configure the same DNS name for the address of the WPI server node (Settings -> Configuration -> Other)
- **DCMP interval for device queries. Between 1-1440 minutes** – Interval that is used by the Client to contact the DMCP to check if new jobs are available.
- **Run DCMP server via TLS** – If the Client supports TLS connection, you can switch it on; please note that none of the Unify Desk Phones support DCMP via TLS
- **External address of the DCMP server node** – URL or IP of the DCMP server. You can set a different port than the default port 80, e.g, osem.unify.com:5561 or 88.201.211.210:7612

16.3 Licensing

As mentioned in section License information on page 8, OSEM can currently be licensed only via the Cloud CLA.

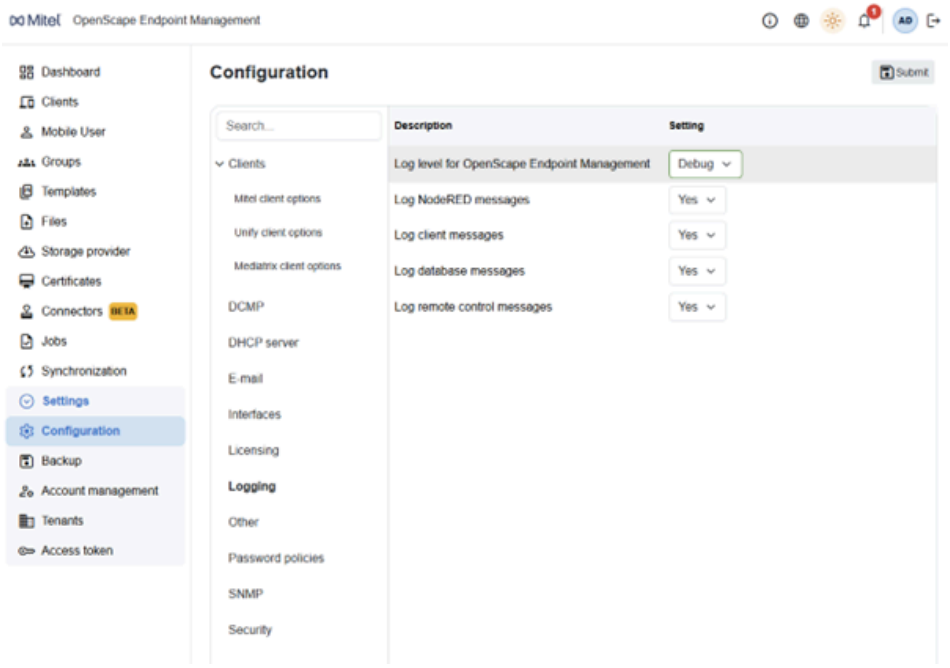
The **License Locking ID** is automatically generated based on uniquely identifiable hardware and software parameters of the machine you install OSEM on.

After you create your License in the Licensing Portal, you need to enter your **Cloud License Key** in the corresponding field.

Validate license agent connection is secure - When enabled, OSEM will validate the secure TLS connection to the licensing server. By default, OSEM uses the cloud-based licensing server and has the issuing CA certificate of this server hard-coded for validation. When disabled, the secure TLS connection is no longer validated.

16.4 Logging

Within the OSEM UI, you can set the Log Level via **Settings -> Configuration -> Logging**.



Log level for OpenScape Endpoint Management lets you set the log level.

The only Log Level required for Error analysis is Debug; other Log Levels are not needed and serve as placeholders for future enhancements and Customer requests.

For a Production System running without known issues, please run at the default **Info** log level, with all other log data turned off.

The default Log Level is "*Log*" for OS4k OSEM installations and "*Info*" for OSEM .iso Standalone/Cluster installations.

Additionally, Logs can be captured by setting the following messages to "*Yes*".

Log NodeRED messages = Captures all NodeRED logs produced

Log client messages = Captures all WPI communication between OSEM and Clients (Please note that GDPR relevant data is captured)

Log database messages = Captures all communication between OSEM and the CouchDB database (Please note that GDPR relevant data is captured)

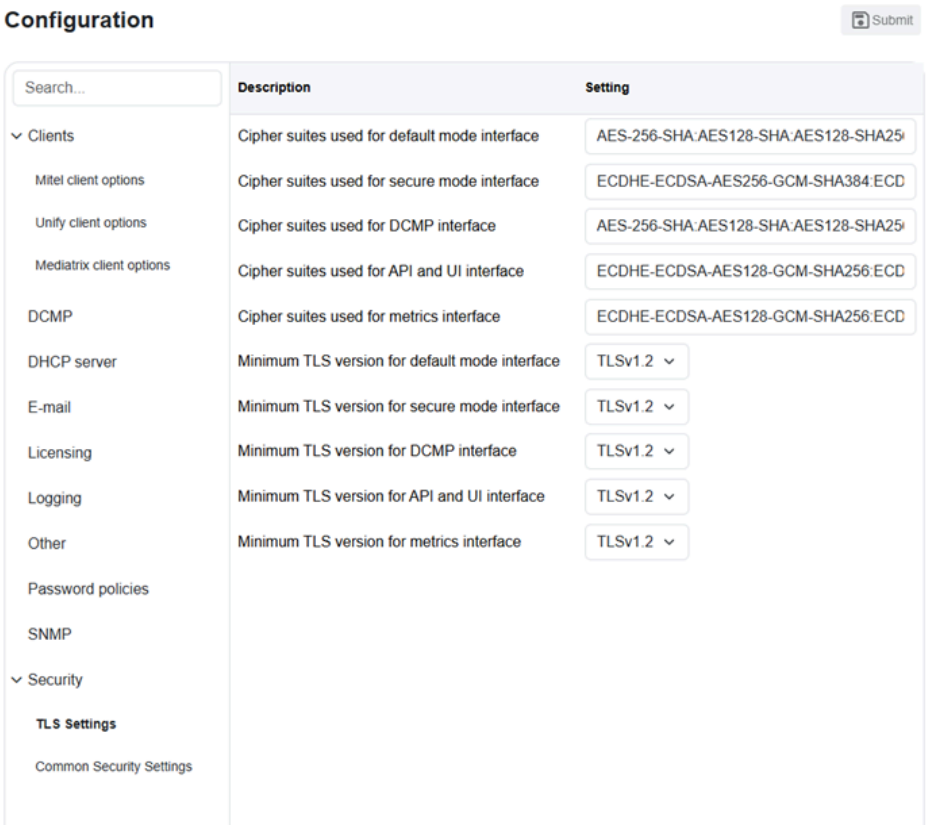
Log remote control messages = Remote logging for remote connection to Clients when using the remote control feature.

For more information about collecting Trace date for OSEM, please refer to the OSEM Troubleshooting and Diagnostic Basics Guide. The Guide can be found on the Software Download Server next to the Release Note.

16.5 OpenStage support

OSEM does support OpenStage Hardware; however, due to higher default security standards to allow OSEM to communicate with OpenStage devices, please change the cipher (Settings) to the following for the **Cipher suites used for the default mode interface** & **Cipher suites used for the DCMP interface**:

AES-256-SHA:AES128-SHA:AES128-SHA256:@SECLEVEL=0



16.6 SNMP & SNMP audit log

OSEM supports SNMP trap versions v1, v2, and v3. OSEM does not support SNMP GET requests; OSEM only supports the sending of SNMP Traps for events. SNMPv3 Traps are also used for Audit Logging.

To use audit logging, you need to use SNMPv3 together with Encryption. Please check your SNMP Trap collector on how to configure it to receive traps from OSEM. The Unify Service Fault Management Product fully supports SNMP trap in version 3 with Encryption.

Audit Logs are sent to the trap collector, for example, in the following scenarios:

- Account added
- Failed login
- Registered new Account
- Account deleted
- Backup uploaded/deleted/downloaded
- Certificate created/uploaded/downloaded/deleted
- Certificate added/removed to/from trust store
- Files uploaded/deleted
- Storage Provider added/deleted
- Access token created